Le Règlement général sur la protection des données et son impact en Suisse

Eva Thelisson

Le Règlement général sur la protection des données et son impact en Suisse

Eva Thelisson

Le Règlement général sur la protection des données et son impact en Suisse

Thèse

Présentée à la Faculté de droit de
l'Université de Fribourg (Suisse)

par
Eva Thélisson

pour l'obtention du grade de docteur en droit.

Acceptée par la Faculté de droit, le 18 juin 2018,

sur proposition du
Prof. Adriano Previtali (Président)
Prof. Henri Torrione (1er rapporteur)
Prof. Astrid Epiney (2ème rapporteur)
Prof. Jacques Dubey (Assesseur)
et
Prof. Arnold Rusch (Assesseur)

Lausanne, Suisse

soutenue le 19 Juin 2020

La Faculté de droit de l'Université de Fribourg (Suisse) n'entend ni approuver, ni désapprouver les opinions émises dans une thèse ; elles doivent être considérées comme propres à l'auteur (décision du Conseil de Faculté du 1er juillet 1916).

Avant-propos

La présente étude a été acceptée comme thèse de doctorat par la Faculté de droit de l'université de Fribourg sur proposition de Monsieur le professeur Henri Torrione (premier rapporteur) et de Madame la rectrice de l'université de Fribourg, Astrid Epiney, second rapporteur.

Ma profonde gratitude va tout d'abord à mon directeur de thèse, Monsieur le Professeur Henri Torrione, qui a su éveiller mon intérêt pour l'analyse juridique et qui m'a fait bénéficier de son expérience et de ses vastes connaissances scientifiques. Qu'il trouve ici l'expression de ma vive reconnaissance pour son soutien, ses conseils, et la confiance témoignés durant l'élaboration de cette thèse.

Mes remerciements s'adressent également à Madame la rectrice Astrid Epiney qui a bien voulu officier en tant que second rapporteur.

Je tiens aussi à remercier tous ceux, qui parmi mes collègues de l'administration fiscale des contributions, ont contribué de près ou de loin à cette étude, en particulier Messieurs Adrian Hug, Marc Bugnon, Alexandre Dumas et Philippe Abgottspon.

Ma vive reconnaissance va à ma famille et à Himanshu Verma pour leur confiance et leur soutien.

Fribourg, 26 avril 2020 Eva Thélisson

Sommaire

Avant-propos i

Sommaire iii

Table des matières v

Table des abrévations xvii

Bibliographie xxv

Table des illustrations cxxi

Introduction 1

I Le fondement du règlement général sur la protection des données 11

1 Les enjeux du Règlement 15

2 Le contexte de l'élaboration du Règlement 27

3 L'analyse juridique du Règlement 177

II Les modalités de mise en œuvre extraterritoriale du règlement général sur la protection des données 249

1 L'analyse du cadre juridique spécifique entre la Suisse et l'Union européenne 253

2 Les éléments principaux 261

3 Le rôle accru des autorités de contrôle 375

III Le développement du droit de la protection des données en Suisse 417

1 Le projet de LPD révisée 423

2 Vers une responsabilité croissante ? 461

3 La portée extraterritoriale du RGPD 489

Conclusion 545

Annexe : Les éléments principaux de mise en conformité au RGPD pour les entreprises suisses 551

Annexe : Repertoire alphabétique des matières 557

Table des matières

Avant-propos **i**
Sommaire **iii**
Table des matières **v**
Table des abrévations **xvii**
Les abréviations usuelles xvii
Les abréviations des réglementations citées xxii
Bibliographie **xxv**
Table des illustrations **cxxi**
Introduction **1**
§1 Le thème 1
§2 L'intérêt du thème 2
§3 Le plan général de la thèse 8
I Le fondement du règlement général sur la protection des données **11**
1 Les enjeux du Règlement **15**
§1 L'extra-territorialité du droit européen de la protection des données 17
I. Le ciblage du citoyen 17
II. Le marché des données à caractère personnel 18
III. L'intégration croissante de l'Europe de la protection des données 22
§2 Les modalités de contrôle *a posteriori* 24
I. Le citoyen 24
II. Le rôle des autorités de contrôle 24
III. Le juge 25
2 Le contexte de l'élaboration du Règlement **27**
§1 Le contexte historique et politique 28
I. Le processus législatif et les travaux préparatoires 28
A. Le contenu de la réforme soumise par la Commission européenne 33
B. Le Règlement : un texte de compromis 35
C. Les révélations d'Edward Snowden . . 36
D. L'invalidation de l'accord Safe Harbour par la Cour de Justice 38
E. L'accord « Privacy Shield » 41
II. L'effectivité du droit fondamental à la protection des données 44

A. Le cas d'espèce Wikileaks, du 7 mars 2017 45
B. La suppression de la neutralité du Net, du 26 mars 2017 45
C. La loi fédérale sur le renseignement en Suisse 46
§2 Le contexte technologique 47
I. Les objets connectés 50
II. Le marché des objets connectés 51
III. Les applications 52
A. Le domaine médical 52
B. Les bâtiments et villes « intelligentes » 58
C. Le transport autonome et la circulation routière 59
D. Les robots intelligents 81
E. Les risques des objets connectés 92
IV. La technologie Blockchain 94
V. Le Cloud Computing 100
VI. Le Big Data 107
VII. L'intelligence artificielle 113
VIII. Les technologies Fintech 125
§3 Le contexte juridique 130
I. Les sources internationales 131
A. L'article 17 du Pacte ONU II et la résolution 45/95 des Nations-Unies 131
B. L'organisation de Coopération et de Développement Économiques (OCDE) . . 131
C. Les normes « ISO » 132
D. Le projet d'une norme mondiale contraignante 135
II. Les sources communautaires 136
A. La charte des droits fondamentaux de l'Union européenne 136
B. L'article 8 de la Convention européenne des droits de l'homme 137
C. La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après « Conv.108 ») 138
D. La Cour de Justice de l'Union Européenne (ci-après « CJUE ») 138

(a) Les éléments historiques 139
(b) L'adoption de la Convention 108 . 141
(c) Les obligations des États signataires 141
(d) Les données sensibles 142
(e) La sécurité 143
(f) Les garanties 143
(g) Les dérogations 144
(h) Les sanctions 144
E. Le protocole additionnel à la Convention 108 146
F. La directive européenne sur la protection des données 95/46/CE 149
G. La directive 2002/58/CE 152
H. Les recommandations du « Groupe 29 » 155
I. La jurisprudence de la Cour de Justice de l'UE 156
(a) Le droit à la protection des données, un droit fondamental de l'Union 157
(b) La limitation des droits fondamentaux (article 52 de la Charte) 157
(c) L'analyse de l'article 52 158
(d) Le contrôle de proportionnalité . . 159
(e) L'analyse d'impact préalable . . . 163
J. L'exigence de garanties suffisantes contre les risques d'abus 167
K. L'arrêt Schwarz 167
L. La proposition de Règlement dédié à la libre-circulation des données non-personnelles 172
III. Les sources nationales 172
A. La Loi fédérale sur la protection des données (LPD) du 19 juin 1992, R.S 235.1 172
3 L'analyse juridique du Règlement 177
§1 Les buts du Règlement européen 177
§2 Le champ d'application matériel 180
§3 Le champ d'application territorial 187
§4 Les définitions 196
I. Les données personnelles (article 4, al. 1 du Règlement) 197
II. Le traitement (article 4, al. 2 du Règlement) . 199

III. Le profilage (article 4, al. 4 du Règlement) . . 201
IV. La pseudonymisation (article 4, al. 5 du Règlement) 202
V. La notion de fichier (article 4, al. 6 du Règlement) 204
VI. Le responsable du traitement (article 4, al. 7 du Règlement) 204
VII. Le sous-traitant (article 4, al. 8 du Règlement) 206
VIII. Le représentant (article 4, al. 17 du Règlement) 207
IX. Le destinataire (article 4, al. 9 du Règlement) 209
X. Le tiers (article 4, al. 10 du Règlement) 210
XI. La notion de consentement (article 4, al. 11 du Règlement) 210
XII. La violation de données à caractère personnel (article 4, al. 12 du Règlement) 214
XIII. Les données génétiques (article 4, al. 13 du Règlement) 217
XIV. Les données biométriques (article 4, al. 14 du Règlement) 218
XV. Les données concernant la santé (article 4, al. 15 du Règlement) 218
XVI. La notion d'établissement principal (article 4, al. 16 du Règlement) 219
XVII. La notion d'entreprise (article 4, al. 18 du Règlement) 220
XVIII. Les règles d'entreprises contraignantes (article 4, al. 19 du Règlement) 220
XIX. L'autorité de contrôle (article 4, al. 21 du Règlement) 220
XX. L'autorité de contrôle concernée (article 4, al. 22 du Règlement) 220
XXI. Le traitement transfrontalier (article 4, al. 23 du Règlement) 221
XXII. L'objection pertinente et motivée (article 4, al. 24 du Règlement) 222
§5 Les principes de protection des données 222
I. La licéité, la loyauté et la transparence (articles 5 et 6 du Règlement) 223
A. Le consentement 223
B. Le traitement nécessaire pour des finalités déterminées 230

(a) Le traitement nécessaire à l'exécution d'un contrat avec la personne concernée ou à l'exécution de mesures préparatoires à un tel contrat (article 6, al. 1 b) du Règlement) . . 230
(b) Le traitement nécessaire au respect d'une obligation légale (article 6, al. 1 c) du Règlement) 232
(c) Le traitement nécessaire à la sauvegarde des intérêts vitaux de la personne (article 6, al. 1 d) du Règlement) 232
(d) La mission d'intérêt public (article 6, al. 1, let e), du Règlement) 233
(e) Le traitement nécessaire aux fins d'intérêts légitimes (article 6, al. 1, f) du Règlement) 234
(f) Les autres fondements 237
II. La limitation des finalités 238
III. La minimisation des données (article 5, al. 1er, c du Règlement) 240
IV. Le principe d'exactitude des données (article 5, al. 1er, d du Règlement) 241
V. Le principe d'intégrité et de confidentialité (article 5, al. 1er, f du Règlement) 241
VI. Le principe de loyauté et de transparence (article 5, al. 1, a) du Règlement) 244
VII. Les données sensibles et judiciaires 245

II Les modalités de mise en œuvre extraterritoriale du règlement général sur la protection des données 249

1 L'analyse du cadre juridique spécifique entre la Suisse et l'Union européenne 253
§1 Les accords bilatéraux 253
I. Les aspects historiques 253
II. La présentation des accords bilatéraux 253
§2 Les acquis de Schengen et de Dublin 256
I. L'acquis de Schengen 256
II. L'acquis de Dublin 257
III. La reprise du Règlement européen en droit suisse 258

2 Les éléments principaux 261
§1 Les acteurs 261
§2 Le renforcement des droits des personnes concernées 263
I. Le droit à l'effacement des données (« droit à l'oubli ») 264
II. Droit d'accès, art. 15 RGPD 271
III. Droit à l'information 272
IV. Droit à la rectification des données 276
V. Droit à la portabilité des données 276
VI. Droit à la limitation du traitement 278
VII. Droit d'opposition 280
VIII. Profilage et décisions automatisées 282
A. La notion de décision automatisée . . . 282
(a) Le principe d'interdiction 283
(b) Les exceptions 283
(c) Les garanties à mettre en place pour le responsable du traitement 286
B. La spécificité du profilage effectuée sur la base du consentement explicite ou d'un contrat 291
C. Traitement automatisé licite 291
D. Les données sensibles 291
E. Le cas spécifique des mineurs 292
F. Les applications Blockchain 292
§3 La responsabilité des responsables du traitement et des sous-traitants 293
I. Le concept de Privacy-by-Design 301
II. Le concept de Privacy by Default 305
III. Le principe de transparence 308
IV. Le registre des activités de traitement 310
V. Analyse d'impact 311
VI. La notification d'une violation de données à caractère personnel 314
VII. Le contrôle *a posteriori* et les actions de mise en œuvre de ce contrôle 319
A. Éléments de procédure 319
B. L'action en responsabilité contre le responsable du traitement et les sous-traitants 320
C. Le droit à réparation et à la responsabilité du responsable du traitement et du sous-traitant 324

D. Les sanctions 327
VIII. Les nouvelles obligations du sous-traitant . . 329
IX. La désignation d'un délégué à la protection des données (ci-après « DPO ») 330
A. La notion de traitement à grande échelle 334
B. La notion de « suivi régulier et systématique » 336
C. Le profil requis 339
D. La nécessaire absence de conflit d'intérêts 343
E. Le statut de DPO 344
F. L'obligation au secret professionnel . . 345
G. Les obligations du responsable du traitement ou du sous-traitant envers le DPO 346
§4 Les flux transfrontaliers 347
I. Principe d'interdiction des flux transfrontaliers de données personnelles 348
A. La notion de transfert 349
B. Les sous-traitants 349
C. Les groupes d'entreprises 350
II. La compétence de la Commission européenne pour la décision d'adéquation (art. 45 RGPD) 350
A. Les nouveaux principes applicables aux transferts 351
(a) La décision d'adéquation 351
(b) Les conditions pour bénéficier d'une décision d'adéquation 352
(c) La procédure d'adoption d'une décision d'adéquation 353
(d) Les garanties fondamentales . . . 354
(e) L'examen périodique des décisions d'adéquation 355
III. L'accord Privacy Shield (article 45 RGPD) . . 358
IV. Les transferts fondés sur la base de garanties appropriées (art. 46 RGPD) 366
A. Les règles d'entreprises contraignantes ou Binding Corporate Rules (ci-après « BCR ») 368
B. Les clauses contractuelles 369
C. Les clauses types de protection des données adoptées par la Commission. . . . 370

(a) Les clauses contractuelles types approuvées par la Commission. . . . 371
(b) Les clauses types adoptées par une autorité de contrôle et approuvées par la Commission 371
D. Les codes de conduite et mécanismes de certification 372
3 Le rôle accru des autorités de contrôle 375
§1 Le mandat des autorités de contrôle 378
§2 Les missions des autorités de contrôle 379
I. L'indépendance des autorités de contrôle . . 382
A. La jurisprudence du Tribunal fédéral . 382
B. La jurisprudence de la CJUE 384
II. Le Règlement et la notion d'indépendance . 387
III. Les pouvoirs de l'autorité de contrôle 389
IV. Les mécanismes de coopération : l'autorité-chef de file et le mécanisme de guichet unique 394
V. La mise en œuvre du droit applicable 394
§3 L'autorité-chef de file 396
§4 Le mécanisme de guichet unique 396
I. Le principe 396
II. Les exceptions au mécanisme de guichet unique 400
§5 L'assistance mutuelle et les opérations conjointes 406
§6 Le Comité européen de la protection des données 409
I. Les missions du Comité 410
II. Le mécanisme du contrôle de la cohérence . 411
III. Les décisions contraignantes du Comité européen 413
IV. Les recours juridictionnels 414
III Le développement du droit de la protection des données en Suisse 417
1 Le projet de LPD révisée 423
§1 Historique 423
I. Les étapes de la révision 423
II. Avant-projet 429
A. Les définitions 430
B. Les principes 430
C. Le responsable du traitement 430
D. Le sous-traitant 433
E. Les personnes décédées 434
F. L'autorité de contrôle 434

G. Les flux transfrontaliers 436
III. La procédure de consultation 438
IV. La prise de position du Conseil Fédéral . . . 439
§2 Analyse comparée du projet de loi et du Règlement 444
§3 Les aspects politiques 452
§4 Les conséquences pour les cantons 453
§5 L'amélioration relative du cadre législatif suisse . 453
2 Vers une responsabilité croissante ? 461
§1 Les fonctions du droit de la responsabilité 462
I. La compensation des dommages 462
II. L'aspect dissuasif 463
III. La création d'un standard de comportement 465
§2 Vers une meilleure compréhension du contrôle a posteriori 467
I. L'action civile - Private Enforcement 470
A. La notion de Private Enforcement . . . 470
B. Les éléments principaux du Private Enforcement en droit américain 471
C. Le Private Enforcement en droit européen 471
D. Vers un mécanisme de Private Enforcement en droit suisse ? 476
II. L'action administrative - Public Enforcement 483
A. Droit européen de la protection des données 483
B. Droit suisse 485
3 La portée extraterritoriale du RGPD 489
§1 Le caractère extra-territorial du Règlement général sur la protection des données 489
I. Un champ d'application étendu du Règlement : Aperçu et caractéristiques des critères de l'art. 3 al. 2 RGPD 492
A. La notion d'extra-territorialité 492
B. Le critère de rattachement de l'établissement 493
C. Le critère du ciblage 498
D. Le critère du suivi de comportement . . 499
E. Le critère du droit international public 500
F. Le caractère extra-territorial en lien avec les transferts internationaux 501

§2 La question de la légitimité du caractère extra-territorial du RGPD 504
I. Une dérogation au principe de souveraineté territoriale 504
A. Le principe de souveraineté 504
B. Les principes du droit international . . 505
C. Les mutations du principe de souveraineté territoriale 509
D. La déterritorialisation du droit 511
E. Le rôle croissant du droit international privé 514
F. Applicabilité du droit étranger impératif 516
(a) Analyse critique 518
§3 La Jurisprudence de la CJUE 521
I. La portée géographique du droit au déréférencement 521
II. La portée géographique du Cloud Act 523
A. Une application extra-territoriale pour garantir un niveau de protection étendu 527
III. L'extra-territorialité justifiée par une volonté de sécurité juridique 532
A. Vers une juridiction sans lien avec le territoire ? 532
B. Un nouvel espace de circulation des données personnelles 532
C. Un nouveau rapport aux territoires institutionnels classiques 534
§4 La mise en oeuvre effective de l'extraterritorialité du RGPD 536
§5 Une mise en oeuvre effective á confirmer 537
I. Droit international privé 540
A. Compétence du juge 541
B. Droit applicable 542
§6 Conclusion 543
Conclusion **545**
§1 L'effectivité de la protection des données : un enjeu majeur à l'ère digitale 545
Annexe : Les éléments principaux de mise en conformité au RGPD pour les entreprises suisses **551**
§1 Identifier les traitements de données à caractère personnel et les flux de données 551

§2 Désigner un délégué à la protection des données (DPO) . . . 551
§3 Mettre à jour la déclaration relative à la vie privée (privacy notice) . . . 552
§4 Identifier la base légale de chaque traitement . . . 552
§5 Revoir la validité des consentements reçus . . . 552
§6 Développer des procédures pour répondre aux requêtes des personnes concernées qui voudront exercer leurs droits . . . 553
§7 Protection des mineurs de moins de 16 ans . . . 554
§8 Procédure en cas de violation des données à caractère personnel . . . 554
§9 Protection dès la conception et Protection par défaut . . . 555
§10 Analyse d'impact en matière de protection des données . . . 555
Annexe : Repertoire alphabétique des matières 557

Table des abrévations

Les abréviations usuelles

§	alinéa
ANSSI	Agence nationale de la sécurité des systèmes d'information
AP	avant-projet
art.	Article
ATAF	Arrêt du Tribunal administratif fédéral (BVGE)
ATF	Arrêt du Tribunal fédéral publié au recueil officiel des arrêts du Tribunal fédéral
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch (Code civil allemand), du 18 août 1896
BGH	Bundesgerichtshof
BK	Berner Kommentar
BO (année) E	Bulletin officiel de l'Assemblée fédérale (Conseil des Etats)
BO (année) N	Bulletin officiel de l'Assemblée fédérale (Conseil national)
BSK	Basler Kommentar
BV	Bundesverfassung
CC	Code civil suisse, du 10 décembre 1907 (RS 210)
CEPD	Comité européen de la protection des données
CF	Conseil fédéral
Cf.	Voir
Ch.	Chiffre
CICR	Comité international de la Croix-Rouge

Cir.	Circulaire
CIISE	Commission internationale de l'intervention et de la souveraineté des États (Ottawa)
CJCE	Cour de Justice des Communautés européennes (avant le 1er décembre 2009)
CJUE	Cour de Justice de l'Union européenne (après le 1er décembre 2009)
CN	Conseil national
CNIL	Commission nationale de l'informatique et des libertés (France)
CNPD	Commission nationale pour la protection des données (Grand-Duché de Luxembourg)
CNUDCI	Commission des Nations Unies pour le droit commercial international
COE	Conseil de l'Europe (Council of Europe)
COMCO	Commission de la concurrence
Com. UE	Commission de l'Union européenne
Cons. CE	Conseil des Communautés européennes
Cons. UE	Conseil de l'Union européenne
consid.	considérant
CourEDH	Cour européenne des droits de l'homme
CRID	Cahiers du centre de recherches informatique et droit
DARPA	Defense Advanced Research Projects Agency (United States of America) / Agence pour les projets de recherche avancée de défense
DDPS	Département fédérale de la défense, de la protection de la population et des sports.
DFAE / DAE	Département fédéral des affaires étrangères
DFJP	Département fédéral de justice et police
Digma	Zeitschrift für Datenrecht und Informationssicherheit
Dir.	Directive
direct.	sous la direction
disp. trans	dispositions transitoires
éd.	Édition
édit.	édité ou éditeur

EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖK	Eidgenössische Datenschutz- und Öffentlichkeitskommission
EDPB	European Data Protection Board / Comité Européen de la Protection des Données
EDPS	European Data Protection Supervisor / Le contrôleur européen de la protection des données
EDRi	European Digital Rights / Droits numériques européens
EPFL	Ecole Poythechnique Fédérale de Lausanne
EPIC	Electronic Privacy Information Center / Centre d'information électronique sur la vie privée
et al.	et alia
ex.	exemple
FAQ	Frequently Asked Questions / Foire aux questions
FINMA	Autorité fédérale de surveillance des marchés financiers
FF	Feuille fédérale
GPEN	Global Privacy Enforcement Network
IEEE	Institute of Electrical and Electronics Engineers / Institut des ingénieurs électriciens et électroniciens
IPRG	Bundesgesetz vom 18. Dezember 1987 über das internationale Privatrecht (LDIP, RS 291)
ISO	International Organization for Standardization / Organisation internationale de normalisation
JAAC	Jurisprudence des autorités administratives de la Confédération
JdT	Journal des Tribunaux
J.O.	Journal officiel
JOUE L. ou C.	Journal officiel de l'Union européenne (nouvelle dénomination). Législation ou Communication
KAPP	International Association for Privacy Professionnal

LAr	Loi fédérale sur l'archivage, du 26 juin 1998 (RS 152.1)
LCart	Loi fédérale du 6 octobre 1995 sur les cartels et autres restrictions á la concurrence (Loi sur les cartels) (RS 251)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (Loi sur la protection des données)(RS 235.1)
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement (LRens, RS 121)
LTrans	Loi fédérale du 17 décembre 2004, sur le principe de la transparence dans l'administration (Loi sur la transparence, R.S 152.3)
OCDE	Organisation de coopération et de développement économiques
OECD	Organisation for Economic Co-operation and Development
OFCOM	Office fédéral de la communication
OFJ	Office fédéral de la justice
OLPD	Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993, RS 235.11
p.	Page
PFPDT	Prépose fédéral à la protection des données et à la transparence
pp.	Pages
RDTI	Revue de Droit des Technologies de l'Information
Rev.tri.DH	Revue trimestrielle des droits de l'homme
RIDC	Revue international de droit comparé
s.a.	sans année
s.l.	sans location
SRC	Service de renseignement de la Confédération
ss	et suivants
STOA	Science and Technology Options Assessment Panel / Panel for the Future of Science and Technology (European Parliament)

TF	Tribunal fédéral
TPICE	Tribunal de 1ere instance des Communautés européennes
Trib. UE	Tribunal de l'Union européenne
U.E.	Union européenne
WP	Working Party / Group de travail
WP29	Article 29 Data Protection Working Party / Groupe de travail Article 29 sur la protection des données

Les abréviations des réglementations citées

CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales, du 4 novembre 1950 (R.S 0.101)
Charte	Charte des droits fondamentaux de l'Union européenne, du 26 octobre 2012 (2012/C 326/02)
Conv. 108	Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981 (R.S 0.235.1, STE no 108)
Cst.féd	Constitution fédérale, du 18 avril 1999 (RS 101)
Directive 95/46	Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 23.11.1995 L281/31)
Directive (UE) 2002/58/CE	Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
Directive (UE) 2015/2366	Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE
Directive (UE) 2016 / 680	Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

Directive SRI	Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (RS 235.1)
LAGH	Loi fédérale sur l'analyse génétique humaine, du 8 octobre 2004
Lar	Loi fédérale sur l'archivage, du 26 juin 1998 (RS 152.1)
LPD	Loi fédérale sur la protection des données, du 19 juin 1992 (RS 235.1)
Pacte ONU II	Pacte international relatif aux droits civils et politiques, du 13 décembre 1966, (RS. 0. 103. 2)
Protocole	Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de surveillance et les flux transfrontières de données
Résolution 45/95 des Nations-Unies	Résolution 45/95/ du 14 décembre 1990, relative aux principes directeurs pour la réglementation des fichiers personnels informatisés
Règlement (UE) 2016/679	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Traité	Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007

Bibliographie

Ouvrages

Abolhassan Ferri (édit.), *The Drivers of Digital Transformation : Why There's No Way Around the Cloud*, 1e éd., Cham 2017.

Agamben Giorgio / Thüring Hubert, *Die souveräne Macht und das nackte Leben*, 1e éd., Frankfurt am Main 2002.

Agrawal Ajay / Gans Joshua / Goldfarb Avi, *Prediction machines the simple economics of artificial intelligence*, 1e éd., Boston 2018.

Algan Yann / Cazenave Thomas, *L'État en mode start-up*, 1e éd., Paris 2016 (Cité : Algan / Cazenave, *L'État en mode start-up*).

Amstutz Marc / Hochreutener Inge / Stoffel Walter (édit.), *Die Praxis des Kartellgesetzes im Spannungsfeld von Recht und Ökonomie = La Loi sur les cartels dans la pratique : entre droit et économie*, 6e éd., Zürich 2011.

Arnold Martin / Meier Alfred / Spinnler Peter, *Steuerpflicht bei Auslandbezug*, in : Uebersax Peter / Münch Peter / Geiser Thomas / Arnold Martin (édit.), *Ausländerrecht : Ausländerinnen und Ausländer im öffentlichen Recht, Privatrecht, Strafrecht, Steuerrecht und Sozialrecht der Schweiz*, 1e éd., Basel 2002 (Cité : Arnold / Meier / Spinnler, *Steuerpflicht bei Auslandbezug*).

Asimov Isaac, *The Naked Sun*, London 2018 (Cité : Asimov, *The Naked Sun*).

Asimov Isaac / Hodgson Jeffrey, *Robot visions*, 3e éd., London 1990 (Cité : Asimov / Hodgson, *Robot visions*).

Bachimont Bruno, *Patrimoine et numérique : technique et politique de la mémoire*, 1e éd., Bry-sur-Marne 2017.

Baldwin Robert / Cave Martin / Lodge Martin, *Understanding regulation : theory, strategy, and practice*, 2e éd., Oxford 2012.

Banck Aurélie, *RGPD : la protection des données à caractère personnel : 18 fiches pour réussir votre mise en conformité*, 1e éd., Issy-les-Moulineaux 2018 (Cité : Banck, *RGPD*).

Barroso Luiz André / Hölzle Urs / Parthasarathy Ranganathan, *The datacenter as a computer : designing warehouse-scale machines*, 3e éd., San Rafael 2019.

Bauer Hannes / Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, Berlin 2019.

Belser Eva Maria / Epiney Astrid / Waldmann Bernhard / Bickel Jürg, *Datenschutzrecht : Grundlagen und öffentliches Recht*, 1e éd., Bern 2011.

Benkler Yochai / Cashman Marc, *The penguin and the leviathan : how cooperation triumphs over self-interest*, New York 2011.

Bensoussan Alain (direct.), *Règlement européen sur la protection des données : Textes, commentaires et orientations pratiques*, 1e éd., Bruxelles 2016 (Cité : Bensoussan, *Règlement européen sur la protection des données (1e éd.)*).

Bensoussan Alain (direct.), *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques*, 2e éd., Bruxelles 2018 (Cité : Bensoussan, *Règlement européen sur la protection des données (2e éd.)*).

Benyekhlef Karim / Trudel Pierre (édit.), *Etat de droit et virtualité*, Montréal 2009.

Berger Kurzen Brigitte, *E-health und Datenschutz*, thèse, Zürich 2004 (Cité : Berger Kurzen, *E-health und Datenschutz*).

Besson Samantha, *Droit international public*, 1e éd., Berne 2019 (Cité : Besson, *Droit international public*).

Bizzozero Alessandro / Falleti André / Meregalli Do Duc Samantha (édit.), *Le mandat de gestion de fortune*, 2e éd., Zürich 2017.

Bizzozero Alessandro / Robinson Christopher, *Activités financières cross-border vers et depuis la Suisse*, 1e éd., Bulle 2010 (Cité : Bizzozero / Robinson, *Activités financières cross-border vers et depuis la Suisse*).

Boillet Véronique / Maiani Francesco / Poltier Etienne / Rietiker Daniel / Wilson Barbara (édit.), *L'influence du droit de l'Union européenne et de la Convention européenne des droits de l'homme sur le droit suisse*, 1e éd., Genève 2016.

Bostrom Nick, *Superintelligence : paths, dangers, strategies*, Oxford 2017 (Cité : Bostrom, *Superintelligence*).

Bourgeois Matthieu / Bounedjoum Amira / Lepage Agathe / Souvira Anne, *Droit de la donnée : principes théoriques et approche pratique*, 1e éd., Paris 2017.

Boutonnet Christophe, *Rapport CIGREF « Economie des données personnelles »*, Paris 2015 (Cité : Boutonnet, *Rapport CIGREF*).

Braibant Guy, *La Charte des droits fondamentaux de l'Union européenne*, 1e éd., Paris 2001 (Cité : Braibant, *La Charte des droits fondamentaux de l'UE*).

Breitenmoser Stephan, *Internationale Amts- und Rechtshilfe*, in : Uebersax Peter / Münch Peter / Geiser Thomas / Arnold Martin (édit.), *Ausländerrecht : Ausländerinnen und Ausländer im öffentlichen Recht, Privatrecht, Strafrecht, Steuerrecht und Sozialrecht der Schweiz*, 1e éd., Basel 2002 (Cité : Breitenmoser, *Internationale Amts- und Rechtshilfe*).

Breitenmoser Stephan / Gless Sabine / Lagodny Otto (édit.), *Schengen in der Praxis : Erfahrungen und Ausblicke*, 1e éd., Zürich 2009.

Brosset Estelle / Gambardella Sophie / Guylène Nicolas, *La santé connectée et «son» droit : approches de droit européen et de droit français*, 1e éd., Aix-en-Provence 2017.

Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016 (Cité : Calo / Froomkin / Kerr, *Robot Law*).

Castets-Renard Céline (direct.), *Quelle protection des données personnelles en Europe ?*, 1e éd., Bruxelles 2015 (Cité : Castets-Renard, *Quelle protection des données personnelles en Europe ?*).

Cavoukian Ann / Tapscott Don, *Who knows : safeguarding your privacy in a networked world*, 2e éd., New York 1997 (Cité : Cavoukian / Tapscott, *Who knows*).

de Clercq Chloë / Dechamps Frédéric, *« Internet à l'épreuve du droit ou le droit à l'épreuve d'Internet : une analyse au regard de la problématique de l'étendue géographique du droit européen au déréférencement »*, in : Féral-Schuhl Christiane (édit.), *Cyberdroit : le droit à l'épreuve de l'Internet*, 7e éd., Paris 2018 (Cité : de Clercq / Dechamps, *« Internet à l'épreuve du droit »*).

Cooper Diana Marina, *The application of a "sufficiently and selectively open license" to limit liability and ethical concerns associated with robotics*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016 (Cité : Cooper, *The application of a "sufficiently and selectively open license"*).

Coutellier Clyde / Botchorichvili Nana, *Le rôle nouveau accordé au sous-traitant dans la protection des données à caractère personnel par le Règlement général sur la protection des données*, thèse, Paris 2017.

Crombois Kimberley, *Le profilage et les nouveaux défis du droit de la vie privée et de la protection des données à caractère personnel : analyse du profilage au regard du Règlement européen : peut-on parler d'une renonciation à la vie privée ?*, thèse, Louvain 2016.

Custers Bart / Calders Toon / Schermer Bart / Zarsky Tal (édit.), *Discrimination and Privacy in the Information Society : Data Mining and Profiling in Large Databases*, Berlin 2014.

De Rosnay Joël, *Je cherche à comprendre : les codes cachés de la nature*, 1e éd., Paris 2016 (Cité : De Rosnay, *Je cherche à comprendre*).

De Terwangne Cécile / Rosier Karen (direct.), *Le Règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie*, 1e éd., Bruxelles 2018.

Decaux Emmanuel, *L'application extraterritoriale du droit économique, Cahiers du CEDIN*, 3e éd., Paris 1987 (Cité : Decaux, *L'application extraterritoriale du droit économique*).

Degrave Elise / de Terwangne Cécile / Dusollier Séverine / Queck Robert (édit.), *Law, norms and freedoms in cyberspace : liber amicorum Yves Poullet*, 1e éd., Bruxelles 2018.

Delmas-Marty Mireille, *Vers une communauté de valeurs ? : les forces imaginantes du droit (IV)*, 1e éd., Paris 2011 (Cité : Delmas-Marty, *Vers une communauté de valeurs ?*).

Delort Pierre, *Le big data (Que sais-je ?)*, 2e éd., Paris 2018 (Cité : Delort, *Le big data*).

Dewitte Pierre, *Protection des données à caractère personnel + moteurs de recherche = droit à l'oubli ? Deux ans après la jurisprudence Google Spain et à l'aube du nouveau règlement, retour sur la mise en oeuvre d'une algèbre controversée*, thèse, Louvain 2016.

Docquir Benjamin (édit.), *Vers un droit européen de la protection des données ?*, 1e éd., Bruxelles 2017 (Cité : Docquir, *Vers un droit européen de la protection des données ?*).

Docquir Benjamin, *Droit du numérique : contrats, innovation, données et sécurité*, 1e éd., Bruxelles 2018 (Cité : Docquir, *Droit du numérique*).

Domingo-Ferrer Josep / Hansen Marit / Hoepman Jaap-Henk / Le Métayer Daniel / Tirtea Rodica / Schiffner Stefan / Danezis George, *Privacy and data protection by design - from policy to engineering*, Heraklion 2014 (Cité : Domingo-Ferrer, *Privacy and data protection by design*).

Domingos Pedro, *The Master Algorithm : How the Quest for the Ultimate Learning Machine will Remake Our World*, 1e éd., New York 2018 (Cité : Domingos, *The Master Algorithm*).

Dupont Anne-Sylvie, *Les données confiées aux assureurs sociaux*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019 (Cité : Dupont, *Les données confiées aux assureurs sociaux*).

Ehmann Eugen / Selmayr Martin (édit.), *Datenschutz - Grundverordnung*, 2e éd., Wien 2018 (Cité : Ehmann / Selmayr, *Datenschutz - Grundverordnung*).

Epiney Astrid, *Zu ausgewählten Herausforderungen des Datenschutzrechts*, in : Epiney Astrid / Progin-Theuerkauf Sarah (édit.), *Datenschutz in Europa und die Schweiz = La protection des données en Europe et la Suisse*, 1e éd., Zürich 2006.

Epiney Astrid, *Zu den völker- und europarechtlichen Rahmenbedingungen der Revision des Datenschutzgesetzes*, in : Epiney Astrid / Brunner Stephan C. (édit.), *Revision des Datenschutzgesetzes = La révision de la Loi sur la protection des données*, 1e éd., Zürich 2009.

Epiney Astrid / Brunner Stephan C. (édit.), *Revision des Datenschutzgesetzes = La révision de la Loi sur la protection des données*, 1e éd., Zürich 2009.

Epiney Astrid / Hänni Julia / Brülisauer Flavia (édit.), *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, Zürich 2012 (Cité : Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*).

Epiney Astrid / Kern Markus, *Zu den Neuerungen im Datenschutzrecht der Europäischen Union*, in : Epiney Astrid / Nüesch Daniela (édit.), *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, 1e éd., Zürich 2016 (Cité : Epiney / Kern, *Zu den Neuerungen im Datenschutzrecht der Europäischen Union*).

Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015 (Cité : Epiney / Nüesch, *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*).

Epiney Astrid / Nüesch Daniela (édit.), *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, 1e éd., Zürich 2016 (Cité : Epiney / Nüesch, *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*).

Epiney Astrid / Probst Thomas / Gammenthaler Nina (édit.), *Datenverknüpfung, Problematik und rechtlicher Rahmen = L' interconnexion de données, problématique et cadre juridique*, Zürich 2011.

Epiney Astrid / Progin-Theuerkauf Sarah (édit.), *Datenschutz in Europa und die Schweiz = La protection des données en Europe et la Suisse*, 1e éd., Zürich 2006.

Epiney Astrid / Progin-Theuerkauf Sarah, *Datenschutz in Europa : Überblick und Implikationen in den Bilateralen II*, in : Epiney Astrid / Progin-Theuerkauf Sarah (édit.), *Datenschutz in Europa und die Schweiz = La protection des données en Europe et la Suisse*, 1e éd., Zürich 2006.

Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019.

Ervik Sara, *Privacy by Design applied in Practice and the Consequences for System Developers*, thèse, Stockholm 2019 (Cité : Ervik, *Privacy by Design applied in Practice and the Consequences for System Developers*).

European Commission / Directorate-General Communication, *A digital single market in Europe : bringing down barriers to unlock online opportunities.*, 1e éd., Luxembourg 2016.

Fallon Marc, *Les règles d'applicabilité en droit international privé*, in : Vander Elst Raymond (édit.), *Mélanges offerts à Raymond Vander Elst*, 1e éd., Bruxelles 1986 (Cité : Fallon, *Les règles d'applicabilité en droit international privé*).

Falque-Pierrotin Isabelle / Avignon Céline / Bensoussan-Brulé Virginie / Torres Chloé / Bensoussan Alain, *Règlement européen sur la protection des données : Le règlement européen « Data protection » adopté le 27 avril 2016 consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés*, Cork 2016 (Cité : Falque-Pierrotin, *Règlement européen sur la protection des données*).

Fasnacht Tobias, *Die Einwilligung im Datenschutzrecht Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht*, thèse, Freiburg 2017 (Cité : Fasnacht, *Die Einwilligung im Datenschutzrecht*).

Feral-Schuhl Christiane, *Comment les droits de la personne concernée sont-ils renforcés ?*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Feral-Schuhl, *Comment les droits de la personne concernée sont-ils renforcés ?*).

Féral-Schuhl Christiane (édit.), *Cyberdroit : le droit à l'épreuve de l'Internet*, 7e éd., Paris 2018.

Ferry Luc, *La révolution transhumaniste*, Paris 2016 (Cité : Ferry, *La révolution transhumaniste*).

Fischer Philipp / Richa Alexandre, *U.S. pretrial discovery on Swiss soil*, 1e éd., Basel 2010 (Cité : Fischer / Richa, *U.S. pretrial discovery on Swiss soil*).

Flückiger Alexandre, *Jurisprudence actuelle en matière de protection des données*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015 (Cité : Flückiger, *Jurisprudence actuelle en matière de protection des données*).

Ford Martin, *Rise of the robots : technology and the threat of a jobless future*, New York 2015 (Cité : Ford, *Rise of the robots*).

Forest David, *Droit des données personnelles*, 2e éd., Paris 2011.

Frei Nula, *Die Datenschutz-Grundverordnung und die Schweiz*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019 (Cité : Frei, *Die Datenschutz-Grundverordnung*).

Frenzel Eike Michael, *Grundsätze - Rechtmäßigkeit der Verarbeitung*, in : Paal Boris P. / Pauly Daniel A. (édit.), *Datenschutz - Grundverordnung*, 2e éd., München 2017 (Cité : Frenzel, *Grundsätze*).

Friedel-Souchu Evelyne, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*, thèse, Paris 1992 (Cité : Friedel-Souchu, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*).

Fukuyama Francis, *La fin de l'homme : les conséquences de la révolution biotechnique*, Paris 2002 (Cité : Fukuyama, *La fin de l'homme*).

Fukuyama Francis, *State Building : Gouvernance et ordre du monde au XXIème siècle*, Paris 2005.

Gallardo Meseguer Marc, *Aperçu de la dimension internationale du Règlement général sur la protection des données à caractère personnel*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Gallardo Meseguer, *Aperçu de la dimension internationale*).

Gavroy Robin, *Les drones et le droit au respect de la vie privée : Big Brother a-t-il le droit de voler en Belgique ?*, thèse, Louvain 2016 (Cité : Gavroy, *Les drones et le droit au respect de la vie privée*).

Geffaray Edouard, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*).

Gilchrist Alasdair, *IoT security issues*, 1e éd., Boston 2017.

Goertzel Ben / Goertzel Ted (édit.), *The End of the Beginning : Life, Society and Economy on the Brink of the Singularity*, 1e éd., Los Angeles 2015.

Gola Peter, *EU-DS-GVO EU-Datenschutz-Grundverordnung*, 1e éd., München 2016 (Cité : Gola, *EU-DS-GVO EU - Datenschutz - Grundverordnung*).

González Fuster Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 1e éd., Cham 2014 (Cité : González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*).

Grisel Guillaume, *Application extraterritoriale du droit international des droits de l'homme*, thèse, Lausanne 2010 (Cité : Grisel, *Application extraterritoriale du droit international des droits de l'homme*).

Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*).

Guerin Antoine, *Quelle doit être la place du public enforcement et du private Enforcement en droit de la concurrence ?*, thèse, Paris 2016 (Cité : Guerin, *Quelle doit être la place du public enforcement et du private enforcement en droit de la concurrence ?*).

Guillaume Florence, *Droit international privé : partie générale et procédure civile internationale*, 4e éd., Bâle 2018 (Cité : Guillaume, *Droit international privé*).

Habermas Jürgen, *L'avenir de la nature humaine : vers un eugénisme libéral ?*, 3e éd., Paris 2015 (Cité : Habermas, *L'avenir de la nature humaine*).

Harari Yuval Noah, *21 Lessons for the 21st Century*, 1e éd., London 2018 (Cité : Harari, *21 Lessons*).

Harari Yuval Noah, *Homo Deus : A brief history of tomorrow*, 1e éd., New York 2018 (Cité : Harari, *Homo Deus*).

Harrison Harry / Minsky Marvin, *The Turing option : A Novel*, New York 1992 (Cité : Harrison / Minsky, *The Turing option*).

Härting Niko, *Datenschutz-Grundverordnung*, Köln 2016 (Cité : Härting, *Datenschutz-Grundverordnung*).

Helbing Dirk / Frey Bruno S. / Gigerenzer Gerd / Hafen Ernst / Hagner Michael / Hofstetter Yvonne / van den Hoven Jeroen / Zicari Roberto V. / Zwitter Andrej, *Will Democracy Survive Big Data and Artificial Intelligence ?*, in : Helbing Dirk (édit.), *Towards Digital Enlightenment : Essays on the Dark and Light Sides of the Digital Revolution*, Cham 2019 (Cité : Helbing, *Will Democracy Survive Big Data and AI ?*).

Heylighen Francis, *Return to Eden ? Promises and Perils on the Road to a Global Superintelligence*, in : Goertzel Ben / Goertzel Ted (édit.), *The End of the Beginning : Life, Society and Economy on the Brink of the Singularity*, 1e éd., Los Angeles 2015 (Cité : Heylighen, *Return to Eden ?*).

Hildebrandt Mireille, *The New Imbroglio - Living with Machine Algorithms*, in : Janssens Liisa (édit.), *The Art of Ethics in the Information Society*, 1e éd., Amsterdam 2016 (Cité : Hildebrandt, *The New Imbroglio*).

Hilgendorf Eric / Seidel Uwe (édit.), *Robotics, autonomics, and the law : legal issues arising from the autonomics for industry 4.0 technology programme of the German federal Ministry for economic affairs and energy*, 1e éd., Baden-Baden 2017 (Cité : Hilgendorf / Seidel, *Robotics, autonomics, and the law*).

Hummler Konrad / Schönenberger Fabian (édit.), *Total Data - Total Control Nulltoleranz in allen Lebensbereichen*, Zürich 2017.

Hurni Béatrice, *L'action civile en droit de la concurrence : étude du droit suisse à la lumière du droit comparé et du droit de l'Union européenne*, thèse, Fribourg 2017 (Cité : Hurni, *L'action civile en droit de la concurrence*).

Israel Marc, *Cloud privé, hybride et public : Quel modèle pour quelle utilisation ? Un état de l'art et des bonnes pratiques*, 1e éd., St. Herblain 2018.

Jammet Adrien / Lavenue Jean-Jacques, *La prise en compte de la vie privée dans l'innovation technologique*, thèse, Lille 2018.

Janssens Liisa (édit.), *The Art of Ethics in the Information Society*, 1e éd., Amsterdam 2016.

Jessup Philip Caryl, *Transnational law*, Yale 1956 (Cité : Jessup, *Transnational law*).

Kern Markus / Epiney Astrid, *Durchsetzungmechanismen im EU - Recht und ihre Implikationen für die Schweiz*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015 (Cité : Kern / Epiney, *Durchsetzungmechanismen im EU*).

Kerr Ian / Szilagyi Katie, *Asleep at the switch ? How killer robots become a force multiplier of military necessity*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016 (Cité : Kerr / Szilagyi, *Asleep at the switch ?*).

Knyrim Rainer (édit.), *Kommentar zum Datenschutzrecht, DSGVO samt DSG und Nebenbestimmungen Kommentar in Faszikeln*, 1e éd., Wien 2018.

Koumpli Christina, *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données personnelles - Etude comparée : Union Européenne, Allemagne, France, Grèce, Royaume-Uni*, thèse, Paris 2019 (Cité : Koumpli, *Les données personnelles sensibles*).

Kühling Jürgen, *Die Europäisierung des Datenschutzrechts : Gefährdung deutscher Grundrechtsstandards ?*, 1e éd., Baden-Baden 2014.

Kühling Jürgen / Buchner Benedikt (édit.), *Datenschutz - Grundverordnung : Kommentar*, 1e éd., München 2017 (Cité : Kühling / Buchner, *Datenschutz - Grundverordnung*).

Kühling Jürgen / Buchner Benedikt (édit.), *Datenschutz - Grundverordnung / BDSG : Kommentar*, 2e éd., München 2018 (Cité : Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*).

Kurzweil Ray, *The singularity is near : when humans transcend biology*, New York 2005.

Lebon Lydia, *La territorialité et l'Union européenne : approches de droit public*, thèse, Bordeaux 2013 (Cité : Lebon, *La territorialité et l'Union européenne*).

Leenes Ronald / Brakel Rosamunde van / Gutwirth Serge / Hert Paul de (édit.), *Data protection and privacy : (in)visibilities and infrastructures*, Cham 2017.

Lemberger Pirmin / Batty Marc / Morel Médéric / Raffaëlli Jean-Luc / Géron Aurélien, *Big data et machine learning : les concepts et les outils de la data science*, 2e éd., Malakoff 2016 (Cité : Lemberger, *Big data et machine learning*).

Lhemery François / Roques-Bonnet Marie-Charlotte, *Peering into the Future of Privacy*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Lhemery / Roques-Bonnet, *Peering into the Future of Privacy*).

Li Deyi / Du Yi, *Artificial intelligence with uncertainty*, 2e éd., Boca Raton 2017.

Locher Peter (édit.), *Kommentar zum DBG : Bundesgesetz über die direkte Bundessteuer*, 1e éd., Basel 2001 (Cité : Locher, *Kommentar zum DBG*).

Lutzi Tobias, *The Platform Economy and Private International Law*, in : Pretelli Ilaria (édit.), *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales : actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, 1e éd., Genève 2018 (Cité : Lutzi, *The Platform Economy*).

Mayer Anna, *Diskussionsansätze in der Debatte um die Regulierung von Dateneigentum : Ein Vergleich zwischen Deutschland und Japan*, in : Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, 3e éd., Leipzig 2019 (Cité : Mayer, *Diskussionsansätze*).

Meier Philippe, *Protection des données : fondements, principes généraux et droit privé*, 1e éd., Berne 2011.

Millar Jason / Kerr Ian, *Delegation, relinquishment and responsibility : The prospect of expert robots*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016 (Cité : Millar / Kerr, *Delegation, relinquishment and responsibility*).

Moerel Lokke, *Binding Corporate Rules : Corporate Self-Regulation of Global Data Transfers*, Oxford 2012 (Cité : Moerel, *Binding Corporate Rules*).

Müller Gerhard F., *Der Datenschutzbeauftragte.*, München 1981 (Cité : Müller, *Datenschutzbeauftragte*).

Narayanan Arvind / Bonneau Joseph / Felten Edward / Miller Andrew / Goldfeder Steven, *Bitcoin and cryptocurrency technologies : a comprehensive introduction*, 1e éd., Princeton 2016 (Cité : Narayanan, *Bitcoin and cryptocurrency technologies*).

Neale Alan Derrett / Stephens Mel L., *International business and national jurisdiction*, 1e éd., Oxford 1988 (Cité : Neale / Stephens, *International business and national jurisdiction*).

Nerbonne Sophie, *Le nouveau rôle des autorités de contrôle*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Nerbonne, *Le nouveau rôle des autorités de contrôle*).

Nivert Nirmal, *Intérêt général et droits fondamentaux*, thèse, Saint-Denis 2012 (Cité : Nivert, *Intérêt général et droits fondamentaux*).

O'Neil Cathy, *Weapons of math destruction : how big data increases inequality and threatens democracy*, 1e éd., London 2017.

Orwell George, *Nineteen eighty-four*, Boston 1987 (Cité : Orwell, *Nineteen eighty-four*).

Paal Boris P. / Pauly Daniel A. (édit.), *Datenschutz - Grundverordnung*, 2e éd., München 2017.

Paal Boris P. / Pauly Daniel A., *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, 1e éd., München 2018 (Cité : Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*).

Patklom Thasanee, *Herausforderungen bei der Umsetzung des Datenschutzes für ein Schweizer Unternehmen*, 1e éd., Zürich 2018 (Cité : Patklom, *Herausforderungen bei der Umsetzung des Datenschutzes*).

Perrin Olivier, *L'anonymisation des informations et l'authentification biométrique pourraient permettre de lutter efficacement contre les vols de données bancaires*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Perrin, *L'anonymisation des informations*).

Pinaud Florence, *#MaVieSous algorithmes*, 1e éd., Paris 2018 (Cité : Pinaud, *#MaVieSous algorithmes*).

Placco Agostino Valerio, *La protection des données à caractère personnel dans le cadre de la jurisprudence de la cour de justice de l'union européenne relative aux droits fondamentaux*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Placco, *La protection des données à caractère personnel*).

Plath Kai-Uwe / Becker Thomas, *DSGVO/BDSG : Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG*, 3e éd., Köln 2018.

Poullet Yves, *La vie privée à l'heure de la société du numérique*, 1e éd., Bruxelles 2019 (Cité : Poullet, *La vie privée à l'heure de la société du numérique*).

Poullet Yves / Rouvroy Antoinette, *Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie*, in : Benyekhlef Karim / Trudel Pierre (édit.), *Etat de droit et virtualité*, Montréal 2009 (Cité : Poullet / Rouvroy, *Le droit à l'autodétermination informationnelle et la valeur du développement personnel*).

Préteceille Nicolas, *IoT & RGPD : maximisez les opportunités et minimisez les risques*, 1e éd., St. Herblain 2018.

Pretelli Ilaria (édit.), *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales : actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, 1e éd., Genève 2018 (Cité : Pretelli, *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales*).

Prévost Stéphane / Royer Erwan, *Le RGPD*, 1e éd., Paris 2018.

Ragheno Nathalie, *Data protection & privacy. Le GDPR dans la pratique / De GDPR in de praktijk.*, 1e éd., Louvain-La Neuve 2017.

Raiser Thomas, *Grundlagen der Rechtssoziologie : das lebende Recht*, 6e éd., Tübingen 2013.

Richards Neil M. / Smart William D., *How should the law think about robots ?*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot law*, 1e éd., Cheltenham 2016 (Cité : Richards / Smart, *How should the law think about robots ?*).

Rifkin Jeremy, *The Age of Access : The New Culture of Hypercapitalism Where all of Life is a Paid-For Experience*, 1e éd., New York 2001.

Rigaux François / Delpérée Francis, *Le concept du peuple*, 1e éd., Bruxelles 1988 (Cité : Rigaux / Delpérée, *Le concept*).

Roberto Vito, *Schweizerisches Haftpflichtrecht*, 1e éd., Zürich 2002 (Cité : Roberto, *Schweizerisches Haftpflichtrecht*).

Ross Alec, *The industries of the future*, 1e éd., London 2017 (Cité : Ross, *The industries of the future*).

Rouvroy Antoinette, *Homo juridicus est-il soluble dans les données ?*, in : Degrave Elise / de Terwangne Cécile / Dusollier Séverine / Queck Robert (édit.), *Law, norms and freedoms in cyberspace : liber amicorum Yves Poullet*, 1e éd., Bruxelles 2018 (Cité : Rouvroy, *Homo juridicus est-il soluble dans les données*).

Salmon Jean / Cahier Philippe / Caflisch Lucius / Dominicé Christian / Kolb Robert / de Chazournes Laurence Boisson (édit.), *Dictionnaire de droit international public*, Bruxelles 2001 (Cité : Salmon, *Dictionnaire de droit*).

Sassenberg Thomas / Faber Tobias (édit.), *Rechtshandbuch Industrie 4.0 und Internet of Things Praxisfragen und Perspektiven der digitalen Zukunft.*, 1e éd., München 2017.

Sauvain Monique Cossali, *L'effectivité des mécanismes de mise en oeuvre du point de vue de l'OFJ*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015 (Cité : Sauvain, *L'effectivité des mécanismes*).

Schindler Dietrich, *Die Europaverträglichkeit des schweizerischen Rechts*, 1e éd., Zürich 1990 (Cité : Schindler, *Die Europaverträglichkeit des schweizerischen Rechts*).

Schneider Jochen, *Datenschutz : nach der EU - Datenschutz - Grundverordnung*, 2e éd., München 2019 (Cité : Schneider, *Datenschutz*).

Schwab Klaus, *The fourth industrial revolution*, 1e éd., London 2017.

Schweer Dieter / Sahl Jan Christian, *The Digital Transformation of Industry – The Benefit for Germany*, in : Abolhassan Ferri (édit.), *The Drivers of Digital Transformation : Why There's No Way Around the Cloud*, Cham 2017 (Cité : Schweer / Sahl, *The Digital Transformation of Industry*).

Simitis Spiros, *Entwicklung und Dilemmata des Datenschutzes*, in : Epiney Astrid / Hänni Julia / Brülisauer Flavia (édit.), *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, Zürich 2012 (Cité : Simitis, *Entwicklung und Dilemmata des Datenschutzes*).

Simitis Spiros (édit.), *Bundesdatenschutzgesetz : Kommentar*, 8e éd., Baden-Baden 2014 (Cité : Simitis, *Bundesdatenschutzgesetz*).

Simitis Spiros / Hornung Gerrit / Döhmann Spiecker Indra (édit.), *Datenschutzrecht : DSGVO mit BDSG*, 1e éd., Baden-Baden 2018 (Cité : Simitis / Hornung / Döhmann, *Datenschutzrecht : DSGVO mit BDSG*).

Sironi Paolo, *FinTech innovation : from robo-advisors to goal based investing and gamification*, 1e éd., Chichester West Sussex 2016.

Skouma Georgia / Léonard Laura, *Les grands changements liés à la règlementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professonnels*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : Skouma / Léonard, *Les grands changements*).

Spindler Gerald / Schuster Fabian (édit.), *Recht der elektronischen Medien : Kommentar*, 3e éd., München 2015 (Cité : Spindler / Schuster, *Recht der elektronischen Medien*).

Springer Paul J. (édit.), *Encyclopedia of Cyber Warfare*, Santa Barbara 2017 (Cité : Springer, *Encyclopedia of Cyber Warfare*).

Stanford University, *Artificial intelligence and life in 2030 : one hundred year study on artificial intelligence; report of the 2015 study panel*, Stanford 2016.

Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, 3e éd., Leipzig 2019.

Stoffel Walter A., *Das neue Kartell - Zivilrecht*, in : Zäch Roger (édit.), *Neue schweizerische Kartellgesetz*, 1e éd., Zürich 1996 (Cité : Stoffel, *Das neue Kartell - Zivilrecht*).

Sydow Gernot (édit.), *Europäische Datenschutzgrundverordnung : Handkommentar*, 2e éd., Baden-Baden 2018 (Cité : Sydow, *Europäische Datenschutzgrundverordnung*).

Tapscott Don / Tapscott Alex, *Blockchain Revolution : How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 1e éd., London 2016 (Cité : Tapscott / Tapscott, *Blockchain Revolution*).

de Terwangne Cécile, *Droit à l'oubli, droit à l'effacement ou droit au déréferencement ? Quand le législateur et le juge européen dessinent les contours du droit à l'oubli numérique*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015 (Cité : de Terwangne, *Droit à l'oubli, droit à l'effacement ou droit au déréferencement ?*).

Thelisson Eva, *Un État mondial via Internet ?*, 1e éd., Paris 2012 (Cité : Thelisson, *Un État mondial via Internet ?*).

Thouvenin Florent, *Privatversicherungen : Datenschutzrecht als Grenze der Individualisierung ?*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019 (Cité : Thouvenin, *Privatversicherungen*).

Thouvenin Florent / Hettich Peter / Burkert Herbert / Gasser Urs, *Remembering and forgetting in the digital age*, Cham 2018.

Uebersax Peter / Münch Peter / Geiser Thomas / Arnold Martin (édit.), *Ausländerrecht : Ausländerinnen und Ausländer im öffentlichen Recht, Privatrecht, Strafrecht, Steuerrecht und Sozialrecht der Schweiz*, 1e éd., Basel 2002.

Van Asbroeck Benoît / Debussche Julien, *Les obligations de « compliance » des entreprises*, in : Docquir Benjamin (édit.), *Vers un droit européen de la protection des données ?*, 1e éd., Bruxelles 2017 (Cité : Van Asbroeck / Debussche, *Les obligations de « compliance » des entreprises*).

Vander Elst Raymond (édit.), *Mélanges offerts à Raymond Vander Elst*, 1e éd., Bruxelles 1986.

Veruggio Gianmarco / Operto Fiorella / Bekey George, *Roboethics : Social and Ethical Implications*, in : Siciliano Bruno / Khatib Oussama (édit.), *Springer Handbook of Robotics*, Cham 2016 (Cité : Veruggio / Operto / Bekey, *Roboethics*).

Von Burg Johanna, *L'exécution fidèle : le devoir de discrétion / le secret bancaire du négociant*, in : Bizzozero Alessandro / Falleti André / Meregalli Do Duc Samantha (édit.), *Le mandat de gestion de fortune*, 2e éd., Zürich 2017 (Cité : Von Burg, *L'exécution fidèle*).

Von Hannes Bauer / Fuhr Alfred / Heynike François / Schönhagen Leonie, *Risikofeststellung Dateneigentum*, in : Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, 3e éd., Leipzig 2019 (Cité : Von Hannes, *Risikofeststellung*).

Wagner Lorin-Johannes, *Datenschutz in der EU*, 1e éd., Wien 2015 (Cité : Wagner, *Datenschutz in der EU*).

Wallach Wendell / Allen Colin, *Moral Machines : Teaching Robots Right from Wrong*, 1e éd., New York 2008 (Cité : Wallach / Allen, *Moral Machines*).

Walter Jean-Philippe, *L'effectivité des mécanismes de mise en oeuvre du point de vue du PFPDT*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015 (Cité : Walter, *L'effectivité des mécanismes*).

Weber Rolf H., *Datenschutz : zum Aufstieg einer neuen Rechtsdisziplin*, Bern 2015 (Cité : Weber, *Datenschutz*).

Weber Rolf H., *Big data und Datenschutzrecht = Big Data et droit de la protection des donées*, in : Epiney Astrid / Nüesch Daniela (édit.), *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, Zürich 2016.

Weber Rolf H. / Staiger Dominic, *Transatlantic Data Protection in Practice*, 1e éd., Zürich 2017 (Cité : Weber / Staiger, *Transatlantic Data Protection in Practice*).

Wright David / de Hert Paul (édit.), *Privacy Impact Assessment*, 6e éd., Dordrecht 2012 (Cité : Wright / de Hert, *Privacy Impact Assessment*).

Wright David / de Hert Paul (édit.), *Enforcing Privacy : Regulatory, Legal and Technological Approaches*, 1e éd., Cham 2016 (Cité : Wright / de Hert, *Enforcing Privacy*).

Wybitul Tim / Bausewein Christoph, *EU - Datenschutz - Grundverordnung : Handbuch*, 1e éd., Frankfurt am Main 2017 (Cité : Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*).

Zäch Roger (édit.), *Neue schweizerische Kartellgesetz*, 1e éd., Zürich 1996.

Articles

Agarwal Sonali / Tarbotton Lee Codel Lawson, *System and method for preventing data loss using virtual machine wrapped applications*, in : United States Patent 2017, pp. 1-15 (Cité : Agarwal / Tarbotton, *System and method for preventing data loss using virtual machine wrapped applications*).

Ailincai Mihaela, *Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel*, in : Revue de l'Union européenne 2014 2014/576, pp. 170-177.

Alavi Hamed S. / Bahrami Farzaneh / Verma Himanshu / Lalanne Denis, *Is Driverless Car Another Weiserian Mistake ?*, in : Proceedings of the 2017 ACM Conference Companion Publication on Designing Interactive Systems, New York 2017, pp. 249-253 (Cité : Alavi, *Is Driverless Car Another Weiserian Mistake ?*).

Alavi Hamed S. / Verma Himanshu / Papinutto Michael / Lalanne Denis, *Comfort : A Coordinate of User Experience in Interactive Built Environments*, in : Human-Computer Interaction – INTERACT 2017, pp. 247-257 (Cité : Alavi, *Comfort*).

Albrecht Jan Philipp, *Starker EU - Datenschutz wäre Standortvorteil : Notwendigkeit eines international einheitlichen Datenschutzstandards*, in : Datenschutz Datensich Datenschutz und Datensicherheit - DuD 2013 37/10, pp. 655-657.

Albrecht Jan Philipp, *Das neue EU-Datenschutzrecht-von der Richtlinie zur Verordnung*, in : Computer und Recht 2016 32/2, p. 88 (Cité : Albrecht, *Das neue EU-Datenschutzrecht-von der Richtlinie zur Verordnung*).

Albrecht Jan Philipp, *How the GDPR will change the world*, in : European Data Protection Law Review 2016/2, p. 287.

Anderson Timothy L., *Extraterritorial Application of National Antitrust Laws : The Need for More Uniform Regulation*, in : Wayne Law Review 1991/38, p. 1579 (Cité : Anderson, *Extraterritorial Application of National Antitrust Laws*).

Angwin Julia, *Opinion | Make Algorithms Accountable*, in : The New York Times (https ://www.nytimes.com/), New York 2018, p. « https://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html » (26/10/2018).

Angwin Julia / Larson Jeff / Mattu Surya / Kirchner Lauren, *Machine bias : There's software used across the country to predict future criminals and it's biased against blacks*, in : ProPublica (https ://www.propublica.org/), New York 2016, p. « https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing » (05/04/2020) (Cité : Angwin, *Machine bias*).

Araki Brandon / Strang John / Pohorecky Sarah / Qiu Celine / Naegeli Tobias / Rus Daniela, *Multi-robot path planning for a swarm of robots that can both fly and drive*, in : IEEE International Conference on Robotics and Automation (ICRA), Singapore 2017, pp. 5575-5582 (Cité : Araki, *Multi-robot path planning for a swarm of robots that can both fly and drive*).

Arnold Thomas / Kasenberg Daniel / Scheutz Matthias, *Value Alignment or Misalignment – What Will Keep Systems Accountable ?*, in : 3rd International Workshop on AI, Ethics, and Society 2017, p. 8.

Association for Computing Machinery, *Fathers of the Deep Learning Revolution Receive ACM A.M. Turing Award*, in : ACM (https ://acm.org/), New York 2018, p. « https://awards.acm.org/about/2018-turing » (14/12/2019) (Cité : Association for Computing Machinery, *Fathers of the Deep Learning Revolution Receive ACM A.M. Turing Award*).

ATS, *UBS visée par une action collective en Grande-Bretagne*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2019, p. « https://www.letemps.ch/economie/ubs-visee-une-action-collective-grandebretagne » (30/07/2019) (Cité : ATS, *UBS visée par une action collective en Grande-Bretagne*).

Avignon Céline, *Règlement UE protection des données et balance des intérêts*, in : Lexing - Alain Bensoussan Avocats (https ://www.alain-bensoussan.com/), Paris 2017, p. « https://www.alain-bensoussan.com/avocats/reglement-ue-protection-donnees-balance-des-interets/2016/09/14/ » (07/12/2018) (Cité : Avignon, *Règlement UE protection des données et balance des intérêts*).

Azoulai Loic / Van Der Sluis Marjin, *Institutionalizing personal data protection in times of institutional distrust : the Schrems Case*, in : Common Market Law Review 2016 53/5, pp. 1343-1371 (Cité : Azoulai / Van Der Sluis, *Institutionalizing personal data protection in times of institutional distrust*).

Baeriswyl Bruno, *Anonymisierung von genetischen Daten ? : (datenschutz)rechtliche Aspekte der Anonymisierung bei Biobanken*, in : Digma - Zeitschrift für Datenrecht und Informationssicherheit 2008/8, pp. 14-17 (Cité : Baeriswyl, *Anonymisierung von genetischen Daten ?*).

Baeriswyl Bruno, *Die Wirksamkeit der Datenschutzbehörden : Effizienz und Effektivität der Datenschutzbehörden sind Schlüsselfaktoren eines wirkungsvollen Datenschutzes*, in : Digma - Zeitschrift für Datenrecht und Informationssicherheit 2008/8, pp. 66-69.

Baeriswyl Bruno, *Die Anwendbarkeit des Datenschutzgesetzes : schweizerisches Datenschutzrecht ist auch auf den Internetdienst "Street View" anwendbar*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2009/9, pp. 98-101.

Baeriswyl Bruno, *Kleingedrucktes unter der Lupe : die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2010/10, pp. 56-59.

Bailleux Antoine, *L'histoire de la loi belge de compétence universelle– une valse à trois temps : ouverture étroitesse, modestie*, in : Droit et société : revue internationale de théorie du droit et de sociologie juridique 2005 2005/1/5, pp. 107-134.

Bamdé Aurélien, *Les sources du droit de la protection des données à caractère personnel*, in : A. Bamdé & J. Bourdoiseau (https ://aurelienbamde.com/), s.l. 2018, p. « https://aurelienbamde.com/2018/11/15/les-sources-du-droit-de-la-protection-des-donnees-a-caractere-personnel/ » (21/05/2019) (Cité : Bamdé, *Les sources du droit de la protection des données à caractère personnel*).

Bär Rolf, *Extraterritoriale Wirkung von Gesetzen*, in : Schweizerische Rechtsordnung in ihren internationalen Bezügen : Festgabe zum schweizerischen Juristentag 1988, dargeboten von der juristischen Abteilung der Rechts- und Wirtschaftswissenschaftlichen Fakultät der Universität Bern 1988, pp. 3-26 (Cité : Bär, *Extraterritoriale Wirkung von Gesetzen*).

Bär Rolf, *Das Auswirkungsprinzip im schweizerischen und europäischen Wettbewerbsrecht*, in : Neue schweizerische Wettbewerbsordnung im internationalen Umfeld, Berner Tage für die juristische Praxis 1997, pp. 87-108 (Cité : Bär, *Das Auswirkungsprinzip im schweizerischen und europäischen Wettbewerbsrecht*).

Bartlett Marian Stewart / Littlewort Gwen / Fasel Ian / Movellan Javier R., *Real Time Face Detection and Facial Expression Recognition : Development and Applications to Human Computer Interaction*, in : 2003 Conference on computer vision and pattern recognition workshop, Madison 2003/5, p. 53.

Bauchner Joshua S., *State sovereignty and the globalizing effects of the Internet : A case study of the privacy debate*, in : Brooklyn Journal of International Law 2000 26/2, pp. 689-722 (Cité : Bauchner, *State sovereignty and the globalizing effects of the Internet*).

Baudoin Claude R, *The Impact of Data Residency on Cloud Computing*, in : 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow 2018, pp. 430-435.

Beisenherz Gerhard / Tinnefeld Marie-Theres, *Aspekte der Einwilligung : Zivil- und strafrechtliche Bezüge der Einwilligung im Datenschutzrecht*, in : DuD Datenschutz und Datensicherheit - DuD 2011 35/2, pp. 110-115.

Bembaron Elsa, *Emmanuel Macron fait de la 5G un enjeu de souveraineté européenne*, in : Le Figaro (https ://www.lefigaro.fr/), Paris 2019, p. « https://www.lefigaro.fr/secteur/high-tech/emmanuel-macron-fait-de-la-5g-un-enjeu-de-souverainete-europeenne-20191107 » (06/01/2020) (Cité : Bembaron, *Emmanuel Macron fait de la 5G un enjeu de souveraineté européenne*).

Benhamou Yaniv / Braidi Guillaume / Nussbaumer Arnaud, *La restitution d'informations : quelques outils à la disposition du praticien*, in : Pratique juridique actuelle 2017/11, pp. 1302-1317 (Cité : Benhamou / Braidi / Nussbaumer, *La restitution d'informations*).

Bensoussan Alain, *Charte des droits et obligations des robots*, in : Lexing - Alain Bensoussan Avocats (https ://www.alain-bensoussan.com/), Paris 2015, p. « https://www.alain-bensoussan.com/wp-content/uploads/2014/10/Charte-droits-des-robots-Version-5.pdf » (29/09/2017) (Cité : Bensoussan, *Charte des droits et obligations des robots*).

Bensoussan Alain / Barbry Éric, *La vie privée des objets*, in : Annales des Mines - Réalités industrielles 2013 2013/2, pp. 61-65 (Cité : Bensoussan / Barbry, *La vie privée des objets*).

Bergé Jean-Sylvestre / Grumbach Stéphane, *La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires*, in : Journal du droit international 2016/4, pp. 1153-1173 (Cité : Bergé / Grumbach, *La sphère des données et le droit*).

Berset Alain, *Berset plaide pour la numérisation de la santé*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2017, p. « https://www.tdg.ch/suisse/berset-plaide-numerisation-sante/story/31505261 » (27/10/2018) (Cité : Berset, *Berset plaide pour la numérisation de la santé*).

Besse Philippe / Castets-Renard Céline / Garivier Aurélien, *Loyauté des Décisions Algorithmiques*, in : HAL Archives-Ouverts 2017, pp. 1-29 (Cité : Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*).

Beyer Marcus, *Sicherheitsrisiko facebook, Twitter & Co.*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2010 10/1, pp. 40-43 (Cité : Beyer, *Sicherheitsrisiko facebook, Twitter & Co.*).

Bittner Timo, *Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf*, in : RDV 2014, pp. 183-189 (Cité : Bittner, *Der Datenschutzbeauftragte gemäß*).

Blockchain France, *Qu'est-ce que la blockchain ?*, in : Blockchain France (https ://blockchainfrance.net/), Paris 2015, p. « https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/ » (27/10/2018) (Cité : Blockchain France, *Qu'est-ce que la blockchain ?*,).

Blonski Dominika, *Datenschutz : Kundendaten nutzen und schützen : Tagung des Europa Instituts an der Universität Zürich vom 28. Januar 2009*, in : Recht 2009/3, pp. 109-114.

Blume Peter, *Will it be a better world ? The proposed EU Data Protection Regulation*, in : International Data Privacy Law 2012 2/3, pp. 130-136 (Cité : Blume, *Will it be a better world ?*).

Blume Peter, *An alternative model for data protection law : changing the roles of controller and processor*, in : International Data Privacy Law 2015 5/4, pp. 292-297 (Cité : Blume, *An alternative model for data protection law*).

Bödi Richard, *Scoring als Methode zur Entscheidfindung*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2007 7/2, pp. 68-71 (Cité : Bödi, *Scoring als Methode zur Entscheidfindung*).

Bondallaz Stéphane, *Le « droit à une télécommunication protégée » ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques*, in : Jusletter 25 (https ://jusletter.weblaw.ch/), s.l. 2008, p. « https://jusletter.weblaw.ch/en/juslissues/2008/460/_6256.html__ONCE&login=false » (02/01/2020).

Borchert Christopher J. / Pinguelo Fernando M. / Thaw David, *Reasonable Expectations of Privacy Settings : Social Media and the Stored Communications Act*, in : Duke Law and Technology Review 2014/13, pp. 36-65 (Cité : Borchert / Pinguelo / Thaw, *Reasonable Expectations of Privacy Settings*).

Boshell Paige M., *The Power of Place : Geolocation Tracking and Privacy*, in : Business Law Today (https ://businesslawtoday.org/), Chicago 2019, p. « https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ » (19/06/2019) (Cité : Boshell, *The Power of Place*).

Bostrom Nick / Roache Rebecca, *Smart policy : Cognitive enhancement and the public interest*, in : Contemporary Readings in Law and Social Justice 2010 2/1, pp. 68-84 (Cité : Bostrom / Roache, *Smart policy*).

Botta Alessio / de Donato Walter / Persico Valerio / Pescapé Antonio, *Integration of Cloud computing and Internet of Things : A survey*, in : Future Generation Computer Systems 2016/56, pp. 684-700 (Cité : Botta, *Integration of Cloud computing and Internet of Things*).

Bounie David / Dubus Antoine / Waelbroeck Patrick, *Selling Strategic Information in Digital Competitive Markets*, in : HAL Archives-Ouverts 2018, pp. 1-51 (Cité : Bounie / Dubus / Waelbroeck, *Selling Strategic Information in Digital Competitive Markets*).

Bouri Mohamed, *Exosquelettes d'assistance à la marche : une opportunité pour les activités quotidiennes*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https://www.isdc.ch/fr/evenements/prochains-evenements/droit-robot » (21/03/2020) (Cité : Bouri, *Exosquelettes d'assistance à la marche*).

Brambilla Arianna / Alavi Hamed / Verma Himanshu / Lalanne Denis / Jusselme Thomas / Andersen Marilyne, *"Our inherent desire for control" : a case study of automation's impact on the perception of comfort*, in : Energy Procedia 2017/122, pp. 925-930 (Cité : Brambilla, *"Our inherent desire for control"*).

Bräutigam Peter / Schmidt-Wudy Florian, *Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU - Datenschutzgrundverordnung*, in : Computer und Recht 2015 31/1, pp. 56-63.

Brinon Jacques, *Avec Calico, Google veut s'attaquer à la vieillesse et à la maladie*, in : Le Monde (https ://www.lemonde.fr/), Paris 2013, p. « https://www.lemonde.fr/technologies/article/2013/09/18/avec-calico-google-veut-s-attaquer-a-la-vieillesse-et-a-la-maladie_3480153_651865.html » (28/10/2018) (Cité : Brinon, *Avec Calico, Google veut s'attaquer à la vieillesse et à la maladie*).

Brkan Maja, *Do Algorithms Rule the World ? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in : Social Science Research Network (SSRN) Scholarly Paper (https ://papers.ssrn/com/), Rochester 2017, p. « https://papers.ssrn.com/abstract=3124901 » (26/10/2018).

Brun Alain, *La directive européenne relative à la protection des données : convergences et divergences avec le droit suisse*, in : Datenschutz in der Schweiz und in Europa = La protection des données en Suisse et en Europe, Freiburg 1999, pp. 11-24 (Cité : Brun, *La directive européenne relative à la protection des données*).

Bryson Joanna / Winfield Alan, *Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems*, in : Computer 2017 50/5, pp. 116-119 (Cité : Bryson / Winfield, *Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems*).

Bühler Tiphanie, *Les coffres forts de vos données sensibles*, in : Brainserve (https ://www.brainserve.ch/), Crissier 2016, p. « https://www.brainserve.ch/brainserveweb2/wp-content/uploads/2016/01/201601-PME_Magazine-Datacenters.pdf?516c84 » (04/07/2017) (Cité : Bühler, *Les coffres forts de vos données sensibles*).

Bühlmann Lukas / Reinle Michael, *Extraterritoriale Wirkung der DSGVO : Anwendung der DSGVO der EU auf schweizerische Unternehmen : schwierige Anwendungs - und Vollstreckungsfragen*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2017/17, pp. 8-13.

Burton Cédric / Cadiot Sarah / De Boel Laura, *What's Next for U.S.-EU Data Transfers ? An Analysis of Recent Developments Following Schrems*, in : The WSGR Data Advisor (https ://www.wsgrdataadvisor.com/), s.l. 2015, p. « https://www.wsgrdataadvisor.com/2015/11/whats-next-for-u-s-eu-data-transfers-an-analysis-of-recent-developments-following-schrems/ » (26/10/2018) (Cité : Burton / Cadiot / De Boel, *What's Next for U.S.-EU Data Transfers ?*).

Burton Cédric / Cadiot Sarah / De Boel Laura, *EU Commission Publishes Proposal for e-Privacy Regulation : The Top Nine Key Points You Need to Know*, in : The WSGR Data Alert (https ://www.wsgrdataadvisor.com/), s.l. 2017, p. « https://www.wsgrdataadvisor.com/2017/01/eu-commission-publishes-proposal-for-e-privacy-regulation-the-top-nine-key-points-you-need-to-know/ » (04/03/2020) (Cité : Burton / Cadiot / De Boel, *EU Commission Publishes Proposal for e-Privacy Regulation*).

Buterin Vitalik, *A Next Generation Smart Contract & Decentralized Application Platform*, in : Etherium White Paper (https ://cryptorating.eu/), s.l. 2014, p. « https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf » (04/03/2020) (Cité :

Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*).

Buttarelli Giovanni, *The EU GDPR as a clarion call for a new global digital gold standard*, in : International Data Privacy Law 2016 6/2, pp. 77-78.

Bygrave Lee A., *European Data Protection : Determining Applicable Law Pursuant to European Data Protection Legislation*, in : Computer Law & Security Review 2000 16/4, pp. 252-257 (Cité : Bygrave, *European Data Protection*).

Callao Susana / Jarne José Ignacio, *Have IFRS affected earnings management in the European Union ?*, in : Accounting in Europe 2010 7/2, pp. 159-189 (Cité : Callao / Jarne, *Have IFRS affected earnings management in the European Union ?*).

Calo Ryan, *Open Robotics*, in : Social Science Research Network (SSRN) Scholarly Paper (https ://papers.ssrn.com/), Rochester 2010, p. « https://papers.ssrn.com/abstract=1706293 » (01/11/2018).

Calo Ryan, *Robots and Privacy*, in : Social Science Research Network (SSRN) Scholarly Paper (https ://papers.ssrn.com/), Rochester 2010, p. « https://papers.ssrn.com/abstract=1599189 » (27/10/2018) (Cité : Calo, *Robots and Privacy*).

Cassart Alexandre, *Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD*, in : Revue du Droit des Technologies de l'information 2018, pp. 41-53 (Cité : Cassart, *Premières réflexions sur le Cloud Act*).

Cavaliere Victoria / Fung Brian, *Equifax exposed 150 million Americans' personal data. Now it will pay up to $700 million*, in : CNN Business (https ://edition.cnn.com/), Atlanta 2019, p. « https://edition.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html » (22/07/2019) (Cité : Cavaliere / Fung, *Equifax exposed 150 million Americans' personal data*).

Cavoukian Ann, *Privacy by design : The 7 foundational principles. Implementation and mapping of fair information practices*, in : Information and Privacy Commissioner of Ontario 2010/5, pp. 1-11 (Cité : Cavoukian, *Privacy by design : The 7 foundational principles*).

Cavoukian Ann, *Operationalizing privacy by design : A guide to implementing strong privacy practices*, in : Information and Privacy Commissioner (https ://gpsbydesign.org/), Ontario 2012, p. « https://gpsbydesign.org/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/ » (17/01/2020) (Cité : Cavoukian, *Operationalizing privacy by design*).

Chang Victor / Ramachandran Muthu, *Towards Achieving Data Security with the Cloud Computing Adoption Framework*, in : IEEE Transactions on Services Computing 2016 9/1, pp. 138-151 (Cité : Chang / Ramachandran, *Towards Achieving Data Security with the Cloud Computing Adoption Framework*).

Chavanne Yannick, *Une nouvelle association veut promouvoir l'hébergement des données en Suisse*, in : ICT Journal (https ://www.ictjournal.ch/), Lausanne 2016, p. « https://www.ictjournal.ch/news/2016-02-15/une-nouvelle-association-veut-promouvoir-lhebergement-des-donnees-en-suisse » (21/05/2019) (Cité : Chavanne, *Une nouvelle association veut promouvoir l'hébergement des données en Suisse*).

Chavanne Yannick / Schneider Olivier, *Le cloud suisse de Google est ouvert*, in : ICT Journal (https ://www.ictjournal.ch/), Lausanne 2019, p. « https://www.ictjournal.ch/articles/2019-03-12/le-cloud-suisse-de-google-est-ouvert » (09/06/2019) (Cité : Chavanne / Schneider, *Le cloud suisse de Google est ouvert*).

Ciocchetti Corey A., *The Future of Privacy Policies : A Privacy Nutrition Label Filled with Fair Information Practices*, in : John Marshall Journal of Computer and Information Law 2008/26, pp. 1-46.

Cohen-Jonathan Gérard, *La territorialisation de la juridiction de la Cour européenne des droits de l'homme*, in : Revue trimestrielle des droits de l'homme 2002/52, pp. 1055-1082 (Cité : Cohen-Jonathan, *La territorialisation de la juridiction de la Cour européenne des droits de l'homme*).

Crawford Kate / Calo Ryan, *There is a blind spot in AI research*, in : Nature News 2016 538/7625, pp. 311-313 (Cité : Crawford / Calo, *There is a blind spot in AI research*).

Crawford Kate / Schultz Jason, *Big data and due process : Toward a framework to redress predictive privacy harms*, in : Boston College Law Review 2014/55, pp. 93-128.

Cuquet Marti / Vega-Gorgojo Guillermo / Lammerant Hans / Finn Rachel / Hassan Umair ul, *Societal impacts of big data : challenges and opportunities in Europe*, in : arXiv preprint (http ://arxiv .org/), s.l. 2017, p. « http://arxiv.org/abs/1704.03361 » (28/10/2018) (Cité : Cuquet, *Societal impacts of big data*).

DAPRA, *Six Paths to the Nonsurgical Future of Brain-Machine Interfaces*, in : Defense Advanced Research Projects Agency (https ://www.darpa.mil/), Arlington County 2019, p. « https://www.darpa.mil/news-events/2019-05-20 » (09/06/2019) (Cité : DAPRA, *Six Paths to the Nonsurgical Future of Brain-Machine Interfaces*).

Datta Amit / Tschantz Michael Carl / Datta Anupam, *Automated Experiments on Ad Privacy Settings : A Tale of Opacity, Choice, and Discrimination*, in : Proceedings on Privacy Enhancing Technologies 2015 2015/1, pp. 92-112.

Day Suzanne, *MIT art installation aims to empower a more discerning public*, in : MIT News (http ://news.mit.edu/), Boston 2019, p. « http://news.mit.edu/2019/mit-apollo-deepfake-art-installation-aims-to-empower-more-discerning-public-1125 » (31/12/2019) (Cité : Day, *MIT art installation aims to empower a more discerning public*).

Decaux Emmanuel, *Le territoire des droits de l'homme*, in : Liber amicorum Marc-André Eissen 1995, pp. 65-78 (Cité : Decaux, *Le territoire des droits de l'homme*).

Delahaye Jean-Paul, *Une épée de Damoclès sur le Bitcoin*, in : Complexités (http ://www.scilogs.fr/), s.l. 2016, p. « http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/ » (27/10/2018) (Cité : Delahaye, *Une épée de Damoclès sur le Bitcoin*).

Delmas-Marty Mireille, *International Law - Legal Theory (Lecture)*, in : UN Audiovisual Library of International Law (https ://legal.un.org/), Geneva s.a., p. « https://legal.un.org/avl/ls/Delmas-Marty_IL.html » (28/12/2019) (Cité : Delmas-Marty, *International Law*).

Demon Valérie, *Vers une norme internationale de protection de la vie privée*, in : La Croix (https ://www.la-croix.com/), Madrid 2009, p. « https://www.la-croix.com/Monde/Vers-une-norme-internationale-de-protection-de-la-vie-privee-2009-11-16-568829 » (24/03/2020) (Cité : Demon, *Vers une norme internationale de protection de la vie privée*).

Deroudille Alexis / Fatah Farid, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, in : Revue du marche commun et de l'Union Européenne 2019, pp. 442-452 (Cité : Deroudille / Fatah, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*).

DigitalEurope, *Digitaleurope's views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242)*, in : DigitalEurope (https ://www.digitaleurope.org/), Brussels 2017, p. « https : / / www . digitaleurope . org / resources / position - paper - digitaleuropes - views - on - article - 29 - working - party - draft - guidelines - on - the - right - to - data - portability - wp - 242/ » (15/12/2019) (Cité : DigitalEurope, *Digitaleurope's views on Article 29 Working Party*).

Dignum Virginia, *Responsible Autonomy*, in : Proceedings of the 26th International Joint Conference on Artificial Intelligence, Melbourne 2017, pp. 4698-4704 (Cité : Dignum, *Responsible Autonomy*).

Djonova Ivette, *La coexistence de plusieurs normes en matière de protection des données pèse sur les entreprises suisses*, in : Economiesuisse (https ://www.economiesuisse.ch/), Zürich 2019, p. « https : / / www . economiesuisse . ch / fr / articles / la - coexistence - de - plusieurs - normes - en - matiere - de - protection - des - donnees - pese - sur - les » (22/12/2019) (Cité : Djonova, *La coexistence*).

Dochow Carsten, *Gesundheitsdatenschutz gemäß der EU - Datenschutzgrundverordnung*, in : GesundheitsRecht 2016 15/7, pp. 401-409.

Dodge William S., *International Comity in American Law*, in : Columbia Law Review 2015 115/8, pp. 2071-2141 (Cité : Dodge, *International Comity in American Law*).

Dubois Camille, *Révision de la loi fédérale sur la protection des données : mettre l'accent sur la transparence et le contrôle*, in : La Vie économique (https ://dievolkswirtschaft.ch/), Berne 2015, p. « https : / / dievolkswirtschaft . ch / fr / 2015 / 10 / dubois - 11 - 2015 - franz/ » (01/11/2018).

Editorial Board, *US Department of Justice must make antitrust fit for the age of Big Tech*, in : Financial Times (https ://www.ft.com/), London 2019, p. « https://www.ft.com/content/fca13e16-ae32-11e9-8030-530adfa879c2 » (06/08/2019) (Cité : Editorial Board, *US Department of Justice must make antitrust fit for the age of Big Tech*).

Edwards Lilian / Finck Michèle / Veale Michael / Zingales Nicolo, *Data subjects as data controllers : a Fashion (able) concept ?*, in : Internet Policy Review (https ://policyreview.info/), Berlin 2019, p. « https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400 » (12/12/2019) (Cité : Edwards, *Data subjects as data controllers*).

Edwards Lilian / Veale Michael, *Enslaving the Algorithm : From a "Right to an Explanation" to a "Right to Better Decisions"?*, in : IEEE Security & Privacy 2018 16/3, pp. 46-54.

Ehlermann Claus-Dieter, *Ein Plädoyer für die dezentrale Kontrolle der Anwendung des Gemeinschaftsrechts durch die Mitgliedstaaten*, in : Du droit international au droit de l'intégration 1987, pp. 205-226.

Ehmann Eugen, *Der weitere Weg zur Datenschutzgrundverordnung– Näher am Erfolg, als viele glauben*, in : ZD 2015, pp. 6-12 (Cité : Ehmann, *Der weitere Weg zur Datenschutzgrundverordnung*).

Epiney Astrid, *Datenschutz und Bilaterale II : zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht : ausgewählte Aspekte*, in : Schweizerische Juristen-Zeitung 2006, pp. 121-129.

Epiney Astrid, *Besonders schützenswerte Personendaten : zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage*, in : Mélanges en l'honneur de Paul-Henri Steinauer 2013, pp. 97-111 (Cité : Epiney, *Besonders schützenswerte Personendaten*).

Etzioni Amitai / Etzioni Oren, *Designing AI Systems That Obey Our Laws and Values*, in : Communications of the ACM 2016 59/9, pp. 29-31 (Cité : Etzioni / Etzioni, *Designing AI Systems That Obey Our Laws and Values*).

European Digital Rights, *US lobbying against draft Data Protection Regulation*, in : EDRi (http ://www.edri.org/), Brussels 2011, p. « https://edri.org/US-DPR/ » (12/04/2019) (Cité : European Digital Rights, *US lobbying against draft Data Protection Regulation*).

Fagnant Daniel J. / Kockelman Kara, *Preparing a nation for autonomous vehicles : opportunities, barriers and policy recommendations*, in : Transportation Research Part A : Policy and Practice 2015/77, pp. 167-181 (Cité : Fagnant / Kockelman, *Preparing a nation for autonomous vehicles*).

Fallon Marc, *Les frontières spatiales du droit privé européen selon le droit de l'Union européenne*, in : Frontières du droit privé européen 2012, pp. 65-123 (Cité : Fallon, *Les frontières spatiales du droit privé européen selon le droit de l'Union européenne*).

Fanti Sébastien, *Le nouveau règlement général sur la protection des données et la Suisse : le noeud gordien de la double régulation et le fragile substrat législatif*, in : Expert Focus : schweizerische Zeitschrift für Wirtschaftsprüfung, Steuern, Rechnungswesen und Wirtschaftsberatung = revue suisse pour l'audit, la fiscalité, la comptabilité et le conseil économique 2017, pp. 856-862 (Cité : Fanti, *Le nouveau règlement général sur la protection des données et la Suisse*).

Fanti Sébastien, *Le Réseau Lexing offre d'être votre représentant au sein de l'UE conformément au RGPD !*, in : Lexing Switzerland (https ://lexing.ch/), Sion 2019, p. « https://lexing.ch/le-reseau-lexing-vous-offre-de-vous-representer-au-sein-de-lue-dans-le-cadre-du-rgpd/ » (30/06/2019) (Cité : Fanti, *Le Réseau Lexing*).

Fasnacht Tobias, *Die Revision der Datenschutzkonvention des Europarates : Implikationen für die Schweiz*, in : Schweizerisches Jahrbuch für Europarecht = Annuaire suisse de droit européen 2011, pp. 329-353 (Cité : Fasnacht, *Die Revision der Datenschutzkonvention des Europarates*).

Favre Cléa, *Comment les employés d'Amazon peuvent être virés par un robot*, in : RTS (https ://www.rts.ch/), Genève 2019, p. « https://www.rts.ch/info/economie/10403387-comment-les-employes-d-amazon-peuvent-etre-vires-par-un-robot.html » (07/06/2019) (Cité : Favre, *Comment les employés d'Amazon peuvent être virés par un robot*).

Fawaz Kassem / Linden Thomas / Harkous Hamza, *The Applications of Machine Learning in Privacy Notice and Choice*, in : 11th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru 2019, pp. 118-124.

Fellmann Walter, *Substanziierungspflicht nach der schweizerischen Zivilprozessordnung*, in : Haftpflichtprozess, Zürich 2011, pp. 13-35 (Cité : Fellmann, *Substanziierungspflicht*).

Felten Ed, *What does it mean to ask for an "explainable" algorithm ?*, in : Freedom To Tinker (https ://freedom-to-tinker.com/), s.l. 2017, p. « https://freedom-to-tinker.com/2017/05/31/what-does-it-mean-to-ask-for-an-explainable-algorithm/ » (28/10/2018)

(Cité : Felten, *What does it mean to ask for an "explainable" algorithm ?*).

Feng Shuo / Setoodeh Peyman / Haykin Simon, *Smart Home : Cognitive Interactive People-Centric Internet of Things*, in : IEEE Communications Magazine 2017 55/2, pp. 34-39.

Ferrandon Benoît, *Les leçons de l'affaire Enron*, in : Les cahiers français 2002/309, p. 69 (Cité : Ferrandon, *Les leçons de l'affaire Enron*).

Ferretti Agata / Schneider Manuel / Blasimme Alessandro, *Machine Learning in Medicine : Opening the New Data Protection Black Box*, in : European Data Protection Law Review 2018/4, pp. 320-332 (Cité : Ferretti / Schneider / Blasimme, *Machine Learning in Medicine*).

Finck Michèle, *Blockchains and Data Protection in the EU*, in : European Data Protection Law Review 2018/4, pp. 17-35 (Cité : Finck, *Blockchains and Data Protection in the EU*).

FINMA, *FINMA is investigating ICO procedures*, in : FINMA (https ://www.finma.ch/), Bern 2017, p. « https://www.finma.ch/en/news/2017/09/20170929-mm-ico/ » (10/10/2017) (Cité : FINMA, *FINMA is investigating ICO procedures*).

FINMA, *Autorisation Fintech : la FINMA publie un guide pratique*, in : FINMA (https ://www.finma.ch/), Bern 2018, p. « https://www.finma.ch/fr/news/2018/12/20181203-aktuell-fintech-bewilligung/ » (26/07/2019) (Cité : FINMA, *Autorisation Fintech*).

Floridi Luciano, *Tolerant paternalism : Pro-ethical design as a resolution of the dilemma of toleration*, in : Science and engineering ethics 2016 22/6, pp. 1669-1688 (Cité : Floridi, *Tolerant paternalism*).

Fontanel Jacques / Sushcheva Natalia, *La puissance des GAFAM : Réalités, apports et dangers*, in : Annuaire français de relations internationales : La Documentation française 2019, pp. 1-26 (Cité : Fontanel / Sushcheva, *La puissance des GAFAM*).

Forstmoser Peter, *10 Jahre Gesetz - 30 Jahre Diskussion : von den Anfängen des Datenschutzes in der Schweiz*, in : Digma - Zeitschrift für Datenrecht und Informationssicherheit 2003/32003, pp. 50-55.

Fraga Alberto Iglesias, *This Swedish startup is 3D printing human organs*, in : WEF (https ://www.weforum.org/), Cologny 2018, p. « https://www.weforum.org/agenda/2018/10/this-3d-printer-could-one-day-make-new-body-parts-for-transplant-patients/ » (05/07/2019) (Cité : Fraga, *This Swedish startup is 3D printing human organs*).

Frey Carl Benedikt / Osborne Michael A., *The future of employment : How susceptible are jobs to computerisation ?*, in : Technological forecasting and social change 2017/114, pp. 254-280 (Cité : Frey / Osborne, *The future of employment*).

Frison-Roche Marie-Anne, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, in : MAFR (https ://mafr.fr/), Paris 2019, p. « https://mafr.fr/fr/article/lapport-du-droit-de-la-compliance-dans-la-gouverna/ » (07/03/2020) (Cité : Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*).

Fuhrer Stephan, *Anmerkungen zu privatversicherungsrechtlichen Entscheidungen des Bundesgerichts*, in : HAVE : Haftung und Versicherung = REAS : responsabilité et assurance 2013, pp. 140-148, pp. 252-256, pp. 329-335 (Cité : Fuhrer, *Anmerkungen zu privatversicherungsrechtlichen Entscheidungen des Bundesgerichts*).

Fung Brian, *Republicans voted to roll back landmark FCC privacy rules. Here's what you need to know*, in : The Washington Post (https ://www.washingtonpost.com/), Washington D.C. 2017, p. « https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/ » (27/10/2018) (Cité : Fung, *Republicans voted to roll back landmark FCC privacy rules*).

Future of Life Institute, *Autonomous Weapons : An Open Letter from AI and Robotics Researchers*, in : Future of Life Institute (https ://futureoflife.org/), Allston 2015, p. « https://futureoflife.org/open-letter-autonomous-weapons/ » (29/09/2017) (Cité : Future of Life Institute, *Autonomous Weapons*).

Future of Privacy Forum, *FPF and NADA Launch Guide to Consumer Privacy in the Connected Car*, in : FPF (https ://fpf.org/) Washington D.C. 2017, p. « https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-

car/ » (22/06/2017) (Cité : Future of Privacy Forum, *FPF and NADA Launch Guide to Consumer Privacy in the Connected Car*).

Future of Privacy Forum, *Shedding Light on Smart City Privacy*, in : FPF (https ://fpf.org/) Washington D.C. 2017, p. « https://fpf.org/2017/03/30/smart-cities » (25/06/2017) (Cité : Future of Privacy Forum, *Shedding Light on Smart City Privacy*).

Galdon-Clavell Gemma, *(Not so) smart cities ? : The drivers, impact and risks of surveillance-enabled smart environments*, in : Science and Public Policy 2013 40/6, pp. 717-723.

Gardyan-Eisenlohr Eva / Knöpfle Kornel, *Accountability für Datenschutz in einem globalen Unternehmen : Fundament einer nachhaltigen Implementierung*, in : Datenschutz Datensich Datenschutz und Datensicherheit - DuD 2017 41/2, pp. 69-73.

Garessus Emmanuel, *Les robots obtiendront leur propre statut juridique*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/economie/robots-obtiendront-propre-statut-juridique » (27/10/2018) (Cité : Garessus, *Les robots obtiendront leur propre statut juridique*).

Garreau Marion, *2017, année record de ventes de robots industriels dans le monde*, in : L'Usine Nouvelle (https ://www.usinenouvelle.com/), Antony 2018, p. « https://www.usinenouvelle.com/article/2017-annee-record-de-ventes-de-robots-industriels-dans-le-monde.N757124 » (22/03/2020) (Cité : Garreau, *2017, année record de ventes de robots industriels dans le monde*).

Gasiorowski-Denis Elizabeth, *Adopter le nuage en toute confiance*, in : ISO News (https ://www.iso.org/), Genève 2015, p. « https://www.iso.org/fr/news/2015/01/Ref1921.html » (17/01/2020) (Cité : Gasiorowski-Denis, *Adopter le nuage en toute confiance*).

Gasser Urs, *Perspectives on the future of digital privacy*, in : Zeitschrift für schweizerisches Recht = Revue de droit suisse = Rivista di diritto svizzero 2015, pp. 335-448.

Gath-Morad Michal / Schaumann Davide / Zinger Einat / Plaut Pnina O. / Kalay Yehuda E., *How Smart is the Smart City ? Assessing the Impact of ICT on Cities*, in : Agent Based Modelling of Urban Systems 2017, pp. 189-207.

Gayrel Claire, *L'expansion des standards européens de protection des données dans le monde*, in : L'Europe des droits de l'homme à l'heure d'internet Bruxelles 2019, pp. 473-488 (Cité : Gayrel, *L'expansion*).

Geoffray Sylvain, *HP publie un rapport alarmant sur la sécurité des objets connectés*, in : Aruco (https ://aruco.com/), s.l. 2014, p. « https://aruco.com/2014/07/hp-fortify-securite/ » (27/10/2018) (Cité : Geoffray, *HP publie un rapport alarmant sur la sécurité des objets connectés*).

Gibney Elizabeth, *What google's winning go algorithm will do next*, in : Nature News 2016 531/7594, pp. 284-285 (Cité : Gibney, *What google's winning go algorithm will do next*).

Gidari Albert, *What will Microsoft and Ireland do with the new Cloud Act warrant ?*, in : Center of Internet and Society - Stanford Law School (http://cyberlaw.stanford.edu/), Stanford 2018, p. « http://cyberlaw.stanford.edu/blog/2018/04/what-will-microsoft-and-ireland-do-new-cloud-act-warrant » (04/01/2020) (Cité : Gidari, *What will Microsoft and Ireland do with the new Cloud Act warrant ?*).

Goddard Michelle, *The EU General Data Protection Regulation : European regulation that has a global impact*, in : International Journal of Market Research 2017 59/6, pp. 703-705.

Gola Peter / Schulz Sebastian, *DS-GVO–Neue Vorgaben für den Datenschutz bei Kindern*, in : Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD 2013, pp. 475-481 (Cité : Gola / Schulz, *DS-GVO*).

Goldberg John CP, *Twentieth-Century Tort Theory*, in : Georgetown Law Journal 2002/91, pp. 513-560 (Cité : Goldberg, *20^{th} Century Tort Theory*).

Goldsmith Jack L., *Against cyberanarchy*, in : The University of Chicago Law Review 1998 65/4, pp. 1199-1250 (Cité : Goldsmith, *Against cyberanarchy*).

Goodman Bryce W., *A Step Towards Accountable Algorithms ? : Algorithmic Discrimination and the European Union General Data Protection*, in : 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona 2016, pp. 1-9 (Cité : Goodman, *A Step Towards Accountable Algorithms ?*).

Goodman Bryce / Flaxman Seth, *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"*, in : AI magazine 2017 38/3, pp. 50-57 (Cité : Goodman / Flaxman, *Right to Explanation*).

Google, *Recherches supprimées dans le cadre de la législation européenne sur la confidentialité des données*, in : Transparence des informations (https ://transparencyreport.google.com/), s.l. s.a., p. « https://transparencyreport.google.com/eu-privacy/overview?hl=fr » (27/10/2018) (Cité : Google, *Recherches supprimées dans le cadre de la législation européenne sur la confidentialité des données*).

von Grafenstein Maximilian, *Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO*, in : Datenschutz Datensich Datenschutz und Datensicherheit - DuD 2015 39/12, pp. 789-795.

Granville Kevin, *Facebook and Cambridge Analytica : What You Need to Know as Fallout Widens*, in : The New York Times (https ://www.nytimes.com/), New York 2018, p. « https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html » (28/07/2019) (Cité : Granville, *Facebook and Cambridge Analytica*).

Grésillon Gabriel / Perrotte Derek / Barré Nicolas, *Thierry Breton : « Pour accéder au marché européen, il faudra accepter nos règles »*, in : Les Echos (https ://www.lesechos.fr/), Paris 2020, p. « https://www.lesechos.fr/monde/europe/thierry-breton-pour-acceder-au-marche-europeen-il-faudra-accepter-nos-regles-1161004 » (08/01/2020) (Cité : Grésillon / Perrotte / Barré, *« Pour accéder au marché européen, il faudra accepter nos règles »*).

Grigorian Christopher H. / Englund Nicholas / Haake Jack G., *Self Drive Act Passes the House as Senate Prepares Its Own Bill*, in : The National Law Review (https ://www.natlawreview.com/), Chicago 2017, p. « https://www.natlawreview.com/article/self-drive-act-passes-house-senate-prepares-its-own-bill » (27/10/2018) (Cité : Grigorian / Englund / Haake, *Self Drive Act*).

Guizzo Erico, *How google's self-driving car works*, in : IEEE Spectrum Online 2011 18/7, pp. 1132-1141 (Cité : Guizzo, *How google's self-driving car works*).

Gunning David, *Explainable Artificial Intelligence (XAI)*, in : Defense Advanced Research Projects Agency (DARPA) and Web (https ://www.darpa.mil/), s.l. 2017, p. « https://www.darpa.mil/attachments/XAIProgramUpdate.pdf » (17/01/2020) (Cité : Gunning, *Explainable Artificial Intelligence*).

Hajian Sara / Bonchi Francesco / Castillo Carlos, *Algorithmic Bias : From Discrimination Discovery to Fairness-aware Data Mining*, in : Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York 2016, pp. 2125-2126.

HALO Attorneys, *Self Driving Cars - More Questions Than Answers*, in : HALO Attorneys (https ://www.halo-attorneys.com/), Las Vegas 2020, p. « https : / / www . halo - attorneys . com / self - driving - cars/new - rules - of - the - road.html » (21/03/2020) (Cité : HALO Attorneys, *Self Driving Cars*).

Hamet Pavel / Tremblay Johanne, *Artificial intelligence in medicine*, in : Metabolism 2017/69, pp. 36-40.

Hashem Ibrahim Abaker Targio / Yaqoob Ibrar / Anuar Nor Badrul / Mokhtar Salimah / Gani Abdullah / Ullah Khan Samee, *The rise of "big data" on cloud computing : Review and open research issues*, in : Information Systems 2015/47, pp. 98-115 (Cité : Hashem, *The rise of "big data" on cloud computing*).

van Hecke Georges, *Le droit anti-trust : aspects comparatifs et internationaux*, in : Recueil des Cours / Collected Courses Leiden 1962/106 (Cité : van Hecke, *Le droit anti-trust*).

Helbing Dirk / Pournaras Evangelos, *Society : Build digital democracy*, in : Nature News 2015 527/7576, pp. 33-34 (Cité : Helbing / Pournaras, *Society*).

Hickey Matt, *Open Source Project Could Replace Traditional Passports With Bitcoin Tech*, in : Forbes (https ://www.forbes.com/), New Jersey 2014, p. « https://www.forbes.com/sites/matthickey/2014 / 10 / 31 / open - source - project - could - replace - traditional - passports-with-bitcoin-tech/ » (27/10/2018) (Cité : Hickey, *Open Source Project Could Replace Traditional Passports With Bitcoin Tech*).

Hirsch Célian, *L'accès aux données d'une procédure au regard de la LPD : une tentative abusive de Pre-Trial Discovery ?*, in : Jusletter 2018/17 (Cité : Hirsch, *L'accès aux données d'une procédure au regard de la LPD*).

Hoffman Robert R. / Klein Gary / Mueller Shane T., *Explaining Explanation For "Explainable Ai"*, in : Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2018 62/1, pp. 197-201.

Hofmann-Hafner Susanne / Borboën Yan / Colonna Vincent, *Fondamentaux du règlement général sur la protection des données et comment PwC peut vous aider*, in : PwC (https ://news.pwc.ch/), Geneva 2018, p. « https://news.pwc.ch/wp-content/uploads/2016/08/Fondamentaux-du-reglement-general_FR.pdf » (26/10/2018) (Cité : Hofmann-Hafner / Borboën / Colonna, *Fondamentaux du règlement général sur la protection des données*).

Hofmann Susanne / Meyer Michael Adrian, *Que signifie la révision pour les entreprises ?*, in : La Vie économique 2016/11, pp. 59-61 (Cité : Hofmann / Meyer, *Que signifie la révision pour les entreprises ?*).

Hornung Gerrit / Sädler Stephan, *Europas Wolken — Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing*, in : Computer Und Recht : Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation 2012 28/10, pp. 638-645 (Cité : Hornung / Sädler, *Europas Wolken — Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing*,).

Hossain A. K. M. M. / Soh W. S., *A Comprehensive Study of Bluetooth Signal Parameters for Localization*, in : IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications 2007, pp. 1-5.

Husi-Stämpfli Sandra, *Die DSG-Revision oder : Ein Beziehungsdrama in drei Akten - Gedanken zur komplexen Revision des Datenschutzrechts in der Schweiz*, in : Jusletter 2018/7, pp. 1-11 (Cité : Husi-Stämpfli, *Die DSG-Revision oder*).

ICO, *Intention to fine British Airways £183.39m under GDPR for data breach*, in : ICO (https ://ico.org.uk/), Wilmslow 2019, p. « https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ » (23/06/2017) (Cité : ICO, *Intention to fine British Airways £183.39m under GDPR for data breach*).

IEEE, *IEEE Position Statement : Ethical Aspects of Autonomous and Intelligent Systems*, in : IEEE (https ://www.ieee.org), New Jersey 2019, p. « https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE19002.pdf » (05/07/2019) (Cité : IEEE, *Ethical Aspects of Autonomous and Intelligent Systems*).

Ijspeert Auke, *De la biologie à la robotique et de la robotique à la biologie*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https : / / www . isdc . ch / fr / evenements / prochains - evenements / droit - robot » (21/03/2020) (Cité : Ijspeert, *De la biologie à la robotique et de la robotique à la biologie*).

Institut Suisse de Droit Comparé, *Quand le droit rencontre les robots*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https : / / www . isdc . ch / fr / evenements / prochains - evenements / droit - robot » (21/03/2020) (Cité : Institut Suisse de Droit Comparé, *Quand le droit rencontre les robots*).

Ion Iulia / Sachdeva Niharika / Kumaraguru Ponnurangam / Čapkun Srdjan, *Home is safer than the cloud ! : privacy concerns for consumer cloud storage*, in : Proceedings of the Seventh Symposium on Usable Privacy and Security 2011, pp. 1-13 (Cité : Ion, *Home is safer than the cloud !*).

ISO, *Norme ISO 8373*, in : ISO (https ://www.iso.org/), Genève 2012, p. « https://www.iso.org/obp/ui//#iso:std:iso:8373:ed-2:v1:fr » (22/03/2020) (Cité : ISO, *Norme ISO 8373*).

ISO, *ISO/TC 307 - Blockchain and distributed ledger technologies*, in : ISO (https ://www.iso.org/), Sydney 2016, p. « https://www.iso.org/committee/6266604.html » (27/10/2017) (Cité : ISO, *Blockchain and distributed ledger technologies*).

ISO, *À Propos de L'ISO*, in : ISO (https ://www.iso.org/), Genève s.a., p. « https://www.iso.org/fr/about-us.html » (18/04/2017) (Cité : ISO, *À Propos de L'ISO*).

Jacobs Angelika, *Data-storage for eternity*, in : ETH (https ://ethz.ch/), Zürich 2015, p. « https : / / ethz . ch / en / news - and - events / eth - news / news / 2015 / 02 / data - storage - for - eternity . html » (02/05/2017) (Cité : Jacobs, *Data-storage for eternity*).

Jacobs Reto, *Zivilrechtliche Durchsetzung des Wettbewerbsrechts*, in : Das revidierte Kartellgesetz in der Praxis 2006, pp. 209-225 (Cité : Jacobs, *Zivilrechtliche Durchsetzung des Wettbewerbsrechts*).

Jaggi Martin, *Fundamentals of AI*, in : AI Governance Forum (https ://ai-gf.com/), Geneva 2019, p. « https://ai-gf.com/ » (21/03/2020) (Cité : Jaggi, *Fundamentals of AI*).

Jarvis Ray, *Intelligent Robotics : Past, Present and Future*, in : International Journal of Computer Science and Applications 2008 5/3, pp. 23-35 (Cité : Jarvis, *Intelligent Robotics*).

Jault-Seseke Fabienne, *La portée extraterritoriale ou a-territoriale du RGPD*, in : Revue des affaires europeennes 2018/1, pp. 43-51 (Cité : Jault-Seseke, *La portée extraterritoriale ou a-territoriale du RGPD*).

Jault-Seseke Fabienne / Zolynski Célia, *Le règlement 2016/679/UE relatif aux données personnelles*, in : Recueil Dalloz 2016/32, pp. 1874-1880 (Cité : Jault-Seseke / Zolynski, *Le règlement 2016 / 679 / UE*).

Jennings Robert Y., *Extraterritorial Jurisdiction and the United States Antitrust Laws*, in : British Yearbook of International Law 1957/ 33, p. 146 (Cité : Jennings, *Extraterritorial Jurisdiction*).

Johnson David R. / Post David, *Law and Borders–The Rise of Law in Cyberspace*, in : Stanford Law Review 1995/48, pp. 1367-1402 (Cité : Johnson / Post, *Law and Borders*).

Kaminski Margot E., *Binary Governance : Lessons from the GDPR's Approach to Algorithmic Accountability*, in : Southern California Law Review 2019 92/6, pp. 1529-1616 (Cité : Kaminski, *Binary Governance*).

Katal Avita / Wazid Mohammad / Goudar R. H., *Big data : Issues, challenges, tools and Good practices*, in : Sixth International Conference on Contemporary Computing (IC3), Noida 2013, pp. 404-409 (Cité : Katal / Wazid / Goudar, *Big data*).

Katsikas Sokratis K., *Cyber Security of the Autonomous Ship*, in : Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, New York 2017, pp. 55-56 (Cité : Katsikas, *Cyber Security of the Autonomous Ship*).

Kattan Ilana R., *Cloudy privacy protections : why the Stored Communications Act fails to protect the privacy of communications stored in the cloud*, in : Vanderbilt Journal of Entertainment and Technology Law 2010 13/3, pp. 617-656 (Cité : Kattan, *Cloudy privacy protections*).

Kern Markus, *Datenschutzrevision in der EU : Neuer Wein ? Neue Schläuche ?*, in : Digma-Zeitschrift für Datenrecht und Informationssicherheit 2013 13/1, pp. 30-33 (Cité : Kern, *Datenschutzrevision in der EU*).

Kesan Jay P. / Hayes Carol M. / Bashir Masooda N., *Information privacy and data control in cloud computing : Consumers, privacy preferences, and market efficiency*, in : Washington and Lee Law Review 2013 70/1, pp. 341-472 (Cité : Kesan / Hayes / Bashir, *Information privacy and data control in cloud computing*).

Khan M. Imran / Mansoor A Bin, *Real time eyes tracking and classification for driver fatigue detection*, in : International Conference on Image Analysis and Recognition 2008, pp. 729-738.

Khushf George, *The Ethics of NBIC Convergence*, in : Journal of Medicine and Philosophy 2007 32/3, pp. 185-196.

Kipker Dennis-Kenji / Voskamp Friederike, *Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung*, in : Datenschutz Datensich Datenschutz und Datensicherheit - DuD 2012 36/10, pp. 737-742.

Kroschwald Steffen, *Kollektive Verantwortung für den Datenschutz in der Cloud–Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing*, in : Zeitschrift für Datenschutz 2013/3, pp. 388-394 (Cité : Kroschwald, *Kollektive Verantwortung für den Datenschutz in der Cloud*).

Kulesza Joanna / Balleste Roy, *Signs and Portents in Cyberspace : The Rise of Jus Internet as a New Order in International Law*, in : Fordham Intellectual Property Media and Entertainment Law Journal 2012/23, pp. 1333-1346 (Cité : Kulesza / Balleste, *Signs and Portents in Cyberspace*).

Lacour Stéphanie, *Du secret médical aux dossiers de santé électroniques. Réflexions juridiques sur la protection des données de santé*, in : Médecine & Droit 2016/138, pp. 62-69.

Landes-Gronowski Laure, *Le Règlement Général sur la Protection des Données (RGPD) en 10 leçons : L'essentiel du RGPD dans un guide pratique*, in : Avistem Avocats (http ://www.avistem.com/), Paris 2017, p. « http://www.avistem.com/sites/default/files/2017%5C%2001%5C%2010%5C%20Le%5C%20RGPD%5C%20en%5C%2010%5C%20le%5C%C3%5C%A7ons%5C%20V.1_0.pdf » (05/12/2018) (Cité : Landes-Gronowski, *Le RGPD en 10 leçons*).

Langley Pat / Meadows Ben / Sridharan Mohan / Choi Dongkyu, *Explainable Agency for Intelligent Autonomous Systems*, in : 29th Conference on Innovative Applications of Artificial Intelligence, San Francisco 2017, pp. 4762-4764 (Cité : Langley, *Explainable Agency*).

Larousserie David, *Le dilemme macabre des voitures autonomes*, in : Le Monde (https ://www.lemonde.fr/), Paris 2016, p. « https://www.lemonde.fr/sciences/article/2016/06/23/tuer-un-pieton-ou-sacrifier-le-passager-le-dilemme-macabre-des-voitures-autonomes_4956924_1650684.html » (27/10/2018) (Cité : Larousserie, *Le dilemme macabre des voitures autonomes*).

Léchenet Alexandre, *Business, éthique, légalité... Le séquençage du génome en questions*, in : Le Monde (https ://www.lemonde.fr/), Paris 2014, p. « https://www.lemonde.fr/les-decodeurs/article/2014/08/18/le-sequencage-du-genome-comment-ca-marche_4472313_4355770.html » (27/10/2018) (Cité : Léchenet, *Business, éthique, légalité*).

Lecrip, *E-santé et génétique : quand les Gafa s'emparent de notre ADN*, in : CRIP (https ://lecrip.org/), Nanterre 2016, p. « https://lecrip.org/2016/01/25/e-sante-genetique-gafa-semparent-de-adn/ » (27/10/2018) (Cité : Lecrip, *E-santé et génétique*).

Ledger Insights, *China's Shenzhen district uses blockchain for $1 billion of tax invoices*, in : Ledger Insights (https ://www.ledgerinsights.com/), Limassol 2019, p. « https://www.ledgerinsights.com/china-shenzhen-blockchain-tax-invoices/ » (15/12/2019) (Cité : Ledger Insights, *China's Shenzhen district uses blockchain for $1 billion of tax invoices*).

Leese Matthias, *The new profiling : Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, in : Security Dialogue 2014 45/5, pp. 494-511.

Lehmann Matthias, *Legal fragmentation, extraterritoriality and uncertainty in global financial regulation*, in : Oxford Journal of Legal Studies 2017 37/2, pp. 406-434 (Cité : Lehmann, *Legal fragmentation, extraterritoriality and uncertainty in global financial regulation*).

Lesaulnier Frédérique, *Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données*, in : Médecine & Droit 2018, pp. 103-111.

Lessig Lawrence, *The law of the horse : What cyber law might teach*, in : Harvard Law Review 1999/113, pp. 501-546 (Cité : Lessig, *The law of the horse*).

Liu Richard, *How e-commerce giant JD.com uses drones to deliver to far-out areas in China*, in : CNBC (https ://www.cnbc.com/), New Jersey 2017, p. « https://www.cnbc.com/video/2017/06/18/how-e-commerce-giant-jd-com-uses-drones-to-deliver-to-far-out-areas-in-china.html » (27/10/2018) (Cité : Liu, *How e-commerce giant JD.com uses drones to deliver to far-out areas in China*,).

Logean Sylvie, *Joël de Rosnay : « L'avenir de l'Humanité réside dans l'intelligence collective augmentée »*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https : / / www . letemps . ch / sciences / joel - rosnay - lavenir - lhumanite - reside - lintelligence - collective - augmentee » (18/04/2017) (Cité : Logean, *« L'avenir de l'Humanité réside dans l'intelligence collective augmentée »*).

Lombarte Artemi Rallo / Stoddart Jennifer / Vladeck David C. / Türk Alex / Wada Ricardo Morishita / Walter Jean-Philippe / Ouattara Alimata / Shroff Marie / Vassilyeva Larissa B., *Vers une régulation globale du droit à la vie privée : propositions et stratégies*, in : 31ème conférence internationale des commissaires à la protection des données et à la vie privée, Madrid 2009 (Cité : Lombarte, *Vers une régulation globale du droit à la vie privée*).

Loubière Paul, *Vos données personnelles sur internet peuvent valoir de l'or*, in : Challenges (https ://www.challenges.fr/), Paris 2014, p. « https://www.challenges.fr/high-tech/vos-donnees-personnelles-sur-internet-peuvent-valoir-de-l-or_57690 » (27/10/2018) (Cité : Loubière, *Vos données personnelles sur internet peuvent valoir de l'or*).

Loukil Ridha, *Alibaba va étendre son cloud mondial avec quatre nouveaux datacenters d'ici 2018*, in : L'Usine Digitale (https ://www.usine-digitale.fr/), Antony 2017, p. « https://www.usine-digitale.fr/article/alibaba-va-etendre-son-cloud-mondial-avec-quatre-nouveaux-datacenters-d-ici-2018.N594138 » (01/04/2019) (Cité : Loukil, *Alibaba*).

Magnon Xavier, *La loyauté dans le droit institutionnel de l'Union européenne*, in : Revue des affaires europeennes 2011/2, pp. 245-251.

Maguire Michael, *2016 GPEN Privacy Sweep, Internet of Things : Participating Authorities' Press Releases*, in : Global Privacy Enforcement Network (https ://www.privacyenforcement.net/), s.l. 2016, p. « https://www.privacyenforcement.net/node/717 » (27/10/2018) (Cité : Maguire, *2016 GPEN Privacy Sweep, Internet of Things*).

Mantelero Alessandro, *Personal data for decisional purposes in the age of analytics : From an individual to a collective dimension of data protection*, in : Computer law & security review 2016 32/2, pp. 238-255.

Maras Marie-Helen / Wandt Adam Scott, *Enabling mass surveillance : data aggregation in the age of big data and the Internet of Things*, in : Journal of Cyber Policy 2019, pp. 1-18 (Cité : Maras / Wandt, *Enabling mass surveillance*).

Martin Claire / Galliker Dominik, *La Suisse : un coffre-fort numérique*, in : Swisscom Magazine (https ://magazine.swisscom.ch/), Berne 2017, p. « https://magazine.swisscom.ch/securite-des-donnees-infrastructure/la-suisse-un-coffre-fort-numerique/ » (04/12/2018) (Cité : Martin / Galliker, *La Suisse*).

Martin Eladio / Vinyals Oriol / Friedland Gerald / Bajcsy Ruzena, *Precise Indoor Localization Using Smart Phones*, in : Proceedings of the 18th ACM International Conference on Multimedia, New York 2010, pp. 787-790.

Martin Kelly D. / Borah Abhishek / Palmatier Robert W., *Data Privacy : Effects on Customer and Firm Performance*, in : Journal of Marketing 2017 81/1, pp. 36-58.

Martin Paul / Ho Bo-Jhang / Grupen Nicholas / Muñoz Samuel / Srivastava Mani, *An iBeacon Primer for Indoor Localization*, in : Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings, New York 2014, pp. 190-191.

Maupin Julie, *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All*, in : G20 Insights (https ://www.g20 - insights.org/), Berlin 2018, p. « https://www.g20-insights.org/policy_briefs/g20-countries-engage-blockchain-technologies-build-inclusive-transparent-accountable-digital-economy/ » (27/10/2018) (Cité : Maupin, *The G20 Countries Should Engage*).

McCabe David / Alba Davey, *Facebook Says It Will Ban 'Deepfakes'*, in : The New York Times (https ://www.nytimes.com/), New York 2020, p. « https://www.nytimes.com/2020/01/07/technology/facebook-says-it-will-ban-deepfakes.html » (07/01/2020) (Cité : McCabe / Alba, *Facebook Says It Will Ban 'Deepfakes'*).

McFarland Matt, *Amazon's delivery drones may drop packages via parachute*, in : CNN Business (https ://money.cnn.com/), Washington D.C. 2017, p. « https : / / money . cnn . com / 2017 / 02 / 14 / technology / amazon - drone - patent / index . html » (27/10/2018) (Cité : McFarland, *Amazon's delivery drones may drop packages via parachute*).

McLachlan Campbell, *From Savigny to Cyberspace : Does the Internet Sound the Death-Knell for the Conflict of Laws ?*, in : Media and Arts Law Review 2006/11, pp. 418-439 (Cité : McLachlan, *From Savigny to Cyberspace*).

MEDEF, *Livre blanc : « Blockchain pour les entreprises »*, in : CIGREF (http ://www.cigref.fr/), Paris 2017, p. « http://www.cigref.fr/wp/wp-content/uploads/2017/06/Livre-blanc-Blockchain-pour-entreprises.pdf » (30/07/2017) (Cité : MEDEF, *« Blockchain pour les entreprises »*).

Métille Sylvain, *L'informatique en nuage au sein d'une étude d'avocats*, in : Plaidoyer 2013 31/3, pp. 39-43 (Cité : Métille, *L'informatique en nuage au sein d'une étude d'avocats*).

Métille Sylvain, *Directive sur la conservation des données invalidée par la CJUE*, in : Village de la Justice (https ://www.village-justice.com/), Paris 2014, p. « https://www.village-justice.com/articles/Directive-sur-conservation-des,16679.html » (09/12/2019) (Cité : Métille, *Directive sur la conservation des données invalidée par la CJUE*).

Métille Sylvain, *Le droit au respect de la vie privée : Les défis digitaux, une perspective de droit comparée (Suisse)*, in : EPRS | Service de recherche du Parlement européen, Bruxelles 2018, pp. 1-44 (Cité : Métille, *Le droit au respect de la vie privée*).

Métille Sylvain, *L'utilisation de l'informatique en nuage par l'administration publique*, in : AJP/PJA 2019/6, pp. 609-621 (Cité : Métille, *L'utilisation de l'informatique en nuage par l'administration publique*).

Métille Sylvain / Arasteh Yasmine, *Le Règlement général sur la protection des données et les assureurs privés suisses*, in : Jahrbuch SGHVR = Annuaire SDRCA 2018, pp. 111-142 (Cité : Métille / Arasteh, *Le Règlement général sur la protection des données et les assureurs privés suisses*).

Métille Sylvain / di Tria Livio, *Protection des données : responsabilité croissante ?*, in : Expert Focus 2019 2019/4, pp. 308-309 (Cité : Métille / di Tria, *Protection des données*).

van der Meulen Rob, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, in : Gartner (https ://www.gartner.com/), Egham 2017, p. « https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 » (27/10/2018) (Cité : van der Meulen, *8.4 Billion Connected "Things" Will Be in Use*).

Meunier Nicolas, *Audi A8, un pas de plus vers la voiture autonome*, in : Challenges (https ://www.challenges.fr/), Paris 2017, p. « https://www.challenges.fr/automobile/nouveautes/audi-a8-un-pas-de-plus-vers-la-voiture-autonome_486469 » (27/10/2018) (Cité : Meunier, *Audi A8, un pas de plus vers la voiture autonome*).

Meyer David, *Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World*, in : Fortune (https ://fortune.com/), New York 2017, p. « https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/ » (16/12/2019) (Cité : Meyer, *Vladimir Putin Says Whoever Leads in AI Will Rule the World*).

Meyer Paul / Stauffacher Daniel, *WannaCry, the Geneva Digital Convention and the urgent need for Cyber Peace - A commentary by ICT4Peace*, in : ICT4Peace Foundation (https ://ict4peace.org/), Geneva 2017, p. « https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2017-Wannacry-GenevaDigitalConvention.pdf » (03/12/2019) (Cité : Meyer / Stauffacher, *WannaCry*).

Michalon Gilles / Auger Gerard, *Method for the transmission of data among mobile bodies or autonomous vehicles*, in : United States Patent 1994, pp. 1-9 (Cité : Michalon / Auger, *Method for the transmission of data among mobile bodies or autonomous vehicles*).

Millon Louise, *Brainternet : des chercheurs ont lié un cerveau humain à un ordinateur*, in : SiecleDigital (https ://siecledigital.fr/), Lyon 2017, p. « https://siecledigital.fr/2017/09/28/brainternet-des-chercheurs-ont-lie-un-cerveau-humain-un-ordinateur/ » (24/03/2020) (Cité : Millon, *Brainternet*).

Minsky Marvin, *Steps toward Artificial Intelligence*, in : Proceedings of the IRE 1961 49/1, pp. 8-30 (Cité : Minsky, *Steps toward AI*).

Mittelstadt Brent Daniel, *Automation, Algorithms, and Politics | Auditing for Transparency in Content Personalization Systems*, in : International Journal of Communication 2016/10, pp. 1-12.

Mittelstadt Brent Daniel / Allo Patrick / Taddeo Mariarosaria / Wachter Sandra / Floridi Luciano, *The ethics of algorithms : Mapping the debate*, in : Big Data & Society 2016 3/2, pp. 1-21.

Mittelstadt Brent Daniel / Floridi Luciano, *The Ethics of Big Data : Current and Foreseeable Issues in Biomedical Contexts*, in : Science and Engineering Ethics 2016 22/2, pp. 303-341 (Cité : Mittelstadt / Floridi, *The Ethics of Big Data*).

Moerel Lokke, *The long arm of EU data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ?*, in : International Data Privacy Law 2010 1/1, pp. 28-46 (Cité : Moerel, *The long arm of EU data protection law*).

Moerel Lokke, *Back to basics : when does EU data protection law apply ?*, in : International Data Privacy Law 2011 1/2, pp. 92-110 (Cité : Moerel, *Back to basics*).

Molnár-Gábor Fruzsina / Korbel Jo, *Verarbeitung von Patientendaten in der Cloud - Die Freiheit translationaler Forschung und der Datenschutz in Europa*, in : Zeitschrift für Datenschutz (ZD) 2016 6/6, pp. 274-281 (Cité : Molnár-Gábor / Korbel, *Verarbeitung von Patientendaten in der Cloud*).

Moniz Graça Canto, *Finally : a coherent framework for the extraterritorial scope of EU data protection law - the end of the linguistic conundrum of Article 3 (2) of the GDPR*, in : UNIO–EU Law Journal 2018 4/2, pp. 105-116 (Cité : Moniz, *Finally*).

Monteiro Ana Menezes, *First GDPR fine in Portugal issued against hospital for three violations*, in : IAPP (https ://iapp.org/), Portsmouth 2019, p. « https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ » (07/06/2019) (Cité : Monteiro, *First GDPR fine in Portugal*).

de Montjoye Yves-Alexandre / Hidalgo César A. / Verleysen Michel / Blondel Vincent D., *Unique in the Crowd : The privacy bounds of human mobility*, in : Nature Scientific Reports 2013/3, pp. 1-5 (Cité : de Montjoye, *Unique in the Crowd*).

de Montjoye Yves-Alexandre / Radaelli Laura / Singh Vivek Kumar, *Unique in the shopping mall : On the reidentifiability of credit card metadata*, in : Science 2015 347/6221, pp. 536-539.

de Montjoye Yves-Alexandre / Shmueli Erez / Wang Samuel S / Pentland Alex Sandy / Preis Tobias, *openPDS : Protecting the Privacy of Metadata through SafeAnswers*, in : PLoS one 2014 9/7, pp. 1-9 (Cité : de Montjoye, *openPDS*).

Müller Luka, *BCP Framework for Assessment of Crypto Tokens*, in : MME Legal (https ://www.mme.ch/), Zürich 2017, p. « https://www.mme.ch/en/magazine/magazine-detail/url_magazine/conceptual_framework_for_blockchain_crypto_property_bcp/ » (10/10/2017) (Cité : Müller, *BCP Framework for Assessment of Crypto Tokens*).

Murgia Madhumita, *Microsoft quietly deletes largest public face recognition data set*, in : Financial Times (https ://www.ft.com/), London 2019, p. « https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 » (07/06/2019) (Cité : Murgia, *Microsoft quietly deletes largest public face recognition data set*).

Murray Gabriel, *Stoic Ethics for Artificial Agents*, in : Advances in Artificial Intelligence 2017, pp. 373-384.

Nägele Thomas / Jacobs Sven, *Rechtsfragen des Cloud Computing*, in : ZUM : Zeitschrift für Urheber- und Medienrecht/Film und Recht 2010 54/4, pp. 281-292 (Cité : Nägele / Jacobs, *Rechtsfragen des Cloud Computing*).

Nardi Daniele, *« Courtoisie internationale » et portée extraterritoriale du droit européen à la protection des données à l'épreuve de la Cour*, in : Cahiers de droit europeen 2018 54/2, pp. 327-362 (Cité : Nardi, *« Courtoisie internationale »*).

Nembrini Julien / Lalanne Denis, *Human-Building Interaction : When the Machine Becomes a Building*, in : Human-Computer Interaction - INTERACT 2017, pp. 348-369 (Cité : Nembrini / Lalanne, *Human-Building Interaction*).

Noothigattu Ritesh / Gaikwad Snehalkumar S. / Awad Edmond / Dsouza Sohan / Rahwan Iyad / Ravikumar Pradeep / Procaccia Ariel D., *A voting-based system for ethical decision making*, in : Thirty-Second AAAI Conference on Artificial Intelligence 2018, pp. 1587-1594 (Cité : Noothigattu, *A voting-based system for ethical decision making*).

O'Brien David / Budish Ryan / Faris Robert / Gasser Urs / Lin Tiffany, *Privacy and Cybersecurity Research Briefing*, in : Berkman Klein Center Research Publication 2016/17, pp. 1-16 (Cité : O'Brien, *Privacy and Cybersecurity Research Briefing*).

Oberson Xavier, *Taxer les robots ? L'émergence d'une capacité contributive électronique*, in : AJP/PJA 2017, pp. 232-239 (Cité : Oberson, *Taxer les robots ?*).

Okşar İrfan, *A Bluetooth signal strength based indoor localization method*, in : Proceedings of the 2014 IWSSIP, Dubrovnik 2014, pp. 251-254.

Onik Md Mehedi Hassan / Kim Chul-Soo / Lee Nam-Yong / Yang Jinhong, *Privacy-aware blockchain for personal data sharing and tracking*, in : Open Computer Science 2019 9/1, pp. 80-91 (Cité : Onik, *Privacy-aware blockchain*).

Pailler Ludovic, *L'applicabilité spatiale du Règlement géneral sur la protection des données (RGPD) : Commentaire de l´article 3*, in : Journal du droit international 2018 145/3, pp. 823-849 (Cité : Pailler, *L'applicabilité spatiale du Règlement géneral sur la protection des données (RGPD)*).

Papageorgiou Nik, *PlantVillage, une application qui détecte les maladies des plantes*, in : Actu EPFL (https ://actu.epfl.ch/), Lausanne 2016, p. « https://actu.epfl.ch/news/plantvillage-une-application-qui-detecte-les-malad/ » (27/10/2018).

Pascanu Razvan / Weber Theophane / Battaglia Peter / Reichert David / Racanière Sébastien / Li Yazhe, *Agents that imagine and plan*, in : Deepmind (https ://deepmind.com/), London 2017, p. « https://deepmind.com/blog/article/agents-imagine-and-plan » (28/09/2017) (Cité : Pascanu, *Agents that imagine and plan*).

Patel Nilay, *Facebook's $5 billion FTC fine is an embarrassing joke*, in : The Verge (https ://www.theverge.com/), Washington D.C. 2019, p. « https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke » (06/08/2019) (Cité : Patel, *Facebook's $5 billion FTC fine is an embarrassing joke*).

Pato Alexia, *The Collective Private Enforcement of Data Protection Rights in the EU*, in : MPI-IAPL Summer School 3rd edition 2019, pp. 1-20 (Cité : Pato, *The Collective Private Enforcement of Data Protection Rights in the EU*).

Pégny Maël / Thelisson Eva / Ibnouhsein Issam, *The Right to an Explanation : An Interpretation and Defense*, in : Delphi - Interdisciplinary Review of Emerging Technologies 2019 2/4, pp. 161-166 (Cité : Pégny / Thelisson / Ibnouhsein, *The Right to an Explanation*).

Pescatore Pierre, *Aspects judiciaires de l'acquis communautaire*, in : Revue trimestrielle de droit européen 1981 17/4, pp. 617-651 (Cité : Pescatore, *Aspects judiciaires de l'acquis communautaire*).

Petit Jonathan / Shladover Steven E., *Potential Cyberattacks on Automated Vehicles*, in : IEEE Transactions on Intelligent Transportation Systems 2015 16/2, pp. 546-556 (Cité : Petit / Shladover, *Potential Cyberattacks on Automated Vehicles*).

Picht Peter Georg / Loderer Gaspare, *Framing Algorithms – Competition Law and (Other) Regulatory Tools*, in : Max Planck Institute for Innovation & Competition Research Paper 2018, pp. 1-35 (Cité : Picht / Loderer, *Framing Algorithms*).

Polrot Simon, *Panorama des enjeux juridiques de la Blockchain*, in : Blockchain Partner (https ://blockchainpartner.fr/), Paris 2017, p. « https://blockchainpartner.fr/wp-content/uploads/2017/05/Enjeux-juridiques-de-la-blockchain-Blockchain-Partner.pdf?utm_source=Sociallymap&utm_medium=Sociallymap&utm_campaign=Sociallymap » (30/07/2017) (Cité : Polrot, *Panorama des enjeux juridiques de la Blockchain*).

Portouli Evangelia / Karaseitanidis Giannis / Lytrivis Panagiotis / Amditis Angelos / Raptis Odisseas / Karaberi Christina, *Public attitudes towards autonomous mini buses operating in real conditions in a Hellenic city*, in : IEEE Intelligent Vehicles Symposium (IV), Los Angeles 2017, pp. 571-576 (Cité : Portouli, *Public attitudes towards autonomous mini buses*).

Pötters Stephan, *Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts*, in : Recht der Datenverarbeitung (RDV) 2015/1, pp. 10-16 (Cité : Pötters, *Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts*).

Poullet Yves, *Transborder data flows and extraterritoriality : The European Position*, in : Journal of International Comercial Law and Technology 2007 2/3, pp. 141-157 (Cité : Poullet, *Transborder data flows and extraterritoriality*).

Powles Julia / Hodson Hal, *Google DeepMind and healthcare in an age of algorithms*, in : Health and technology 2017 7/4, pp. 351-367 (Cité : Powles / Hodson, *Google DeepMind and healthcare*).

Prainsack Barbara, *Research for personalised medicine : Time for solidarity*, in : Medicine and Law 2017 36/1, pp. 87-98.

Privacy International, *Privacy International and nine other human rights organizations pursue landmark case at European Court of Human Rights directly challenging UK and US mass surveillance revealed by Edward Snowden*, in : Privacy International (http ://privacyinternational.org/), London 2016, p. « https://bit.ly/2CPI1Hg

» (27/10/2018) (Cité : Privacy International, *Privacy International and nine other human rights organizations*).

Privacy Shield Framework, *Welcome to the Privacy Shield*, in : Privacy Shield Framework (https ://www.privacyshield.gov/), Washington D.C. s.a., p. « https://www.privacyshield.gov/welcome » (21/03/2020) (Cité : Privacy Shield Framework, *Welcome to the Privacy Shield*).

Purdy Mike / Daugherty Paul, *Why artificial intelligence is the future of growth ?*, in : Remarks at AI Now : The Social and Economic Implications of Artificial Intelligence Technologies in the Near Term 2016, pp. 1-72 (Cité : Purdy / Daugherty, *Why artificial intelligence is the future of growth ?*).

Racine Jean-Baptiste, *Approches de droit global*, in : Journal du droit international 2019 146/3, pp. 665-693 (Cité : Racine, *Approches de droit global*).

Radio Télévision Suisse, *Les frontières suisses surveillées par des drones*, in : RTS (https ://www.rts.ch/), Genève 2006, p. « https://www.rts.ch/info/suisse/980114-les-frontieres-suisses-surveillees-par-des-drones.html » (27/10/2018) (Cité : Radio Télévision Suisse, *Les frontières suisses surveillées par des drones*).

Reisberg Anthony, *Intelligence artificielle : faut-il craindre un obscurantisme éclairé ?*, in : Le Club des Juristes (https ://www.leclubdesjuristes.com), Paris 2019, p. « https://www.leclubdesjuristes.com/wp-content/uploads/2019/06/Intelligence-artificielle-faut-il-craindre-un-obscurantisme-%C3%A9clair%C3%A9-Anthony-Reisberg-1.pdf » (22/03/2020) (Cité : Reisberg, *Intelligence artificielle*).

Riechert Anne, *Dateneigentum – ein unauflösbarer Interessenkonflikt ?*, in : Datenschutz und Datensicherheit-DuD 2019 43/6, pp. 353-360 (Cité : Riechert, *Dateneigentum*).

Rigaux François, *L'élaboration d'un « right of privacy » par la jurisprudence américaine*, in : Revue internationale de droit comparé 1980 321980/4, pp. 701-730.

Rissland Edwina L. / Ashley Kevin D. / Loui R. P., *AI and Law : A fruitful synergy*, in : Artificial Intelligence 2003 150/1, pp. 1-15.

Ropert Pierre, *En Inde et en Nouvelle-Zélande, le fleuve reconnu comme un être vivant*, in : France Culture (https ://www.franceculture.fr/), Paris 2017, p. « https://bit.ly/3bUxIAs » (29/09/2017) (Cité : Ropert, *En Inde et en Nouvelle-Zélande*).

Rosier Karen / Losdyck Bénédicte / De Terwangne Cécile, *Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel*, in : Revue du Droit des Technologies de l'information 2016/62, pp. 5-56 (Cité : Rosier / Losdyck / De Terwangne, *Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel*).

Rossi Julien, *Guide de la jurisprudence européenne en matière de protection des données à caractère personnel*, in : Cahiers Costech 2017 58/1, pp. 1-80 (Cité : Rossi, *Guide de la jurisprudence européenne*).

Rossnagel Alexander / Nebel Maxi / Richter Philipp, *Was bleibt vom Europäischen Datenschutzrecht ? Überlegungen zum Ratsentwurf der DS-GVO*, in : Zeitschrift für Datenschutz 2015/5, pp. 455-460 (Cité : Rossnagel / Nebel / Richter, *Was bleibt vom Europäischen Datenschutzrecht ?*).

Rossnagel Alexander / Richter Philipp / Nebel Maxi, *Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DS-GVO*, in : Zeitschrift für Datenschutz 2013 3/3, pp. 103-108 (Cité : Rossnagel / Richter / Nebel, *Besserer Internetdatenschutz für Europa*).

Rozières Grégory, *Comment Airbus imagine nos transports du futur*, in : Le Huffington Post (https ://www.huffingtonpost.fr/), Paris 2016, p. « https://www.huffingtonpost.fr/2016/08/20/airbus-transport - futur _ n _ 11605840 . html » (27/10/2018) (Cité : Rozières, *Comment Airbus imagine nos transports du futur*).

Ruben Alexander, *The First Blockchain Wedding*, in : Bitcoin Magazine (https ://bitcoinmagazine.com/) Nashville 2014, p. « https: / / bitcoinmagazine . com / articles / first - blockchain - wedding - 1411842604/ » (30/07/2017) (Cité : Ruben, *The First Blockchain Wedding*).

Ruche Sébastien, *La surveillance des fintechs entre en vigueur*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https:// www.letemps.ch/economie/surveillance-fintechs-entre-vigueur » (28/10/2018) (Cité : Ruche, *La surveillance des fintechs entre en vigueur*).

Russell Stuart / Shi-Nash Amy / Lukose Dickson / Chen Fang, *Panel Discussion "Developments and Challenges with the Data Economy"*, in : Big Data Summit (http ://www.bigdatasummit.co/) Melbourne 2017, p. « http://203.170.84.89/~idawis33/wordpress/

program/BDS2017_Program.pdf » (27/09/2017) (Cité : Russell, *Developments and Challenges with the Data Economy*).

Schürch Simone, *Le programme Helsana+ (2/2)*, in : LawInside (http : //www.lawinside.ch/), Zürich 2019, pp. 1-2, p. « http : / / www . lawinside.ch/748/ » (29/12/2019) (Cité : Schürch, *Le programme Helsana+*).

Selbst Andrew D. / Powles Julia, *Meaningful information and the right to explanation*, in : International Data Privacy Law 2017 7/4, pp. 233-242 (Cité : Selbst / Powles, *Meaningful information and the right to explanation*).

Seydtaghia Anouch, *Qui les voitures autonomes devront-elles tuer et protéger ?*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/economie/voitures-autonomes-devrontelles - tuer - proteger » (27/10/2018) (Cité : Seydtaghia, *Qui les voitures autonomes devront-elles tuer et protéger ?*).

Seydtaghia Anouch, *Google City, la ville intelligente futuriste qui inquiète*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2019, p. « https : / / www . letemps . ch / economie / google - city - ville - intelligente - futuriste - inquiete » (29/06/2019) (Cité : Seydtaghia, *Google City*).

Shay Lisa A. / Hartzog Woodrow / Nelson John / Conti Gregory, *Do robots dream of electric laws ? An experiment in the law as algorithm*, in : Robot Law 2016, pp. 274-305.

Showalter Stephanie, *The Legal Status of Autonomous Underwater Vehicles*, in : Marine Technology Society Journal 2004 38/1, pp. 80-83.

Siemens George / Long Phil, *Penetrating the fog : Analytics in learning and education*, in : EDUCAUSE review 2011 46/5, p. 30.

Sobati Moghadam Somayeh / Darmont Jérôme / Gavin Gérald, *Enforcing Privacy in Cloud Databases*, in : Big Data Analytics and Knowledge Discovery 2017, pp. 53-73 (Cité : Sobati Moghadam / Darmont / Gavin, *Enforcing Privacy in Cloud Databases*).

Solove Daniel J., *Conceptualizing privacy*, in : California Law Review 2002/90, pp. 1087-1156 (Cité : Solove, *Conceptualizing privacy*).

Solove Daniel J., *Reconstructing electronic surveillance law*, in : George Washington Law Review 2003/72, pp. 1264-1310 (Cité : Solove, *Reconstructing electronic surveillance law*).

Soyez Fabien, *L'ADN et le quartz pour stocker nos données pour l'éternité*, in : Techniques de l'Ingénieur (https ://www.techniques-ingenieur.fr/), Saint-Denis 2016, p. « https://www.techniques-ingenieur.fr/actualite/articles/ladn-quartz-stocker-nos-donnees-leternite-33538/ » (21/05/2019) (Cité : Soyez, *L'ADN et le quartz pour stocker nos données pour l'éternité*).

Stahl Bernd Carsten / Wright David, *Ethics and Privacy in AI and Big Data : Implementing Responsible Research and Innovation*, in : IEEE Security & Privacy 2018 16/3, pp. 26-33.

Steinberger Helmut, *Sovereignty*, in : Encyclopedia of Disputes Installment 1987/10, pp. 397-418 (Cité : Steinberger, *Sovereignty*).

Stern Brigitte, *L'extra-territorialité « revisitée » : où il est question des affaires Alvarez-Machain, Pâte de Bois et de quelques autres...*, in : Annuaire français de droit international 1992 38/1, pp. 239-313 (Cité : Stern, *L'extra-territorialité «revisitée»*).

Stolfi Daniel H. / Alba Enrique / Yao Xin, *Predicting Car Park Occupancy Rates in Smart Cities*, in : Smart Cities 2017, pp. 107-117 (Cité : Stolfi / Alba / Yao, *Predicting Car Park Occupancy Rates*).

Strowel Alain, *Robots et gouvernance des données : avons-nous besoin de nouveaux droits et devoirs ?*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https://www.isdc.ch/fr/evenements/prochains-evenements/droit-robot » (21/03/2020) (Cité : Strowel, *Robots et gouvernance des données*).

Sydow Gernot / Kring Markus, *Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug - Konkurrierende Leitbilder für den europäischen Rechtsrahmen*, in : Zeitschrift für Datenschutz 2014, pp. 271-276 (Cité : Sydow / Kring, *Die Datenschutzgrundverordnung*).

Tassel Camille, *Luc Ferry : « Le transhumanisme parie sur le fait que l'homme est perfectible »*, in : Le Monde des Religions (http ://www.lemondedesreligions.fr/), Paris 2016, p. « https://bit.ly/3bUxIAs » (21/05/2019) (Cité : Tassel, *« Le transhumanisme parie sur le fait que l'homme est perfectible »*).

Tene Omer / Polonetsky Jules, *Judged by the tin man : Individual rights in the age of big data*, in : Journal on Telecommunication and High Technology Law 2013/11, pp. 351-368.

Thayer Eric, *Adversarial Testing to Increase the Overall Security of Embedded Systems : A Review of the Process*, in : IEEE Control Systems 2017 37/2, pp. 104-108 (Cité : Thayer, *Adversarial Testing to Increase the Overall Security of Embedded Systems*).

The Public Voice, *Standards mondiaux de respect de la vie privée dans un monde globalisé : Déclaration de la société civile Madrid, Espagne 3 novembre 2009*, in : The Public Voice (https ://thepublicvoice.org/), s.l. 2009, p. « https://thepublicvoice.org/madrid-declaration/fr/ » (29/05/2017) (Cité : The Public Voice, *Standards mondiaux de respect de la vie privée dans un monde globalisé*).

Thelisson Eva, *Towards Trust, Transparency, and Liability in AI/AS Systems*, in : Proceedings of the 26th International Joint Conference on Artificial Intelligence, Melbourne 2017, pp. 5215-5216 (Cité : Thelisson, *Towards Trust, Transparency, and Liability*).

Thelisson Eva / Padh Kirtan / Celis L. Elisa, *Regulatory Mechanisms and Algorithms towards Trust in AI/ML*, in : Proceedings of the IJCAI 2017 Workshop on Explainable Artificial Intelligence (XAI), Melbourne 2017, pp. 1-5 (Cité : Thelisson / Padh / Celis, *Regulatory Mechanisms and Algorithms towards Trust*).

Thierache Corinne, *RGPD vs. Cloud Act : Le nouveau cadre légal américain est-il anti RGPD ?*, in : La Revue juridique Dalloz IP/IT 2019 2019/6, pp. 367-371 (Cité : Thierache, *RGPD vs Cloud Act*).

Trevor Mark / Inglis Keith / Heard Andrew, *Data Centre Risk Index*, in : Cushman and Wakefield (http ://www.cushmanwakefield.com/), London 2016, p. « http://www.cushmanwakefield.com/en/research-and-insight/2016/data-centre-risk-index-2016 » (27/10/2018) (Cité : Trevor / Inglis / Heard, *Data Center Risk Index*).

Tribune de Genève, *Des drones au service des agriculteurs*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2016, p. « https://www.tdg.ch/suisse/drones-service-agriculteurs/story/17274017 » (27/10/2018) (Cité : Tribune de Genève, *Des drones au service des agriculteurs*).

Tribune de Genève, *372'000 clients rejoignent l'action groupée contre VW*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2019, p. « https://www.tdg.ch/economie/372-000-clients-rejoignent-laction-groupee-vw/story/16603789 » (30/06/2019) (Cité : Tribune de Genève, *372'000 clients rejoignent l'action groupée contre VW*).

Troncoso Carmela, *Privacy & Online Rights Knowledge Area*, in : The Cyber Security Body of Knowledge (https ://www.cybok.org/), Bristol 2019, p. « https://www.cybok.org/media/downloads/Privacy__Online_Rights_issue_1.0_K5yBOao.pdf » (09/03/2020) (Cité : Troncoso, *Privacy & Online Rights*).

U. Farooq M. / Waseem Muhammad / Mazhar Sadia / Khairi Anjum / Kamal Talha, *A Review on Internet of Things (IoT)*, in : IJCA International Journal of Computer Applications 2015 113/1, pp. 1-7.

Usman Muhammad / Ahmad Jan Mian / He Xiangjian, *Cryptography - based secure data storage and sharing using HEVC and public clouds*, in : Information Sciences 2017/387, pp. 90-102 (Cité : Usman / Ahmad Jan / He, *Cryptography - based secure data storage and sharing*).

Vallet Félicien, *Les droits de la voix (2/2) - Quelle parole pour nos systèmes ?*, in : Laboratoire d'Innovation Numérique de la CNIL (https ://linc.cnil.fr/), Paris 2019, p. « https://linc.cnil.fr/les-droits-de-la-voix-22-quelle-parole-pour-nos-systemes » (27/06/2019) (Cité : Vallet, *Les droits de la voix*).

Van Loo Rory, *Making innovation more competitive : The case of fintech*, in : UCLA Law Review 2018/65, pp. 232-279 (Cité : Van Loo, *Making innovation more competitive*).

Vasella David, *DSGVO : Stand und Fundstellen*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2016, pp. 28-29 (Cité : Vasella, *DSGVO*).

Veale Michael / Van Kleek Max / Binns Reuben, *Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making*, in : Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York 2018, pp. 1-14 (Cité : Veale / Van Kleek / Binns, *Fairness and accountability design needs*).

Verma Himanshu / Alavi Hamed S. / Lalanne Denis, *Studying Space Use : Bringing HCI Tools to Architectural Projects*, in : Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York 2017, pp. 3856-3866 (Cité : Verma / Alavi / Lalanne, *Studying Space Use*).

Vincent Catherine, *Serge Tisseron : « Les robots vont modifier la psychologie humaine »*, in : Le Monde (https ://www.lemonde.fr/), Paris 2018, p. « https://www.lemonde.fr/idees/article/2018/07/12/serge-tisseron-les-robots-vont-modifier-la-psychologie-humaine_5330469_3232.html » (15/12/2019) (Cité : Vincent, *« Les robots vont modifier la psychologie humaine »*).

Von Lewinski K. / Herrmann C., *Cloud vs. Cloud–Datenschutz im Binnenmarkt*, in : Zeitschrift für Danetschutz 2016 6/10, pp. 467-474 (Cité : Von Lewinski / Herrmann, *Cloud vs. Cloud*).

Vordermayer Markus, *Ein „Abschied von den Grundrechten"?*, in : Rescriptum (http ://www.rescriptum.org/), München 2012, p. « http://www.rescriptum.org/Aufs%C3%A4tze/2012_1_024_Vordermayer.pdf » (18/04/2019) (Cité : Vordermayer, *Ein „Abschied von den Grundrechten"?*).

Wachter Sandra / Mittelstadt Brent Daniel, *A right to reasonable inferences : re-thinking data protection law in the age of Big Data and AI*, in : Columbia Business Law Review 2018, pp. 494-620 (Cité : Wachter / Mittelstadt, *A right to reasonable inferences*).

Wachter Sandra / Mittelstadt Brent Daniel / Floridi Luciano, *Transparent, explainable, and accountable AI for robotics*, in : Science Robotics 2017 2/6, pp. 1-2 (Cité : Wachter / Mittelstadt / Floridi, *Transparent, explainable, and accountable AI for robotics*).

Wachter Sandra / Mittelstadt Brent Daniel / Floridi Luciano, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in : International Data Privacy Law 2017 7/2, pp. 76-99 (Cité : Wachter / Mittelstadt / Floridi, *Why a right to explanation of automated decision-making does not exist*).

Walter Hans Peter, *Prozessuale Aspekte beim Streit zwischen Kunden und Vermögensverwaltern*, in : Zeitschrift für schweizerisches Recht 2008 127/1, pp. 99-134 (Cité : Walter, *Prozessuale Aspekte beim Streit zwischen Kunden und Vermögensverwaltern*).

Walter Jean-Philippe, *Modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*, in : International Conference on Modernisation of Data Protection Legislation in Europe, Skopje 2012, pp. 1-15 (Cité : Walter, *Modernisation of the Council of Europe Convention*).

Walter Jean-Philippe, *La protection des données n'est pas un frein à l'innovation*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/opinions/protection-donnees-nest-un-frein-linnovation » (01/11/2018) (Cité : Walter, *La protection des données n'est pas un frein à l'innovation*).

Wang Cunrui / Zhang Qingling / Liu Wanquan / Liu Yu / Miao Lixin, *Facial feature discovery for ethnicity recognition*, in : Wiley Interdisciplinary Reviews : Data Mining and Knowledge Discovery 2019 9/1, pp. 1-17 (Cité : Wang, *Facial feature discovery for ethnicity recognition*).

Wang Fei-Yue / Zhang Jun Jason / Zheng Xinhu / Wang Xiao / Yuan Yong / Dai Xiaoxiao / Zhang Jie / Yang Liuqing, *Where does AlphaGo go : From church-turing thesis to AlphaGo thesis and beyond*, in : IEEE/CAA Journal of Automatica Sinica 2016 3/2, pp. 113-120 (Cité : Wang, *Where does AlphaGo go*).

Wang Hua / Chignell Mark / Ishizuka Mitsuru, *Empathic tutoring software agents using real-time eye tracking*, in : Proceedings of the 2006 Symposium on Eye Tracking Research & Applications 2006, pp. 73-78.

Waters Richard, *US agency criticises Tesla over fatal crash*, in : Financial Times (https ://www.ft.com/), London 2017, p. « https://www.ft.com/content/a040c84a-97d1-11e7-a652-cde3f882dd7b » (27/10/2018) (Cité : Waters, *US agency criticises Tesla over fatal crash*).

Weber Rolf H., *Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises*, in : Journal of Governance and Regulation and Volume 2012 1/1, pp. 8-14 (Cité : Weber, *Overcoming the Hard Law/Soft Law Dichotomy*).

Weber Rolf H., *EU - Datenschutz - Grundverordnung : Kernelemente und Ausstrahlungswirkung auf die Schweiz*, in : Jusletter IT (http ://jusletter-it.weblaw.ch/), Bern 2015, p. « http://jusletter-it.weblaw.ch / issues / 2015 / 24 - September - 2015 / eu - datenschutz - grund _ bd86ed7481.html » (21/05/2019) (Cité : Weber, *EU - Datenschutz - Grundverordnung*).

Weber Rolf H., *Internet of things : Privacy issues revisited*, in : Computer law & security review 2015 31/5, pp. 618-627 (Cité : Weber, *Internet of things*).

Wells Catharine Pierce, *Tort Law as Corrective Justice : A Pragmatic Justification for Jury Adjudication*, in : Michigan Law Review 1990 88/8, pp. 2348-2413 (Cité : Wells, *Tort Law as Corrective Justice*).

Widmer Pierre, *Aspects de responsabilité civile*, in : « La nouvelle loi fédérale sur la protection des données » (CEDIDAC), Lausanne 1994/28, pp. 179-206 (Cité : Widmer, *Aspects de responsabilité civile*).

Wojtyczek Krzysztof, *Les fonctions de la Constitution écrite dans le contexte de la mondialisation*, in : UMK (https ://www.umk.ro/), Iasi 2011, p. « https://www.umk.ro/images/documente/publicatii/masarotunda2007 / 10 _ les _ fonctions . pdf » (04/01/2020) (Cité : Wojtyczek, *Les fonctions de la Constitution*).

Wooldridge Mike / Millican Peter / Boddington Paula, *Towards a Code of Ethics for Artificial Intelligence Research*, in : Oxford University (https ://www.cs.ox.ac.uk/), Oxford 2015, p. « https : / / www . cs . ox . ac . uk / efai / towards - a - code - of - ethics - for - artificial-intelligence/ » (29/09/2017) (Cité : Wooldridge / Millican / Boddington, *Towards a Code of Ethics for Artificial Intelligence Research*).

Wuthrich Bernard, *La protection des données est mise à mal par le Big Data*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/suisse/protection-donnees-mise-mal-big-data » (27/10/2018) (Cité : Wuthrich, *La protection des données est mise à mal par le Big Data*).

Wybitul Tim / Sörup Thorsten / Pötters Stephan, *Betriebsvereinbarungen und § 32 BDSG : Wie geht es nach der DS-GVO weiter ?*, in : ZD 2015, pp. 1-6.

Wytibul Tim, *Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte ? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen*, in : Zeitschrift für Datenschutz (ZD) 2016/5, pp. 203-208 (Cité : Wytibul, *Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte ?*).

Xiuquan Li / Tao Zhang, *An exploration on artificial intelligence application : From security, privacy and ethic perspective*, in : 2nd IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu 2017, pp. 416-420.

Zagni David, *Drones et voitures volantes : le ciel, nouvel horizon du transport individuel*, in : Les Echos (https ://www.lesechos.fr/), Paris 2017, p. « http://archives.lesechos.fr/archives/cercle/2017/03/20/cercle_167746.htm » (17/01/2020) (Cité : Zagni, *Drones et voitures volantes*).

Zarsky Tal, *Incompatible : The GDPR in the Age of Big Data*, in : Seton Hall Law Review 2017 47/4, pp. 995-1020.

Zhu Zhiwei / Ji Qiang, *Eye and gaze tracking for interactive graphic display*, in : Machine Vision and Applications 2004 15/3, pp. 139-148 (Cité : Zhu / Ji, *Eye and gaze tracking for interactive graphic display*).

Zunger Yonatan, *Computer Science Faces an Ethics Crisis*, in : The Boston Globe (https://www.bostonglobe.com/), Boston 2018, p. « https://www.bostonglobe.com/ideas/2018/03/22/computer-science-faces-ethics-crisis-the-cambridge-analytica-scandal-proves/IzaXxl2BsYBtwM4nxezgcP/story.html » (28/07/2019) (Cité : Zunger, *Computer Science Faces an Ethics Crisis*).

Zyskind Guy / Nathan Oz / Pentland Alex 'Sandy', *Decentralizing Privacy : Using Blockchain to Protect Personal Data*, in : IEEE Security and Privacy Workshops, San Jose 2015, pp. 180-184 (Cité : Zyskind / Nathan / Pentland, *Decentralizing Privacy*).

Sources officielles

Droit allemand

Bundeskartelamt, Facebook ; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung (B6 26/16, CCE 2019, Étude 13), in : Bundeskartelamt (https://www.bundeskartellamt.de/), Bonn 2019, p. « https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html » (30/06/2019) (Cité : Bundeskartelamt, Facebook).

Ethik Kommission, Automatisiertes und Vernetztes Fahren, in : Bundesministerium für Verkehr und digitale Infrastruktur (https://www.bmvi.de), Berlin 2017, p. « https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/06/084-dobrindt-bericht-der-ethik-kommission.pdf » (07/11/2017) (Cité : Ethik Kommission, Automatisiertes und Vernetztes Fahren).

Droit americain

Assembly Committee on Transportation, AB69 Law, An Act relating to transportation : revising requirements for the testing or operation of an autonomous vehicle on a highway within this State ; authorizing the use of driver-assistive platooning technology ; authorizing the use of a fully autonomous vehicle to provide transportation services in certain circumstances by persons licensed by the Department of Motor Vehicles, Nevada Transportation Authority or Taxicab Authority ; providing for the regulation of autonomous vehicle network companies ; providing penalties ; and providing other matters properly relating thereto, in : NELIS (https://www.leg.state.nv.us/), Las Vegas 2017, p. « https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/4750/Overview » (27/10/2018) (Cité : Assembly Committee on Transportation, AB69 Law).

Department of Justice, Justice Department Announces Publication of White Paper on the CLOUD Act, in : US DoJ (https://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/opa/pr/justice-department-announces-publication-white-paper-cloud-act » (16/12/2019) (Cité : Department of Justice, Justice Department Announces Publication of White Paper on the CLOUD Act).

Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act (White Paper), in : US DoJ (https://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/dag/page/file/1153436/download » (04/04/2020) (Cité : Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World).

Department of Justice, The CLOUD Act Resources - Statement of Richard W. Downing, in : US DoJ (https://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american » (29/03/2020) (Cité : Department of Justice, The CLOUD Act Resources).

EPIC, The CLOUD (Clarifying Lawful Overseas Use of Data) Act, in : EPIC (https://epic.org/), Washington D.C. 2018, p. « https://epic.org/privacy/cloud-act/ » (10/06/2019) (Cité : EPIC, The CLOUD

Act).

State of California, Autonomous Vehicles in California, in : California DMV (https://www.dmv.ca.gov/), Sacramento 2019, p. « https://www.dmv.ca.gov/portal/wcm/connect/caa2f466-fe0f-454a-a461-f5d7a079de49/avexpressterms_31017.pdf?MOD=AJPERES » (10/12/2019) (Cité : State of California, Autonomous Vehicles in California).

United States / Executive Office of the President, *Big Data : a report on algorithmic systems, opportunity, and civil rights*, Washington D.C. 2016 (Cité : United States / Executive Office of the President, *Big data : a report*).

United States / Executive Office of the President / Podesta John, *Big data : seizing opportunities, preserving values*, Washington D.C. 2014 (Cité : United States / Executive Office of the President / Podesta, *Big data*).

United States Congress, Consolidated Appropriations Act (H.R. 1625), in : US Congress (https://www.congress.gov/), Washington D.C. 2018, p. « https://www.congress.gov/bill/115th-congress/house-bill/1625 » (04/04/2020) (Cité : United States Congress, Consolidated Appropriations Act).

United States Congress, The Self-Drive Act (H.R. 3388), in : US Congress (https://www.congress.gov/), Washington D.C. 2017, p. « https://www.congress.gov/bill/115th-congress/house-bill/3388/text » (30/09/2017) (Cité : United States Congress, The Self-Drive Act).

United States Senate, Laws and Regulations, in : US Senate (https://www.senate.gov/), Washington D.C. s.a., p. « https://www.senate.gov/reference/reference_index_subjects/Laws_and_Regulations_vrd.htm » (08/11/2017) (Cité : United States Senate, Laws and Regulations).

United States Senate, Tax Haven Banks and U.S. Tax Compliance - Staff Report of the Permanent Subcommittee on Investigations (Released on July 17, 2008), in : US Senate Committee on Homeland Security and Government Affairs, Washington D.C. 2008, pp. 1-114 (Cité : United States Senate, Tax Haven Banks and U.S. Tax Compliance).

Droit anglais

Department for Digital, Culture, Media & Sport, Online Harms White Paper of 8 April 2019, in : UK Government Home Office (https://www.gov.uk/), London 2019, p. « https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper » (05/08/2019) (Cité : Department for Digital, Culture, Media & Sport, Online Harms White Paper).

Droit coréen

Republic of Korea, Intelligent Robots Development and Distribution Promotion Act, in : Statutes of the Republic of Korea (http://elaw.klri.re.kr/), Seoul 2008, p. « http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=39153Źtype=lawnameŹkey=robot » (29/09/2017) (Cité : Republic of Korea, Intelligent Robots Development and Distribution Promotion Act).

Droit européen

Affaires juridiques et parlementaires, Règles européennes de droit civil en robotique, in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2016, p. « https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016/571379_FR.pdf » (20/06/2017) (Cité : Affaires juridiques et parlementaires, Règles européennes de droit civil en robotique).

Agence des droits fondamentaux de l'Union européenne, La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données - Renforcement de l'architecture des droits fondamentaux au sein de l'UE II, in : FRA (https://fra.europa.eu/), Vienne 2010, p. « https://fra.europa.eu/fr/publication/2012/la-protection-des-donnees-caractere-personnel-dans-lunion-europeenne-le-role-des?lang%5B0%5D=fr » (01/04/2020) (Cité : Agence des droits fondamentaux de l'Union européenne, La protection des données à caractère personnel dans l'Union européenne).

Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data"), in : European Commission (https://ec.europa.eu/), Brussels 2011, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2

011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf » (26/03/2020) (Cité : Article 29 Data Protection Working Party, Advice paper on special categories of data).

Article 29 Data Protection Working Party, Appendix : Core Topics in the View of Trilogue, in : European Commission (https://ec.europa.eu/), Brussels 2015, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf » (25/10/2017) (Cité : Article 29 Data Protection Working Party, Core Topics in the View of Trilogue).

Article 29 Data Protection Working Party, Explanatory Document on the Processor Binding Corporate Rules - Adopted on 19 April 2013 (WP 204), in : European Commission (https://ec.europa.eu/), Brussels 2013, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf » (31/03/2020) (Cité : Article 29 Data Protection Working Party, Explanatory Document on the Processor Binding Corporate Rules).

Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf » (27/10/2018) (Cité : Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority).

Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - Adopted on 3 October 2017, Last Revised and Adopted on 6 February 2018 (WP 251 rev.01), in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 » (29/10/2018) (Cité : Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679).

Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 - Adopted on 28 November 2017, Last Revised and Adopted on 10 April 2018 (WP 259 rev.01), in : European Commission (https://ec.europa.eu/), Brussels 2017,

p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 » (31/12/2019) (Cité : Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679).

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 - Adopted on 4 April 2017, Last Revised and Adopted on 4 October 2017 (WP 248 rev.01), in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 » (05/04/2020) (Cité : Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA)).

Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs') - Adopted on 13 December 2016, Last Revised and Adopted on 5 April 2017 (WP 243 rev.01), in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 » (30/03/2020) (Cité : Article 29 Data Protection Working Party, Guidelines on Data Protection Officers).

Article 29 Data Protection Working Party, Letter from the Article 29 Working Party of the European Commission President to the CEO of Google with regards to Google Privacy Policy of 22 September 2014, in : European Commission (https://ec.europa.eu/), Brussels 2014, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf » (03/12/2018) (Cité : Article 29 Data Protection Working Party, Letter from the Article 29 Working Party of the European Commission President to the CEO of Google).

Article 29 Data Protection Working Party, Letter from the Article 29 Working Party of the European Commission President to the CEO of Microsoft of 22 September 2014, in : European Commission (https://ec.europa.eu/), Brussels 2014, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf » (03/12/2018) (Cité : Article 29 Data Protection Working Party, Letter from the Article 29 Working Party of the European Com-

mission President to the CEO of Microsoft).

Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing - Adopted on 1st July 2012 (WP 196), in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf » (04/12/2018) (Cité : Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing).

Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision - Adopted on 13 April 2016 (WP 238), in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf » (31/03/2020) (Cité : Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision).

Article 29 Data Protection Working Party, Opinion 02/2017 of Article 29 Data Protection Working Party on Data Processing at Work - Adopted on 8 June 2018 (WP 249), in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 » (06/12/2018) (Cité : Article 29 Data Protection Working Party, Opinion 02/2017 of Article 29 Data Protection Working Party).

Article 29 Data Protection Working Party, Update of Opinion 8/2010 of Article 29 Data Protection Working Party on applicable law in light of the CJEU judgement in Google Spain - Adopted on 16 December 2015 (WP 179 Update), in : European Commission (https://ec.europa.eu/), Brussels 2015, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf » (27/03/2020) (Cité : Article 29 Data Protection Working Party, Update of Opinion 8/2010 of Article 29 Data Protection Working Party).

Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) - Adopted on 13 April 2016 (WP 237), in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec

.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf » (31/03/2020) (Cité : Article 29 Data Protection Working Party, Working Document 01 / 2016 on the justification of interferences).

Commission européenne, Achever un marché unique numérique inspirant confiance pour tous - Communication de la Commission au Parlement Européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions du 15 mai 2018 (COM(2018) 320 final), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2018, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2018/FR/COM-2018-320-F1-FR-MAIN-PART-1.PDF » (21/07/2019) (Cité : Commission européenne, Achever un marché unique numérique inspirant confiance pour tous).

Commission européenne, Communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire du 27 novembre 2013 - COM (2013) 847 final, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2013, p. « https://eur-lex.europa.eu/procedure/FR/1041465 » (21/03/2020) (Cité : Commission européenne, Communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens).

Commission européenne, « Créer une économie fondée sur les données » - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions du 10 janvier 2017 (COM(2017) 9 final), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2017, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-9-F1-FR-MAIN-PART-1.PDF » (21/05/2019) (Cité : Commission européenne, « Créer une économie fondée sur les données »).

Commission européenne, Décision 2000/518/CE du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse (notifiée sous le numéro C(2000) 2304), in : Office des publications de l'Union européenne (https://op.europa.eu/), Luxembourg 2000, p. « https://op.europa.eu/fr/publication-detail/-/publication/ee7

6f93d-4545-4878-87cb-7750d7f59987 » (10/10/2017) (Cité : Commission européenne, Décision 2000/518/CE du 26 juillet 2000).

Commission européenne, Décision 2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (notifiée sous le numéro C(2001) 1539), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2001, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32001D0497 » (31/03/2020) (Cité : Commission européenne, Décision 2001/497/CE du 15 juin 2001).

Commission européenne, Décision 2004/915/CE du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers (notifiée sous le numéro C(2004) 5271), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2004, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32004D0915 » (31/03/2020) (Cité : Commission européenne, Décision 2004/915/CE du 27 décembre 2004).

Commission européenne, Décision 2010/87/UE du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (notifiée sous le numéro C(2010) 593), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2010, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32010D0087 » (31/03/2020) (Cité : Commission européenne, Décision 2010/87/UE du 5 février 2010).

Commission européenne, Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (C(2016) 4176), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016D1250 » (03/06/2017) (Cité : Commission européenne, Décision d'exécution (UE) 2016/1250).

Commission européenne, Directive 2002/77/CE du 16 septembre

2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2002, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32002L0077 » (04/07/2017) (Cité : Commission européenne, Directive 2002/77/CE du 16 septembre 2002).

Commission européenne, Discours sur l'état de l'Union du Président Juncker du 14 septembre 2016, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/france/news/20160914_discours_soteu_fr » (05/12/2018) (Cité : Commission européenne, Discours sur l'état de l'Union du Président Juncker).

Commission européenne, Échange et protection des données à caractère personnel à l'ère de la mondialisation - Communication de la Commission au Parlement européen et au Conseil du 10 janvier 2017 (COM(2017) 7 final), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2017, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017DC0007 » (29/06/2017) (Cité : Commission européenne, Échange et protection des données à caractère personnel à l'ère de la mondialisation).

Commission européenne, La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde - Communiqué de presse du 23 janvier 2019, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2019, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_421 » (04/06/2019) (Cité : Commission européenne, La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde).

Commission européenne, La Commission européenne lance le bouclier de protection des données UE-États-Unis : une protection renforcée pour les flux de données transatlantiques - Communiqué de presse du 12 juillet 2016, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_2461 » (31/03/2020) (Cité : Commission européenne, La Commission européenne lance le bouclier de protection des données UE-États-Unis).

Commission européenne, La Commission européenne présente le paquet « bouclier de protection des données UE-États-Unis » : des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données - Communiqué de presse du 29 février 2016, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_433 » (21/03/2020) (Cité : Commission européenne, La Commission européenne présente le paquet « bouclier de protection des données UE-États-Unis »).

Commission européenne, La Commission propose de resserrer les règles en matière de respect de la vie privée pour toutes les communications électroniques et actualise les règles relatives à la protection des données pour les instituti - Communiqué de presse du 10 janvier 2017, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_17_16 » (25/03/2020) (Cité : Commission européenne, La Commission propose de resserrer les règles en matière de respect de la vie privée).

Commission européenne, La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises - Communiqué de presse du 25 janvier 2012, in : Commission européenne (https://ec.europa.eu/), Bruxelles 2012, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_12_46 » (04/04/2020) (Cité : Commission européenne, La Commission propose une réforme globale).

Commission Européenne, Libérer tout le potentiel de l'informatique en nuage en Europe – qu'en est-il en pratique ?, in : Commission Européenne (https://ec.europa.eu/), Bruxelles 2012, p. « https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_12_713 » (18/04/2017) (Cité : Commission Européenne, Libérer tout le potentiel de l'informatique en nuage en Europe).

Commission européenne, Livre Vert du 19 décembre 2005 - Actions en dommages et intérêts pour infraction aux règles communautaires sur les ententes et les abus de position dominante (SEC(2005) 1732), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2005, p. « https://eur-lex.europa.eu/legal-content/FR

/TXT/PDF/?uri=CELEX:52005DC0672 » (02/04/2020) (Cité : Commission européenne, Livre Vert du 19 décembre 2005).

Commission européenne, Premier rapport sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE) - (COM(2003) 265/F1), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2003, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52003DC0265 » (01/04/2020) (Cité : Commission européenne, Premier rapport sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE)).

Commission européenne, Protection des données - Règles relatives à la protection des données à caractère personnel au sein et à l'extérieur de l'UE, in : Commission européenne (https://ec.europa.eu/), Bruxelles s.a., p. « https://ec.europa.eu/info/law/law-topic/data-protection_fr » (27/10/2018) (Cité : Commission européenne, Règles relatives à la protection des données).

Commission européenne, Règlement (UE) 2016/2067 du 22 novembre 2016 modifiant le règlement (CE) n° 1126/2008 portant adoption de certaines normes comptables internationales conformément au règlement (CE) n° 1606/2002 du Parlement européen et du Conseil, en ce qui concerne la norme internationale d'information financière IFRS 9, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R2067 » (31/12/2019) (Cité : Commission européenne, Règlement (UE) 2016/2067 du 22 novembre 2016).

Commission européenne, « Une approche globale de la protection des données à caractère personnel dans l'UE » (COM (2010) 609/3), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2010, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2010/FR/COM-2010-609-6-FR-MAIN-PART-1.PDF » (09/12/2019) (Cité : Commission européenne, « Une approche globale de la protection des données à caractère personnel dans l'UE »).

Commission européenne, Un plan coordonné dans le domaine de l'intelligence artificielle - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions du 7 décembre 2018 (COM(2018) 795 final), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2018, p. « https://ec.europa.eu/transparency/regdoc/r

ep/1/2018/FR/COM-2018-795-F1-FR-MAIN-PART-1.PDF » (10/12/2019) (Cité : Commission européenne, Un plan coordonné dans le domaine de l'intelligence artificielle).

Commission européenne, Une stratégie numérique pour l'Europe - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions du 19 mai 2010 (COM(2010) 245 final), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2010, p. « https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FR:PDF » (29/03/2020) (Cité : Commission européenne, Une stratégie numérique pour l'Europe).

Commission européenne, « Vers un cadre horizontal européen pour les recours collectifs » - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 11 juin 2013 (COM (2013) 401 final), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2013, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013DC0401 » (03/04/2020) (Cité : Commission européenne, « Vers un cadre horizontal européen pour les recours collectifs »).

Conseil de l'Europe, Convention 108 + : Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 2018, p. « https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726 » (21/05/2019) (Cité : Conseil de l'Europe, Convention 108 +).

Conseil de l'Europe, Conseil de l'Europe et intelligence artificielle, in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 2020, p. « https://www.coe.int/fr/web/artificial-intelligence/home » (03/01/2020) (Cité : Conseil de l'Europe, Conseil de l'Europe et intelligence artificielle).

Conseil de l'Europe, Modernisation de la « Convention n° 108 » sur la protection des données, in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 2013, p. « https://www.coe.int/fr/web/portal/28-january-data-protection-day-factsheet » (20/10/2017) (Cité : Conseil de l'Europe, Modernisation de la « Convention n° 108 »).

Conseil de l'Europe, Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, in : Série des traités du Conseil de l'Europe, Strasbourg 2018 2018/223, pp. 1-29 (Cité : Conseil de l'Europe, Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes).

Conseil de l'Europe, Resolution (73)22 du 26 septembre 1973 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 1973, p. « https://rm.coe.int/native/090000168050329b » (28/10/2018) (Cité : Conseil de l'Europe, Resolution (73)22 du 26 septembre 1973).

Conseil de l'Europe, Resolution (74)29 du 20 septembre 1974 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 1974, p. « https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804cd7a9 » (31/05/2017) (Cité : Conseil de l'Europe, Resolution (74)29 du 20 septembre 1974).

Conseil de l'UE, Compatibilité avec les droits fondamentaux : Lignes directrices à l'intention des instances préparatoires du Conseil, in : Conseil de l'UE (https://www.consilium.europa.eu/), Bruxelles 2015, p. « https://www.consilium.europa.eu/media/30208/qc0214079frn.pdf » (23/12/2019) (Cité : Conseil de l'UE, Compatibilité avec les droits fondamentaux).

Conseil de l'UE, Conclusions du Conseil sur le rapport 2013 de la Commission sur l'application de la Charte des droits fondamentaux de l'UE et sur la cohérence entre les aspects internes et externes de la protection et de la promotion des droits de l'homme dans l'Union européenne, in : Conseil de l'UE (https://www.consilium.europa.eu/), Bruxelles 2014, p. « https://www.consilium.europa.eu/media/28080/143100.pdf » (23/12/2019) (Cité : Conseil de l'UE, Conclusions du Conseil sur le rapport 2013 de la Commission).

Conseil de l'UE, Décision 7920/16 du 14 avril 2016 - Dossier interinstitutionnel (2012/0011 (COD)), in : EUR-Lex (https://eur-lex.

europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CONSIL:ST_7920_2016_INIT » (04/04/2020) (Cité : Conseil de l'UE, Décision 7920/16 du 14 avril 2016).

Conseil de l'UE, Déclaration conjointe UE-États-Unis à l'issue de la réunion ministérielle UE-États-Unis consacrée à la justice et aux affaires intérieures - Communiqués de presse du 19 juin 2019, in : Conseil de l'UE (https://www.consilium.europa.eu/), Bruxelles 2019, p. « https://www.consilium.europa.eu/fr/press/press-releases/2019/06/19/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/ » (09/12/2019) (Cité : Conseil de l'UE, Déclaration conjointe UE-États-Unis à l'issue de la réunion ministérielle UE-États-Unis consacrée à la justice et aux affaires intérieures).

Conseil de l'UE, Le Conseil donne mandat à la Commission pour négocier des accords internationaux concernant les preuves électroniques en matière pénale - Communiqués de presse du 6 juin 2019, in : Conseil de l'UE (https://www.consilium.europa.eu/), Bruxelles 2019, p. « https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/ » (09/12/2019) (Cité : Conseil de l'UE, Le Conseil donne mandat à la Commission pour négocier des accords internationaux concernant les preuves électroniques en matière pénale).

Conseil de l'UE, Recommandations sur la protection des données du 8 mars 2019, in : Dossier interinstitutionnel : 2019/0024(NLE) - SCH-EVAL 50, DATAPROTECT 84, COMIX 148, Bruxelles 2019, pp. 1-8 (Cité : Conseil de l'UE, Recommandations sur la protection des données du 8 mars 2019).

Delvaux Mady, Rise of the robots : Mady Delvaux on why their use should be regulated, in : European Parliament News (http://www.europarl.europa.eu/), Brussels 2017, p. « http://www.europarl.europa.eu/news/en/headlines/economy/20170109STO57505/rise-of-the-robots-mady-delvaux-on-why-their-use-should-be-regulated » (27/10/2018) (Cité : Delvaux, Rise of the robots).

Directorate-General for Research and Innovation, Horizon 2020 Programme - Guidance - How to complete your ethics self-

assessment, in : European Commission (https://ec.europa.eu/), Brussels 2019, p. « https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf » (22/12/2019) (Cité : Directorate-General for Research and Innovation, How to complete your ethics self - assessment).

EDPB, EU-U.S. Privacy Shield : Second Annual Joint Review report - Adopted on 22 January 2019, in : EDPB (https://edpb.europa.eu/), Brussels 2019, p. « https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf » (31/03/2020) (Cité : EDPB, EU-U.S. Privacy Shield : Second Annual Joint Review report).

EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Adopted on 12 November 2019, in : EDPB (https://edpb.europa.eu/), Brussels 2019, p. « https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf » (04/04/2020) (Cité : EDPB, Guidelines on the territorial scope of the GDPR (Article 3)).

EDPB, Onzième séance plénière : lignes directrices sur les codes de conduite, annexe des lignes directrices sur l'agrément, annexe des lignes directrices sur la certification, in : EDPB (https://edpb.europa.eu/), Bruxelles 2019, p. « https://edpb.europa.eu/news/news/2019/european-data-protection-board-eleventh-plenary-session-guidelines-codes-conduct_fr » (06/07/2019) (Cité : EDPB, Onzième séance plénière).

EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data, in : EDPS (https://edps.europa.eu/), Brussels 2017, p. « https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf » (24/04/2017) (Cité : EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data).

EDPS, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, in : EDPS (https://edps.europa.eu/), Brussels 2019, p. « https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf » (23/03/2020) (Cité : EDPS, EDPS Guidelines on assessing the proportionality).

EDPS, Introduction to the hash function as a personal data pseudonymisation technique, in : EDPS (https://edps.europa.eu/), Brussels 2019, p. « https://edps.europa.eu/node/5553 » (30/12/2019) (Cité : EDPS, Introduction to the hash function).

EDPS, Position paper on the role of Data Protection Officers of the EU institutions and bodies, in : EDPS (https://edps.europa.eu/), Brussels 2018, p. « https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf » (16/12/2019) (Cité : EDPS, Position paper on the role of Data Protection Officers).

European Commission, Communication on Building a European Data Economy, in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy » (23/10/2017) (Cité : European Commission, Communication on Building a European Data Economy).

European Commission, Guide : EU-US Privacy Shield, in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf » (31/03/2020) (Cité : European Commission, Guide : EU-US Privacy Shield).

European Commission, Impact Assessment Report : Damages actions for breach of the EU antitrust rules. Accompanying the proposal for directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (COM(2013) 404 final / SWD(2013) 204 final), in : EUR-Lex (https://eur-lex.europa.eu/), Brussels 2013, p. « https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0203 » (03/04/2020) (Cité : European Commission, Impact Assessment Report : Damages actions for breach of the EU antitrust rules).

European Commission, Proposal for a Regulation on Privacy and Electronic Communications, in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications » (26/03/2020) (Cité : European Commission, Proposal for a Regulation on Privacy and Electronic Communications).

European Commission, Proposal of 13 September 2017 for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017) 495 final), in : European Commission (https://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF » (23/10/2017) (Cité : European Commission, Proposal of 13 September 2017 for a Regulation of the European Parliament and of the Council).

European Commission, Stronger data protection rules for Europe, in : European Commission (https://ec.europa.eu/), Luxembourg 2015, p. « https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_5170 » (22/05/2019) (Cité : European Commission, Stronger data protection rules for Europe).

European Commission, Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive, in : European Commission (https://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive » (04/07/2016) (Cité : European Commission, Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive).

Groupe de Travail de l'Article 29, Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE - Adopté le 30 mai 2002 (WP 56), in : CNPD (https://cnpd.public.lu/), Luxembourg 2002, p. « https://cnpd.public.lu/dam-assets/fr/dossiers-thematiques/nouvelles-tech-communication/cybersurveillance-lieu-travail/wp56_fr_pdf.pdf » (03/04/2020) (Cité : Groupe de Travail de l'Article 29, Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE).

Groupe de Travail de l'Article 29, Avis 03/2010 du Groupe de travail de l'Art. 29 sur le principe de la responsabilité - Adopté le 13 juillet 2010 (WP 173), in : CNPD (https://cnpd.public.lu/), Luxembourg 2010, p. « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp173_fr.pdf » (25/03/2020) (Cité : Groupe

de Travail de l'Article 29, Avis 03/2010 du Groupe de travail de l'Art. 29).

Groupe de Travail de l'Article 29, Avis 8/2010 du Groupe de travail de l'Art. 29 sur le droit applicable - Adopté le 16 décembre 2010 (WP 179), in : CNPD (https://cnpd.public.lu/), Luxembourg 2010, p. « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp179_fr.pdf » (04/04/2020) (Cité : Groupe de Travail de l'Article 29, Avis 8/2010 du Groupe de travail de l'Art. 29).

Groupe de Travail de l'Article 29, Avis 15/2011 du Groupe de travail de l'Art. 29 sur la définition du consentement - Adopté le 13 juillet 2011 (WP 187), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2011, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf » (26/03/2020) (Cité : Groupe de Travail de l'Article 29, Avis 15/2011 du Groupe de travail de l'Art. 29).

Groupe de Travail de l'Article 29, Avis 05/2014 du Groupe de travail de l'Art. 29 sur les Techniques d'anonymisation - Adopté le 10 avril 2014 (WP 216), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2014, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf » (11/03/2019) (Cité : Groupe de Travail de l'Article 29, Avis 05/2014 du Groupe de travail de l'Art. 29).

Groupe de Travail de l'Article 29, Avis 06/2014 du Groupe de travail de l'Art. 29 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE - Adopté le 9 avril 2014 (WP 217), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2014, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf » (31/12/2019) (Cité : Groupe de Travail de l'Article 29, Avis 06/2014 du Groupe de travail de l'Art. 29).

Groupe de Travail de l'Article 29, Critères de références pour l'adéquation - Adoptés le 28 novembre 2017, Version révisée et adoptée le 6 février 2018 (WP 254 rev.01), in : Commission européenne (https://ec.europa.eu/), Bruxelles 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 » (01/04/2020) (Cité : Groupe de Travail de l'Article 29, Critères

de références pour l'adéquation).

Groupe de Travail de l'Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant - Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017 (WP 244 rev.01), in : CNIL (https://www.cnil.fr/), Paris 2016, p. « https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf » (31/03/2020) (Cité : Groupe de Travail de l'Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant).

Groupe de Travail de l'Article 29, Lignes directrices sur la portabilité des données - Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017 (WP 242 rev.01), in : CNIL (https://www.cnil.fr/), Paris 2016, p. « https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf » (29/12/2019) (Cité : Groupe de Travail de l'Article 29, Lignes directrices sur la portabilité des données).

High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, in : European Commission (https://ec.europa.eu/), Brussels 2019, p. « https://ec.europa.eu/futurium/en/ai-alliance-consultation » (21/06/2019) (Cité : High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI).

Le contrôleur européen de la protection des données, Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » (2011/C 181/01), in : Journal officiel de l'Union européenne (https://edps.europa.eu/), Bruxelles 2011, p. « https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_fr.pdf » (07/03/2019) (Cité : Le contrôleur européen de la protection des données, Avis du contrôleur européen de la protection des données).

Milt Kristiina, La protection des données à caractère personnel, in : Fiches techniques sur l'Union européenne (http://www.europarl.europa.eu/), Bruxelles 2019, p. « http://www.europarl.europa.eu/ftu/pdf/fr/FTU_4.2.8.pdf » (22/05/2019) (Cité : Milt, La

protection des données à caractère personnel).

Moraes Claude, Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (A7-0139/2014), in : Parlement européen (http://www.europarl.europa.eu/), Bruxelles 2014, p. « http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//FR » (27/10/2018) (Cité : Moraes, Rapport sur le programme de surveillance de la NSA).

Parlement européen, Annexe VI relative aux compétences des commissions parlementaires permanentes, XVII Commission des libertés civiles, de la justice et des affaires intérieures, in : Règlement intérieur du Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2019, p. « https://www.europarl.europa.eu/doceo/document/lastrules/RESP-LIBE_FR.html » (05/12/2019) (Cité : Parlement européen, Annexe VI relative aux compétences des commissions parlementaires permanentes, XVII Commission des libertés civiles, de la justice et des affaires intérieures).

Parlement européen, Bouclier « vie privée » UE-États-Unis : des améliorations à apporter-Communiqué de presse du 26 mai 2016, in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2016, p. « https://www.europarl.europa.eu/news/fr/press-room/20160524IPR28820/bouclier-vie-privee-ue-etats-unis-des-ameliorations-a-apporter » (09/10/2017) (Cité : Parlement européen, Bouclier « vie privée » UE-États-Unis : des améliorations à apporter).

Parlement européen, Le Parlement européen soulève des questions éthiques sur les robots et l'intelligence artificielle, in : Parlement européen - Multimedia Center (https://multimedia.europarl.europa.eu/), Bruxelles 2017, p. « https://multimedia.europarl.europa.eu/fr/european-parliament-raises-ethical-questions-on-robots-and-artificial-intelligence_NB01-PUB-170111INT_ev » (27/10/2018) (Cité : Parlement européen, Le Parlement européen soulève des questions éthiques sur les robots et l'intelligence artificielle).

Parlement européen, Programme de surveillance de la NSA, organismes de surveillance dans divers États membres et incidences

sur les droits fondamentaux des citoyens européens, débat du 11 mars 2014, in : Parlement européen (http://www.europarl.europa.eu/), Bruxelles 2014, p. « http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-014&language=FR&ring=A7-2014-0139 » (27/10/2018) (Cité : Parlement européen, Programme de surveillance de la NSA).

Parlement européen, Projet de rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)) du 31 mai 2016, in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2016, p. « https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_FR.pdf?redirect » (29/12/2019) (Cité : Parlement européen, Projet de rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015 / 2103 (INL))).

Parlement européen, Rapport (A7-0402/2013) du 22 novembre 2013 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2013, p. « https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//FR » (29/10/2018) (Cité : Parlement européen, Rapport (A7-0402/2013) du 22 novembre 2013).

Parlement européen, Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2017, p. « https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_FR.html?redirect » (21/03/2020) (Cité : Parlement européen, Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))).

Parlement européen, Résolution du 15 décembre 2010 sur la situation des droits fondamentaux dans l'Union européenne - Aspects institutionnels à la suite de l'entrée en vigueur du Traité de Lisbonne (2009/2161(INI)), in : Parlement européen (https://www.europarl.europa.eu/), Bruxelles 2010, p. « https://www.europarl.eur

opa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0483+0+DOC+XML+V0//FR » (10/12/2019) (Cité : Parlement européen, Résolution du 15 décembre 2010).

Parlement européen, Robots : les députés de la commission des affaires juridiques demandent des règles européennes, in : Parlement européen Actualité (http://www.europarl.europa.eu/), Bruxelles 2017, p. « https://www.europarl.europa.eu/news/fr/press-room/20170110IPR57613/robots-vers-des-regles-europeennes » (22/03/2020) (Cité : Parlement européen, Robots).

Parlement européen, Robots et intelligence artificielle : les députés demandent des règles européennes en matière de responsabilité, in : Parlement européen Actualité (http://www.europarl.europa.eu/), Bruxelles 2017, p. « http://www.europarl.europa.eu/news/fr/press-room/20170210IPR61808/robots-les-deputes-veulent-des-regles-europeennes-en-matiere-de-responsabilite » (30/10/2017) (Cité : Parlement européen, Robots et intelligence artificielle).

Parlement européen et Conseil de l'UE, Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 1995, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046 » (04/07/2017) (Cité : Parlement européen et Conseil de l'UE, Directive 95/46/CE du 24 octobre 1995).

Parlement européen et Conseil de l'UE, Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2000, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32000L0031 » (01/10/2017) (Cité : Parlement européen et Conseil de l'UE, Directive 2000/31/CE du 8 juin 2000).

Parlement européen et Conseil de l'UE, Directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2002, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF

/?uri=CELEX:32002L0021 » (27/03/2020) (Cité : Parlement européen et Conseil de l'UE, Directive 2002/21/CE du 7 mars 2002).

Parlement européen et Conseil de l'UE, Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2002, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002L0058 » (04/07/2017) (Cité : Parlement européen et Conseil de l'UE, Directive 2002/58/CE du 12 juillet 2002).

Parlement européen et Conseil de l'UE, Directive 2006/24/CE du 13 avril 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2006, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32006L0024 » (09/12/2019) (Cité : Parlement européen et Conseil de l'UE, Directive 2006/24/CE du 13 avril 2006).

Parlement européen et Conseil de l'UE, Directive (EU) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le Règlement (UE) no. 1093/2010, et abrogeant la directive 2007/64/CE, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2015, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32015L2366 » (09/12/2019) (Cité : Parlement européen et Conseil de l'UE, Directive (EU) 2015/2366 du 25 novembre 2015).

Parlement européen et Conseil de l'UE, Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles

2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680 » (01/04/2020) (Cité : Parlement européen et Conseil de l'UE, Directive (UE) 2016/680 du 27 avril 2016).

Parlement européen et Conseil de l'UE, Règlement (CE) 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2001, p. « https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF » (25/10/2017) (Cité : Parlement européen et Conseil de l'UE, Règlement (CE) 45/2001 du 18 décembre 2000).

Parlement européen et Conseil de l'UE, Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679 » (18/06/2018) (Cité : Parlement européen et Conseil de l'UE, Règlement (UE) 2016/679 du 27 avril 2016).

Parlement européen et Conseil de l'UE, Règlement (UE) 2018 / 1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (Texte présentant de l'intérêt pour l'EEE), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2018, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1807 » (07/12/2019) (Cité : Parlement européen et Conseil de l'UE, Règlement (UE) 2018/1807 du 14 novembre 2018).

Poullet Yves / Frenay Benoît, Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe » (T-PD (2019) 07), in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 2019, p. « https://rm.coe.int/rapport-et-propositions-de-recommandations-sur-le-profilage-et-la-conv/1680973672 » (07/12/2019) (Cité : Poullet / Frenay, « Profilage et la Convention 108+ du Conseil de l'Europe »).

Rouvroy Antoinette, « Des données et des hommes », droits et

libertés fondamentaux dans un monde de données massives (T-PD-BUR (2015) 09REV), in : Conseil de l'Europe (https://www.coe.int/), Strasbourg 2016, p. « https://rm.coe.int/16806b1659 » (26/03/2020) (Cité : Rouvroy, « Des données et des hommes »).

Saugmandsgaard Henrik, Conclusions de l'avocat général dans l'affaire C-311/18 Facebook Ireland et Schrems - Communiqué de presse de la CJUE du 19 décembre 2019, No. 165/2019, in : CJUE (https://curia.europa.eu/), Luxembourg 2019, p. « https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165fr.pdf » (31/03/2020) (Cité : Saugmandsgaard, Conclusions de l'avocat général dans l'affaire C-311/18 Facebook Ireland et Schrems).

STOA, Blockchain and the General Data Protection Regulation, in : European Parliament (https://www.europarl.europa.eu/), Brussels 2019, p. « https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019/634445 » (06/08/2019) (Cité : STOA, Blockchain and the General Data Protection Regulation).

Union européenne, Charte des droits fondamentaux de l'Union européenne (2012/C 326/02), in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2012, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:12012P/TXT » (27/10/ 2018) (Cité : Union européenne, Charte des droits fondamentaux de l'Union européenne).

Union européenne, Traité sur le fonctionnement de l'Union Européenne du 26 octobre 2012, C 326/ 49 - Journal officiel de l'Union européenne, in : EUR-Lex (https://eur-lex.europa.eu/), Bruxelles 2012, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012E/TXT » (02/04/2019) (Cité : Union européenne, Traité sur le fonctionnement de l'Union Européenne du 26 octobre 2012).

Wiewiórowski Wojciech, Preparing DPOs to lead by example : DPO-EDPS meeting in Tallinn, in : EDPS (https://edps.europa.eu/), Brussels 2017, p. « https://edps.europa.eu/node/4221 » (23/06/2017) (Cité : Wiewiórowski, Preparing DPOs to lead by example).

Droit international

Assemblée générale des Nations-Unies, Résolution 3281 (XXIX) du 12 décembre 1974 (29ème session) - Charte des droits et de-

voirs économiques es Etats, in : Nations-Unies (https://undocs.org/), Genève 1974, p. « https://undocs.org/fr/A/RES/3281(XXIX/ » (04/04/2020) (Cité : Assemblée générale des Nations-Unies, Résolution 3281 du 12 décembre 1974 (29ème session)).

CIISE, La Responsabilité de Protéger - Rapport de la commission internationale de l'intervention et de la souveraineté (Décembre 2001), in : Centre de recherches pour le développement international, Ottawa 2001, pp. 1-120 (Cité : CIISE, La Responsabilité de Protéger).

CNUDCI, Loi type de la CNUDCI sur le commerce électronique (1996) avec article 5 bis tel qu'ajouté en 1998 - Adopté le 12 juin 1996 (le nouvel article 5 bis a été adopté en 1998), in : CNUDCI (https://uncitral.un.org/), Vienne 1996, p. « https://uncitral.un.org/fr/texts/ecommerce/modellaw/electronic_commerce » (29/03/2020) (Cité : CNUDCI, Loi type de la CNUDCI sur le commerce électronique (1996) avec article 5 bis tel qu'ajouté en 1998).

Committee of Experts on International Cooperation in Tax Matters, The digitalized economy : selected issues of potential relevance to developing countries (E/C. 18/2017/6), in : United Nations Economic and Social Council (Fifteenth Session), Geneva 2017, pp. 1-5 (Cité : Committee of Experts on International Cooperation in Tax Matters, The digitalized economy).

Delmas-Marty Mireille, International Law - Legal Theory (Lecture), in : UN Audiovisual Library of International Law (https://legal.un.org/), Geneva s.a., p. « https://legal.un.org/avl/ls/Delmas-Marty_IL.html » (28/12/2019) (Cité : Delmas-Marty, International Law).

Nations Unies / Commission pour le droit commercial international, *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*, New York 2002 (Cité : Nations Unies / Commission pour le droit commercial international, *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*).

OCDE, Echange de renseignements, in : OCDE (https://www.oecd.org/), Paris s.a., p. « https://www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/ » (04/01/2020) (Cité : OCDE, Echange

de renseignements).

OECD, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, in : OECD (https://www.oecd.org/), Paris s.a., p. « https://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectionde laviepriveeetlesfluxtransfrontieresdedonneesdecaractereperson nel.htm » (17/04/2017) (Cité : OECD, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel).

OECD, OECD Principles on AI, in : OECD (https://www.oecd.org/), Paris s.a., p. « https://www.oecd.org/going-digital/ai/principles/ » (08/06/2019) (Cité : OECD, OECD Principles on AI).

United Nations, Disarmament in Geneva, in : United Nations (https://www.un.org/), Geneva s.a., p. « https://www.un.org/disarmament/geneva/ccw/background-on-lethal-autonomous-weapons-systems/ » (29/09/2017) (Cité : United Nations, Disarmament in Geneva).

United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows : Implications for Trade and Development, in : UNCTAD (https://unctad.org/), New York 2016, p. « https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf » (27/10/2018) (Cité : United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows).

Droit français

Conseil national des barreaux (France), *Guide pratique : les avocats et le règlement général sur la protection des données (RGPD)*, 1e éd., Issy-les-Moulineaux 2018 (Cité : Conseil national des barreaux (France), *Guide pratique*).

CNIL, Conformité RGPD : comment recueillir le consentement des personnes ?, in : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr/), Paris 2018, p. « https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes » (01/01/2020) (Cité : CNIL, Conformité RGPD).

CNIL, La formation restreinte de la CNIL prononce une sanction de

50 millions d'euros à l'encontre de la société GOOGLE LLC, in : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr/), Paris 2019, p. « https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la » (17/06/2019) (Cité : CNIL, La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC).

CNIL, Objects Connectés, in : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr/), Paris 2016, p. « https://www.cnil.fr/fr/thematique/internet-technologies/objets-connectes » (27/10/2018) (Cité : CNIL, Objects Connectés).

CNIL, Smart city et données personnelles : quels enjeux de politiques publiques et de vie privée ?, in : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr/), Paris 2017, p. « https://www.cnil.fr/fr/smart-city-et-donnees-personnelles-quels-enjeux-de-politiques-publiques-et-de-vie-privee » (27/10/2018) (Cité : CNIL, Smart city et données personnelles).

CNIL, Véhicules connectés : un pack de conformité pour une utilisation responsable des données, in : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr/), Paris 2017, p. « https://www.cnil.fr/fr/vehicules-connectes-un-pack-de-conformite-pour-une-utilisation-responsable-des-donnees » (27/10/2018) (Cité : CNIL, Véhicules connectés).

Droit suisse

Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen (RS 0.362.31), FF 2004 p. 5593 ss (Cité : Accord du 26 octobre 2004).

Accord du 9 novembre 2004 entre la Confédération suisse et la Communauté européenne modifiant l'accord entre la Confédération suisse et la Communauté économique européenne du 22 juillet 1972 pour ce qui concerne les dispositions applicables aux produits agricoles transformés, FF 2004 p. 5927 ss (Cité : Accord du 9 novembre 2004 I).

Accord du 9 novembre 2004 entre la Confédération suisse et la

Communauté européenne prévoyant des mesures équivalentes à celles prévues dans la directive 2003/48/CE du Conseil en matière de fiscalité des revenus de l'épargne sous forme de paiements d'intérêts (avec annexes et mémorandum d'entente), FF 2004 p. 6163 ss (Cité : Accord du 9 novembre 2004 II).

Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen (RS 0.362.31), FF 2004 p. 5593 ss (Cité : Accord du 26 octobre 2004).

Conseil fédéral, Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Convention de Lugano, CL) - Conclue à Lugano le 30 octobre 2007 (RS 0.275.12, RO 2010 5609), in : Conseil fédéral (https://www.admin.ch/), Berne 2007, p. « https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html » (04/04/2020) (Cité : Conseil fédéral, Convention de Lugano (RS 0.275.12, RO 2010 5609)).

Conseil fédéral, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1, RO 2002 2847), in : Conseil fédéral (https://www.admin.ch/), Berne 1981, p. « https://www.admin.ch/opc/fr/classified-compilation/20012356/index.html » (16/12/2019) (Cité : Conseil fédéral, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1)).

Conseil fédéral, Dossier de presse de 15 septembre 2017 : Les sanctions dans le projet de révision totale de la loi sur la protection des données, in : DFJP (https://www.ejpd.admin.ch/), Berne 2017, p. « https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/rohstoff-f.pdf » (20/10/2018) (Cité : Conseil fédéral, Dossier de presse de 15 septembre 2017).

Conseil fédéral, Helsana+ : Le jugement entre en force, in : Conseil fédéral (https://www.admin.ch/), Berne 2019, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75039.html » (17/05/2019) (Cité : Conseil fédéral, Helsana+ : Le jugement entre en force).

Conseil fédéral, Le Conseil fédéral signe la nouvelle Convention du Conseil de l'Europe sur la protection des données, in : Conseil fédéral (https://www.admin.ch/), Berne 2019, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76861.html » (22/12/2019) (Cité : Conseil fédéral, Le Conseil fédéral signe la nouvelle Convention du Conseil de l'Europe sur la protection des données).

Conseil fédéral, Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données - Conclu à Strasbourg le 8 novembre 2001 (RS 0.235.11, RO 2008 731), in : Conseil fédéral (https://www.admin.ch/), Berne 2001, p. « https://www.admin.ch/opc/fr/classified-compilation/20022762/index.html » (01/04/2020) (Cité : Conseil fédéral, Protocole additionnel à la Convention pour la protection des personnes (RS 0.235.11, RO 2008 731)).

Conseil fédéral, Renforcer le contrôle sur ses propres données et rendre leur traitement plus transparent, in : Conseil fédéral (https://www.admin.ch/), Berne 2016, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques/communiques-conseil-federal.msg-id-65055.html » (01/11/2019) (Cité : Conseil fédéral, Renforcer le contrôle sur ses propres données et rendre leur traitement plus transparent).

Conseil fédéral, Une meilleure protection des données et un renforcement de l'économie suisse, in : Conseil fédéral (https://www.admin.ch/), Berne 2017, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-68130.html » (24/03/2020) (Cité : Conseil fédéral, Une meilleure protection des données et un renforcement de l'économie suisse).

DAE, La politique européenne de la Suisse, in : Conseil fédéral (https://www.eda.admin.ch/), Berne 2020, p. « https://www.eda.admin.ch/dam/dea/fr/documents/fs/00-FS-Europapol-lang_fr.pdf » (27/03/2020) (Cité : DAE, La politique européenne de la Suisse).

DAE, Politique européenne de la Suisse - Accords et mise en oeuvre, in : Conseil fédéral (https://www.eda.admin.ch/), Berne 2018, p. « https://www.eda.admin.ch/dea/fr/home/bilaterale-abkommen/abkommen-umsetzung.html » (27/03/2020) (Cité : DAE, Accords et mise en oeuvre).

DAE, Politique européenne de la Suisse - Accords bilatéraux II, in : Conseil fédéral (https://www.eda.admin.ch/), Berne 2004, p. « https://www.eda.admin.ch/dea/fr/home/europapolitik/politique-europeenne/bilaterale-2.html » (30/10/2017) (Cité : DAE, Accords bilatéraux II).

DAE, Votation populaire du 5 juin 2005 - Arrêté fédéral portant approbation et mise en oeuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin, in : Conseil fédéral (https://www.eda.admin.ch/), Berne 2005, p. « https://www.eda.admin.ch/dea/fr/home/europapolitik/abstimmungen/schengen-dublin.html » (23/04/2017) (Cité : DAE, Votation populaire du 5 juin 2005).

DFAE, Politique européenne de la Suisse - Accord institutionnel, in : Conseil fédéral (https://www.dfae.admin.ch/), Berne 2019, p. « https://www.dfae.admin.ch/dea/fr/home/verhandlungen-offene-themen/verhandlungen/institutionelles-abkommen.html » (08/06/2019) (Cité : DFAE, Accord institutionnel).

DFAE / DFE, Schengen / Dublin, in : Conseil fédéral (https://www.sem.admin.ch/), Berne 2008, p. « https://www.sem.admin.ch/dam/data/sem/eu/fza/personenfreizuegigkeit/factsheets/2008/081211-fs2-f.pdf » (04/10/2017) (Cité : DFAE / DFE, Schengen / Dublin).

DFJP, Procédure civile : faciliter l'accès aux tribunaux des particuliers et des entreprises - Communiqué du Conseil fédéral du 2 mars 2018, in : DFJP (https://www.ejpd.admin.ch/), Berne 2018, p. « https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2018/2018-03-02.html » (03/04/2020) (Cité : DFJP, Procédure civile).

Loi fédérale sur la protection des données (LPD) du 19 juin 1992, FF 1992 p. 929 ss (Cité : LPD).

Loi sur l'Assemblée fédérale (Loi sur le Parlement, LParl) du 13 décembre 2002 (Etat le 2 décembre 2019), RS 171.10, RO 2003 p. 3543 ss (Cité : Loi sur l'Assemblée fédérale (Loi sur le Parlement, LParl) du 13 décembre 2002).

Message du 28 juin 2006 relatif au code de procédure civile suisse (06.062), FF 2006 p. 6841 ss (Cité : Message du 28 juin 2006).

Message du 3 novembre 2009 relatif à la politique climatique suisse après 2012 (Révision de la loi sur le CO2 et initiative populaire fédérale « pour un climat sain ») (09.067), FF 2009 p. 6723 ss (Cité : Message du 3 novembre 2009).

Message du 15 septembre 2017 concernant la révision totale de la loi fédérale sur la protection des données et sur la modifications d'autres lois fédérales (17.059), FF 2017 p. 6565 ss (Cité : Message du 15 septembre 2017).

Mission de la Suisse auprès de l'Union européenne, Echange de notes entre la Suisse et l'Union européenne du 1er septembre 2016 entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (Développement de l'acquis de Schengen), in : OFJ (https://www.bj.admin.ch/), Berne 2016, p. « https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/notenaustausch-f.pdf » (17/10/2019) (Cité : Mission de la Suisse auprès de l'Union européenne, Echange de notes entre la Suisse et l'Union européenne du 1er septembre 2016 entre la Suisse et l'Union européenne).

OFCOM, Big Data : atouts, risques et mesures nécessaires pour la Confédération, in : Conseil fédéral (https://www.bakom.admin.ch/), Berne 2016, p. « https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/ofcom-infomailing/ofcom-infomailing-40/big-data--atouts--risques-et-mesures-a-prendre-pour-la-confedera.html » (21/03/2020) (Cité : OFCOM, Big Data : atouts, risques et mesures nécessaires pour la Confédération).

OFJ, Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales : Synthèse des résultats de la procédure de consultation (10 août 2017), in : Conseil fédéral (https://www.admin.ch/), Berne 2017, p. « https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Rapport-resultats_fr.pdf » (02/04/2020) (Cité : OFJ, Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données

et sur la modification d'autres lois fédérales).

OFJ, Esquisse d'acte normatif relative à la révision de la loi sur la protection des données : Rapport du groupe d'accompagnement Révision LPD, in : OFJ (https://www.bj.admin.ch/), Berne 2014, p. « https://www.bj.admin.ch/content/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf » (27/06/2019) (Cité : OFJ, Esquisse d'acte normatif relative à la révision de la loi sur la protection des données).

OFJ, Modification du code de procédure civile, in : OFJ (https://www.bj.admin.ch/), Berne s.a., p. « https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/aenderung-zpo.html » (30/06/2019) (Cité : OFJ, Modification du code de procédure civile).

OFJ, Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, in : OFJ (https://www.bj.admin.ch/), Berne 2016, p. « https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-f.pdf » (27/06/2019) (Cité : OFJ, Rapport explicatif du 21 décembre 2016).

OFJ, Renforcement de la protection des données, in : OFJ (https://www.bj.admin.ch/), Berne s.a., p. « https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html » (27/06/2019) (Cité : OFJ, Renforcement de la protection des données).

Parlement suisse, 17.059 : Loi sur la protection des données. Révision totale et modification d'autres lois fédérales - Propositions du Conseil fédéral du 15 septembre 2017, Projet de la Commission des institutions politiques du Conseil national du 16 août 2019, in : Parlement suisse (https://www.parlament.ch/), Berne 2017, p. « https://www.parlament.ch/centers/eparl/curia/2017/20170059/N3-1%20F.pdf » (30/08/2019) (Cité : Parlement suisse, 17.059 : Loi sur la protection des données. Révision totale et modification d'autres lois fédérales).

Parlement suisse, Heure des questions : Question Glättli Balthasar du 11 mars 2019, Renforcer la Suisse en tant que centre de calcul dans le contexte du Cloud Act au moyen d'un accord bilatéral d'entraide judiciaire avec les Etats-Unis, in : Parlement

suisse (https://www.parlament.ch/), Berne 2019, p. « https://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=45404 » (16/12/2019) (Cité : Parlement suisse, Heure des questions : Question Glättli Balthasar du 11 mars 2019).

Parlement suisse, Le Conseil des Etats examinera la loi sur la protection des données á la session d'hiver - Communiqué de presse du 20 novembre 2019, in : Parlement suisse (https://www.parlament.ch/), Berne 2019, p. « https://www.parlament.ch/press-releases/Pages/mm-spk-s-2019-11-20.aspx » (22/12/2019) (Cité : Parlement suisse, Le Conseil des Etats examinera la loi sur la protection des données á la session d'hiver).

Parlement suisse, Législation sur la protection des données : Révision en deux étapes - Communiqué de presse du 12 janvier 2018, in : Parlement suisse (https://www.parlament.ch/), Berne 2018, p. « https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-01-12.aspx?lang=1036 » (01/11/2019) (Cité : Parlement suisse, Législation sur la protection des données).

Parlement suisse, Réforme de la protection des données : fin de l'examen du projet - Communiqué de presse du 16 août 2019, in : Parlement suisse (https://www.parlament.ch/), Berne 2019, p. « https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx?lang=1036 » (22/12/2019) (Cité : Parlement suisse, Réforme de la protection des données).

Parlement suisse, Suppression du Safe Harbor USA-UE en matière de protection des données. Quelles conséquences pour la Suisse ?, in : Parlement suisse (https://www.parlament.ch/), Berne 2015, p. « https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20151068 » (27/10/2018) (Cité : Parlement suisse, Suppression du Safe Harbor USA-UE en matière de protection des données).

PFPDT, 24ème Rapport d'activités sur la protection des données, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/25--taetigkeitsbericht-2017-2018.html » (27/10/2018) (Cité : PFPDT, 24ème Rapport d'activités).

PFPDT, 26e rapport d'activités 2018/2019 : La Suisse doit maintenir

son niveau de protection des données, in : Conseil fédéral (https://www.admin.ch/), Berne 2019, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75448.html » (27/06/2019) (Cité : PFPDT, 26e rapport d'activités 2018/2019).

PFPDT, Arrêt du Tribunal fédéral dans l'affaire Google Street View : Règles en matière de traitement de données personnelles, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2019, p. « https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/services-en-ligne/google-street-view/arret-du-tribunal-federal-dans-laffaire-google-street-view--regl.html » (24/03/2018) (Cité : PFPDT, Arrêt du Tribunal fédéral dans l'affaire Google Street View).

PFPDT, Conseils pratiques concernant le RGPD, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2019, p. « https://www.edoeb.admin.ch/edoeb/fr/home/actualites/rgpd-last-minute.html » (26/03/2020) (Cité : PFPDT, Conseils pratiques concernant le RGPD).

PFPDT, Explications relatives aux capteurs fitness en lien avec les assurances, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/gesundheit/kranken--und-unfallversicherungen/erlaeuterungen-zum-einsatz-von-fitnesstrackern-im-versicherungsb.html » (27/10/2018) (Cité : PFPDT, Explications relatives aux capteurs fitness en lien avec les assurances).

PFPDT, Le RGPD et ses conséquences sur la Suisse, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2018, p. « https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf.download.pdf/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf » (07/12/2019) (Cité : PFPDT, Le RGPD et ses conséquences sur la Suisse).

PFPDT, Message du 15 septembre 2017 concernant la révision totale de la loi fédérale sur la protection des données : appréciation du PFPDT, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news/zur-botschaft-ueber-die-totalrevision-des-datenschutzgesetzes-de.html » (02/04/2020) (Cité : PFPDT, Message du 15 septembre 2017 concernant la révision totale de la loi

fédérale sur la protection des données).

PFPDT, Swiss-US Privacy Shield : un nouveau cadre pour la transmission des données aux États-Unis, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa/swiss-us-privacy-shield--neuer-rahmen-fuer-datenuebermittlungen-.html » (27/10/2018) (Cité : PFPDT, Swiss-US Privacy Shield).

PFPDT, Vidéosurveillance par des drones dans le domaine privé, in : Conseil fédéral (https://www.edoeb.admin.ch/), Berne s.a., p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/technologien/videoueberwachung/videoueberwachung-mit-drohnen-durch-private/videoueberwachung-mit-drohnen-durch-private.html » (27/10/2018) (Cité : PFPDT, Vidéosurveillance par des drones dans le domaine privé).

Republique et Canton de Genève, Le principe de transparence dans l'administration : Évaluation des dispositions légales concernant l'accès aux documents et l'information du public (LIPAD), in : Cour des Comptes (http://www.cdc-ge.ch/), Genève 2009, p. « http://www.cdc-ge.ch/fr/Publications/Archives-CEPP/Liste-des-rapports-d-evaluation/Principe-de-transparence-dans-l-administration-LIPAD.html » (01/04/2020) (Cité : Republique et Canton de Genève, Évaluation des dispositions légales concernant l'accès aux documents et l'information du public (LIPAD)).

Tribunal fédéral, Communiqué de presse du TF du 5 avril 2017, en lien avec l'arrêt du 17 mars 2017 (2C_1000/2015), in : Tribunal fédéral (https://www.bger.ch/), Lausanne 2017, p. « https://www.bger.ch/files/live/sites/bger/files/pdf/fr/2C_1000_2015_2017_04_05_T_f_09_47_53.pdf » (03/12/2018) (Cité : Tribunal fédéral, Communiqué de presse du TF).

Table des illustrations

2.1 Processus d'élaboration des politiques européennes. (Source : « https://royalsociety.org/ ».) 31
2.2 Exemples de systèmes autonomes. 60
2.3 Les différents niveaux d'autonomie des véhicules autonomes tels que définis par la "Society of Automotive Engineers". Source : Université de Birmingham. 63
2.4 Données collectées par les voitures autonomes. 72
2.5 Véhicule connecté, usages et capteurs. Source : CNIL. . 72
2.6 Description du fonctionnement de la technologie Blockchain. Source : Blockchain France (2016). 96
2.7 Exemple d'une transaction entre deux personnes. Source : Livre blanc sur la Blockchain, Juin 2017. 98
2.8 Schéma synoptique de l'informatique en nuage. Source : Wikipedia. 105
2.9 Périmètre et applications les plus connues de l'IA. Source : Medium.com. 123
2.10 Analogie entre le cycle de la chaîne alimentaire et la transparence des algorithmes. 125

Introduction

§1 Le thème

Sous le titre « le Règlement général sur la protection des données et son impact en droit suisse », cette étude propose d'analyser le régime et les effets, en droit suisse, de ce texte particulier, entré en vigueur le 25 mai 2016, applicable directement le 25 mai 2018, qui s'inscrit dans une réforme européenne de la protection des données. 1

La notion de protection des données se rencontre dans des contextes juridiques divers. Elle existe non seulement en droit privé mais également en droit public. Elle est consacrée comme un droit fondamental par la Constitution suisse (cf. art. 13 al. 2 Cst.). 2

Au niveau du droit international, elle est garantie par l'article 8 de la Convention européenne des droits de l'homme via le droit au respect de la vie privée et familiale. Au niveau du droit de l'Union, un droit fondamental à la protection des données à caractère personnel a été consacré, pour la première fois, avec la Charte des droits fondamentaux de l'Union (ci-après « la Charte ») proclamée à Nice le 7 décembre 2000 et désormais dotée d'une valeur juridique contraignante au même titre que les Traités, depuis le 1er décembre 2009, du fait de l'entrée en vigueur du Traité de Lisbonne. L'article 8 de la Charte garantit ce droit et le distingue du droit au respect de la vie privée et familiale, visé à l'article 7 de la Charte. 3

La directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, fait également partie de la réforme européenne en matière de protection des données [1]. 4

Le contexte de la présente étude n'est pas aussi vaste : 5

Nous limiterons notre analyse à l'impact extra-territorial du Règlement général en matière de protection des données. La directive 6

1. Voir point 120 de ce document.

(UE) 2016/680 est exclue de cette étude.

7 Nous nous concentrerons sur l'impact du Règlement général en matière de protection des données pour les entreprises suisses concernées par le Règlement, à l'exclusion des administrations publiques.

8 Nous examinerons le projet de révision totale de la loi fédérale sur la protection des données, à l'exclusion de la loi actuelle suisse en matière de protection des données.

9 Nous nous en tiendrons à l'analyse du droit suisse, même si quelques références sont faites aux droits européen, américain et coréen.

§2 L'intérêt du thème

10 Ce thème présente tout d'abord un intérêt théorique. Il soulève la question de la place que peut ou doit occuper le contrôle *a posteriori* par le biais de l'action civile en droit de la protection des données. En Europe, le Règlement général sur la protection des données marque une nette volonté d'encourager l'action civile, à titre individuel ou collectif, afin de responsabiliser les responsables du traitement et les sous-traitants, de sanctionner les comportements fautifs ou négligents et de garantir la réparation des dommages subis par les personnes concernées, en cas de violation des dispositions du Règlement.

11 Le droit de la protection des données est de manière inhérente un droit á portée économique, guidé par des considérations économiques [2]. Le Règlement en est une illustration : il renonce au mécanisme d'autorisation préalable à tout traitement de données personnelles, pour favoriser la libre circulation des données personnelles au sein de l'Union européenne afin de soutenir la création d'un marché unique des données et faciliter l'innovation technologique. Il instaure un contrôle de légalité *a posteriori* qui repose sur des principes généraux et un standard of « due care » pour les responsables du traitement. Il offre des garanties aux utilisateurs (ci-après « personnes concernées ») dont les données sont traitées en reconnaissant le droit de former des actions collectives en responsabilité (« *class action* »), ce qui constitue une innovation majeure

2. Hurni Béatrice, *L'action civile en droit de la concurrence : étude du droit suisse à la lumière du droit comparé et du droit de l'Union européenne*, thèse, Fribourg 2017, p. 57.

dont la Suisse pourrait s'inspirer.

Cette thèse va s'intéresser à la généralisation du contrôle a posteriori par le Règlement, avec transformation des autorités de protection des données personnelles en autorité de contrôle a posteriori. Ce changement externe et visible correspond à une transformation profonde de la nature du droit de la protection des données personnelles, tel qu'il est mis en place comme droit positif européen par le Règlement : ce droit positif européen de la protection des données personnelles devient un droit de nature essentiellement économique, comme le droit antitrust, qu'il complète désormais. Ce droit approche en effet la circulation des données personnelles dans le même esprit que le droit de la concurrence approche la libre circulation des personnes, des capitaux, des marchandises, etc., mais alors que le droit antitrust se concentre sur le coût trop élevé (en terme de prix des services ou des marchandises) en raison de certaines pratiques critiquables (pratiques cartellaires, par exemple), le droit de la protection des données se concentre sur le coût trop élevé (en terme d'atteinte à la sphère privée) de certaines pratiques des responsables de traitement (toutes celles qui ne sont pas conformes au Règlement). 12

La présente étude propose de reprendre le débat sur la protection des données dans le contexte technologique de l'ère digitale pour évaluer l'impact du Règlement général sur la protection des données en Europe et en Suisse. 13

Après quatre années de négociations, les États membres de l'Union européenne sont convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995. Intitulé « Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », le Règlement général sur la protection des données est un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants. 14

Contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril 2016, par le Parlement européen, et publié au J.O. de l'Union Européenne le 4 mai 2016 est d'application directe. Entré en vigueur le 25 mai 2016, il est entré en application le 25 mai 2018. Il est obligatoire dans tous ses éléments 15

et directement applicable dans tout État membre. Il n'a pas besoin d'être transposé dans les législations nationales. L'adoption du Règlement européen sur la protection des données personnelles permet, dans toute l'Union, l'application et l'interprétation d'un seul texte. Il s'agit d'un instrument d'intégration puissant pour l'Union et de sécurité juridique, donc de stabilité propice au développement économique pour les entreprises. La directive 1995/46/CE présentait en effet l'inconvénient de créer des lois nationales différentes au sein de l'Union européenne.

16 Le Règlement a pour objectif déclaré de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles (considérant n°7 du Règlement) [3], tout en simplifiant, en l'unifiant, la réglementation pour les entreprises. Augmenter le niveau de responsabilité des « responsables du traitement (administrations, entreprises, organisations, etc.) » et leurs pouvoirs de contrôle, afin de créer un climat de confiance essentiel au développement de l'économie digitale, accroître la cohérence des réglementations nationales tout en continuant à inscrire la protection des données dans le cadre plus large du respect des droits fondamentaux, telles furent les priorités du législateur [4]. Les citoyens de l'UE pourront désormais recourir à l'action civile en droit de la protection des données pour ouvrir une action en responsabilité civile afin d'obtenir réparation du dommage causé par une pratique non-conforme à la protection des données personnelles.

17 La mise en œuvre du droit de la protection des données est en principe considérée comme une tâche des autorités publiques.

18 Le Règlement transforme cependant les autorités européennes dédiées à la protection des données en autorités de contrôle, au moyen de la généralisation du contrôle *a posteriori*.

19 Le Règlement introduit la possibilité d'une action publique ouverte par les autorités nationales compétentes en matière de protection des données et autorise de surcroît l'action privée, ce qui présente un intérêt théorique certain.

20 Le Règlement introduit donc la notion américaine de Private En-

3. González Fuster Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 1e éd., Cham 2014, p. 242.
4. Docquir Benjamin (édit.), *Vers un droit européen de la protection des données ?*, 1e éd., Bruxelles 2017, p. 8.

forcement en droit européen de la protection des données.

Plus précisément, avec le Règlement, la personne concernée a désormais le double droit d'introduire une réclamation auprès d'une autorité de contrôle (art. 77 RGPD) et de former un recours juridictionnel effectif à l'encontre de l'entreprise détentrice des données personnelles ou de son sous-traitant. L'action en responsabilité impose à l'auteur du dommage de démontrer qu'il s'est comporté de manière responsable, de cesser le comportement illicite qui a lésé autrui et expose le responsable du traitement à des sanctions financières, administratives ou pénales dissuasives. 21

L'action en responsabilité a pour objet d'établir si une personne particulière, l'auteur du dommage, en est responsable. L'auteur du dommage est confronté à une obligation de réparer le dommage. En ce sens, l'action en responsabilité est rattachée à la notion de justice corrective. 22

Outil de réparation des dommages, l'action civile rend possible la mise en œuvre effective du droit de la protection des données. Par conséquent, il serait opportun de faciliter l'ouverture d'actions civiles en Suisse afin de renforcer l'effectivité des règles de la protection des données. 23

En Europe, les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives. En Suisse, le Conseil fédéral a amorcé la révision du code de procédure civile pour autoriser les actions de groupes. 24

Pour faire valoir ses droits, en application du Règlement, le demandeur doit établir l'existence d'une infraction aux règles de la protection des données, de la même manière que le fait l'autorité administrative. Il invoquera donc le droit de la protection des données, à l'appui de ses prétentions privées. 25

Le droit de la protection des données revêt une importante dimension politique. Instrument de politique publique, il a la capacité d'impacter les traitements de données personnelles des acteurs économiques, ainsi de freiner ou bien de stimuler l'innovation et l'activité économique d'un pays. 26

Compte tenu des enjeux, le législateur doit effectuer une pesée des intérêts en présence : recherche la compétitivité des entreprises na- 27

tionales tout en maintenant l'Etat de droit.

28 Le droit de la protection des données doit en effet tenir compte d'impératifs juridiques en lien avec la protection des libertés fondamentales et des droits de la personnalité des personnes concernées, comme celui de l'autodétermination informationnelle et de la protection de la sphère privée.

29 Cette étude revêt ensuite un intérêt pratique.

30 Le Règlement introduit un changement de paradigme visant à instaurer une véritable culture de la protection des données en Europe.

31 Ce changement de paradigme s'exprime par de nouvelles règles de droit dans le domaine de la protection des données à caractère personnel. Ces modifications ont des conséquences pratiques non négligeables pour la plupart des entreprises et des organisations européennes. Celles-ci doivent mettre en place une véritable gouvernance des données personnelles et définir des processus spécifiques pour se conformer aux obligations du Règlement.

32 La mise en œuvre d'une gouvernance des données s'inscrit dans une préoccupation de même nature que la protection de l'environnement et constitue un des éléments de la responsabilité sociale des entreprises [5].

33 Le Règlement est inspiré par la volonté de faire prendre conscience aux entreprises et organisations qui traitent des données à caractère personnel, de leurs devoirs envers les personnes concernées dont les données sont collectées. A défaut de prise de conscience, il prévoit des sanctions strictes.

34 La Suisse est concernée indirectement par la mise en œuvre du Règlement. Elle ne fait pas partie de l'Union européenne et le Règlement n'est en principe pas directement applicable aux traitements de données personnelles de manière générale en Suisse. Le Règlement ne fait en effet pas partie du droit positif en Suisse.

35 Seuls les traitements de données à caractère personnel qui remplissent les conditions de l'article 3 al. 2 RGPD sont en effet soumis

5. GROSJEAN Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, pp. 373-378 ; MOEREL Lokke, *Binding Corporate Rules : Corporate Self-Regulation of Global Data Transfers*, Oxford 2012, pp. 175-227.

au Règlement.

Il s'agit des traitements de données à caractère personnel relatifs « à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : 36

1. à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non ;
2. au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Le Règlement vise à instaurer une égalité de traitement entre les entreprises de l'UE et les entreprises étrangères traitant des données personnelles de citoyens européennes dans l'Union européenne. 37

Sur le plan international, le caractère extra-territorial du Règlement incite les États non-membres de l'Union Européenne, comme la Suisse, le Royaume-Uni (post- Brexit), les pays d'Asie, d'Amérique latine ou d'Afrique, à modifier leur législation sur la protection des données personnelles ou à adopter de nouvelles législations. L'enjeu est triple pour les États et les entreprises : 38

— maintenir la licéité des transferts de données personnelles avec l'UE, condition d'une libre circulation effective des données entre États,

— conserver la décision d'adéquation rendue par la Commission européenne pour certains États qui en bénéficient,

— offrir des garanties élevées concernant la sécurité et la protection des données des ressortissants de l'Union européenne.

Les conceptions des États sur la protection des données varient en fonction de leur culture. Il existe cependant des indices de convergence des législations sur ce thème [6]. 39

A titre d'exemple, le Japon a négocié une décision d'adéquation avec la Commission européenne afin de garantir la libre circula- 40

6. United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows : Implications for Trade and Development*, in : UNCTAD (https ://unctad.org/), New York 2016, p. « http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf » (27/10/2018), p. 63.

tion des données personnelles entre ces deux zones géographiques et la licéité des transferts transfrontaliers, après l'entrée en vigueur du Règlement. Cette décision d'adéquation a été octroyée officiellement en date du 5 septembre 2018. De même, les Etats-Unis examinent l'opportunité de préparer un projet de Loi fédérale sur la protection des données.

41 Pour les entreprises, la priorité consiste à déterminer dans quelle mesure le Règlement s'applique aux traitements de données personnelles et comment mettre en œuvre une gouvernance effective des données personnelles au sein de leur organisation.

42 La définition d'une stratégie concernant la gouvernance des données, la création d'un plan d'action pour s'assurer de la conformité des entreprises au Règlement sont incontournables. La sécurité des données devrait figurer en première place de l'agenda de nombreux comités exécutifs et conseils d'administration de même que la désignation d'un délégué à la protection des données.

43 A l'intersection entre le droit public de la protection des données et le droit de la responsabilité civile, le Règlement général sur la protection des données tente de concilier des notions appartenant à deux domaines distincts. La première question discutée sera de savoir si le nouveau droit applicable réussit à servir à la fois les impératifs économiques et technologiques de l'ère digitale tout en offrant des garanties adéquates pour le respect du droit fondamental à la protection des données. Le débat nécessite de comprendre les fondements du Règlement général sur la protection des données et son impact en Suisse. Nous examinerons dans ce cadre le caractère extra-territorial du Règlement et son impact en Suisse en étudiant notamment le rôle attribué aux actions en responsabilité en droit de la protection des données, et, de façon générale, l'importance du contrôle *a posteriori* de la par des autorités de contrôle.

§3 Le plan général de la thèse

44 Cette étude est articulée en trois titres :

45 Le titre *premier* décrit les fondements nécessaires à la compréhension du Règlement général sur la protection des données. Il porte sur les enjeux, le contexte de l'élaboration du Règlement et sur les

sources juridiques de la protection des données.

Le titre *deuxième* définit les modalités de mise en œuvre extra- 46
territoriale du Règlement. Il examine le cadre juridique spécifique entre la Suisse et l'Union européenne, les acteurs concernés par la mise en œuvre du Règlement en Suisse et les droits et obligations des acteurs,en particulier la responsabilité des responsables du traitement et des sous-traitants.

Le titre *troisième* traite du développement du droit de la protection 47
des données en Suisse, en particulier sa mise en conformité avec le droit européen. Il s'agit d'un changement de paradigme pour la Suisse, transformant le Préposé fédéral à la protection des données en autorité de contrôle.

Première partie

Le fondement du règlement général sur la protection des données

La protection des données se fonde en Europe sur la protection de la sphère privée et sur la protection des droits de la personnalité. La protection de la sphère privée examine les relations entre l'individu et la société. Les droits de la personnalité, quant à eux, visent au respect des libertés civiles individuelles. 48

La Suisse reconnaît le droit à la protection des données comme un droit fondamental reconnu par la Constitution (art. 13 al. 2). La Convention européenne des droits de l'homme consacre ce droit fondamental à l'article 8 [7] et à la Déclaration universelle des droits de l'homme à l'article 12. 49

Ces textes entérinent le « droit à l'auto-détermination informationnelle [8], qui vise à déterminer « qui utilise des informations nous concernant, qui les propage et à quelles fins [9] ». 50

La protection des données et l'auto-détermination informationnelle [10], sont des conditions pour une démocratie libre, le maintien de l'État de droit et de la liberté d'expression [11]. 51

Le Préposé fédéral suisse à la protection des données, Monsieur Lobsiger l'a spécifiquement souligné lors de la présentation de son rapport annuel en juin 2017 : « Les applications du Big Data, l'intelligence artificielle et la robotique doivent garantir l'exercice du droit fondamental à l'auto-détermination informationnelle et à la protection de la vie privée [12] ». 52

Conscient de ces enjeux démocratiques, le législateur européen a conduit une refonte du droit de la protection des données au sein de l'Union européenne, qui a donné lieu au Règlement, après plus 53

7. Cet article fait référence à la Conv. 108 du Conseil de l'Europe du 28 janvier 1981, p. 3.
8. Poullet Yves / Rouvroy Antoinette, *Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie*, in : Benyekhlef Karim / Trudel Pierre (édit.), *Etat de droit et virtualité*, Montréal 2009, pp. 157-222.
9. Epiney Astrid, *Interview à la RTS*, Lausanne, 2013.
10. Solove Daniel J., *Conceptualizing privacy*, in : California Law Review 2002/90, p. 90.
11. *Ibidem.*
12. Wuthrich Bernard, *La protection des données est mise à mal par le Big Data*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/suisse/protection-donnees-mise-mal-big-data » (02/12/2019).

de quatre années de négociations.

54 La présentation des fondements du Règlement nous amène à traiter des enjeux de ce texte (chapitre I), du contexte de son élaboration (chapitre II), et de ses sources juridiques (chapitre III).

Chapitre 1: Les enjeux du Règlement

En principe, le cadre juridique devrait correspondre au contexte technologique et social d'une époque et répondre aux besoins de chacun des acteurs. La problématique de l'adaptation du droit au contexte sociétal est centrale dans un domaine fortement marqué par la transformation technologique. C'est précisément le cas du droit de la protection des données [13]. 55

La rapidité des transformations technologiques et les modifications du droit de la protection des données s'inscrivent dans des temporalités fondamentalement différentes. Ceci n'est pas sans conséquences. 56

L'essor des technologies digitales permet l'essor de biens et de services personnalisés et un maillage extrêmement fin de la vie privée d'une personne, jusqu'à remettre en cause la notion de sphère privée et d'autodétermination informationnelle. Les moyens de tracer l'individu, son comportement, sa personnalité, offrent des possibilités de surveillance, de connaissance et de manipulation privée ou publique inédites par leur ampleur et leur sophistication [14]. Dans le même temps, la sensibilité des citoyens sur ces questions est forte [15], comme en témoigne les demandes de déréférencement adressées à Google depuis juin 2014 [16]. 57

C'est pour cette raison que l'effectivité des droits des personnes est centrale [17]. Elle nécessite que la personne se réapproprie autant que 58

13. Weber Rolf H., *Datenschutz : zum Aufstieg einer neuen Rechtsdisziplin*, Bern 2015, p. 612.
14. Geffaray Edouard, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 20.
15. *Idem*, p. 19.
16. Google, *Recherches supprimées dans le cadre de la législation européenne sur la confidentialité des données*, in : Transparence des informations (https ://transparencyreport.google.com/), s.l. s.a., p. « https : / / transparencyreport.google.com/eu-privacy/overview?hl=fr » (27/10/2018), p. 1.
17. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 19.

possible la maîtrise de ses données personnelles [18].

59 Mais est-ce encore possible du fait des volumes de données concernés et de la puissance de calcul des ordinateurs, capables d'effectuer jusqu'à 93,014,125,436 d'opérations par seconde ? Ces données sont en outre traitées par des acteurs privés de dimension internationale, qui s'affranchissent dans leur modèle d'affaire du territoire des États [19], et dont la capitalisation boursière excède parfois le PIB de certains Etats (Apple a atteint USD 1000 milliards de dollars de capitalisation boursière en 2018) [20].

60 Comment assurer l'effectivité des droits des personnes sans empêcher les pouvoirs publics d'avoir accès à certaines informations, lorsque des motifs impérieux d'ordre public le justifient, et ne pas bloquer une innovation source de croissance et de solidarité, dont la valorisation des données personnelles est un des moteurs [21].

61 Le Règlement a tenté de répondre à ces impératifs contradictoires. En identifiant trois enjeux de la protection des données : le premier enjeu majeur est celui de la souveraineté du droit européen de la protection des données, c'est-à-dire de sa pleine applicabilité lorsque les données d'un résident européen sont traitées. Le second enjeu est celui de l'intégration croissante de l'Europe de la protection des données. Le troisième enjeu est celui de l'effectivité de la protection des données par des modalités de contrôle a posteriori [22].

18. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 19.
19. Pretelli Ilaria (édit.), *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales : actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, 1e éd., Genève 2018, p. 18.
20. Fontanel Jacques / Sushcheva Natalia, *La puissance des GAFAM : Réalités, apports et dangers*, in : Annuaire français de relations internationales : La Documentation française 2019, p. 5.
21. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 20.
22. *Idem*, p. 21 ss.

§1 L'extra-territorialité du droit européen de la protection des données

Pour que les citoyens européens soient pleinement en mesure d'exercer leurs droits, il est fondamental que l'Union dispose d'un droit dont l'applicabilité territoriale soit certaine. Le Règlement européen remplit cet objectif en harmonisant le droit européen des données dans les États membres, du fait de son application directe et de l'absence de transposition en droit national. 62

Le Règlement européen confère également plus de sécurité juridique du fait de son caractère extra-territorial. Il s'applique en effet aux traitements de données à caractère personnel effectués en dehors de l'UE dès lors que des personnes domiciliées dans l'UE sont concernées par le traitement. Il élève ainsi le standard de la protection des personnes concernées. Si la directive 95/46/CE posait comme critère du droit applicable celui de la localisation du responsable du traitement et de ses moyens de collecte, le Règlement retient quant à lui comme critère du droit applicable le « ciblage du citoyen [23] ». 63

I. Le ciblage du citoyen

Cette stratégie a pour but de renforcer la souveraineté du droit européen, c'est-à-dire sa pleine applicabilité lorsque les données d'un résident européen sont traitées [24]. 64

En application de ce nouveau critère, un responsable du traitement, même sans aucune attache physique ou logique en Europe, sera tenu de respecter le droit européen à l'égard des ressortissants européens [25]. 65

Pour garantir l'efficacité de ce nouveau critère, les transferts internationaux des données personnelles des résidents européens ont été encadrés par des instruments contraignants. Les débats dans le cadre du Règlement européen, sur les différents outils à dispo- 66

23. Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*, p. 442.
24. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 20.
25. *Ibidem.*

sition (Binding Corporate Rules, clauses contractuelles types, etc.) ont pris en compte les révélations de l'affaire PRISM et ont conduit à retenir des instruments contraignants, dont la méconnaissance sera susceptible de sanctions.

67 Faire en sorte que le droit européen ne puisse pas être contourné lorsque les données des européens sont en cause constitue un élément fondamental de souveraineté, de crédibilité de l'action européenne mais aussi de promotion d'un système qui concilie protection des droits et développement économique des technologies digitales et qui peut donc incarner un cadre juridique propice au développement économique [26].

II. Le marché des données à caractère personnel

68 « La valeur de l'économie européenne fondée sur les données pourrait atteindre plus de 700 milliards d'euro d'ici à 2020, ce qui représente 4 pour cent de l'économie de l'UE [27] ».

69 Éléments de la personnalité mais également actifs stratégiques de l'entreprise, les données personnelles sont devenues un bien marchand, une matière première, répondant à la logique économique de l'offre et de la demande.

70 Comme toute matière première disponible en abondance, la donnée a peu de valeur en-soi, c'est le résultat de son traitement qui lui en fait prendre. A titre d'exemple, la valeur d'une donnée disponible sur Facebook correspond à la capitalisation de Facebook, divisée par le nombre d'abonnés, ce qui correspond environ à 40 dollars

26. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 20.

27. Commission européenne, *Achever un marché unique numérique inspirant confiance pour tous - Communication de la Commission au Parlement Européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions du 15 mai 2018 (COM(2018) 320 final)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2018, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2018/FR/COM-2018-320-F1-FR-MAIN-PART-1.PDF » (21/07/2019), p. 2 ; Riechert Anne, *Dateneigentum – ein unauflösbarer Interessenkonflikt ?*, in : Datenschutz und Datensicherheit-DuD 2019 43/6, pp. 353-360.

par personne [28].

La valeur d'une donnée peut également être calculée par le manque à gagner, lors de sa disparition, par exemple à la suite d'un vol de données. Il peut également résulter du risque de sanction administrative ou de versement de dommages-intérêts lors du contrôle a posteriori effectué par les autorités de contrôle ou les recours juridictionnels effectifs des parties lésées. A titre d'exemple, le vol de données subi par Equifax (perte des données de 147 millions d'américains) va coûter entre 575 millions et 700 millions de dollars à l'établissement de crédit en compensation des dommages individuels et en sanctions civiles, dans le cadre d'un accord avec l'agence de régulation fédérale, l'agence de protection des consommateurs et les 50 États et territoires américains [29]. 71

Considérées comme un bien marchand au États-Unis, les données personnelles font l'objet de transactions á titre rémunéré sur une bourse des données avec des intermédiaires spécialisés dans le courtage des données personnelles (data broker) [30]. La doctrine européenne reconnaît la double nature de la donnée, notamment son statut de marchandise [31]. 72

Aux États-Unis, une adresse vaut 50 cents, une date de naissance 2 dollars, un numéro de sécurité sociale 8 dollars, un livret militaire 35 dollars [32]. 73

A contrario, on peut également estimer la valeur des données personnelles en calculant combien coûte leur non-divulgation. Ainsi, 74

28. Loubière Paul, *Vos données personnelles sur internet peuvent valoir de l'or*, in : Challenges (https ://www.challenges.fr/), Paris 2014, p. « https://www.challenges.fr/high-tech/vos-donnees-personnelles-sur-internet-peuvent-valoir-de-l-or_57690 » (22/05/2019), p. 1.
29. Cavaliere Victoria / Fung Brian, *Equifax exposed 150 million Americans' personal data. Now it will pay up to $700 million*, in : CNN Business (https ://edition.cnn.com/), Atlanta 2019, p. «https://edition.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html » (22/07/2019).
30. Bounie David / Dubus Antoine / Waelbroeck Patrick, *Selling Strategic Information in Digital Competitive Markets*, in : HAL Archives-Ouverts 2018, p. 2 ss.
31. Nardi Daniele, *« Courtoisie internationale » et portée extraterritoriale du droit européen à la protection des données à l'épreuve de la Cour*, in : Cahiers de droit europeen 2018 54/2, p. 1.
32. Loubière, *Vos données personnelles sur internet peuvent valoir de l'or*, p. « https://www.challenges.fr/high-tech/vos-donnees-personnelles-sur-internet-peuvent-valoir-de-l-or_57690 » (22/05/2019), p. 1.

une start-up californienne, dénommée "Protect my ID", protège les données personnelles d'une divulgation au prix mensuel de 15,95 dollar par mois [33].

75 Le marché des données volées a quant à lui la capacité de créer des problèmes politiques de grande ampleur [34]. La récente jurisprudence du Tribunal fédéral suisse [35] rappelle l'existence d'une présomption de bonne foi entre États, tel qu'elle découle de la Convention de Vienne sur le droit des Traités [36].

76 Malgré la volonté des entreprises de limiter les risques de sécurité, et de préserver la confiance de leurs clients en lien avec les traitements des données personnelles [37], la cybersécurité constitue une priorité pour de nombreuses organisations, le nombre de violations de données ne cessant d'augmenter [38].

77 La gestion de ces risques portent principalement sur l'accès aux données, la « cyber infrastructure » constituée des serveurs, des dorsales internet (backbones), des commutateurs et routeurs [39]. La lutte contre les virus et les malwares est également au centre des enjeux de cybersécurité (Exemple du logiciel pirate ransomware

33. Boutonnet Christophe, *Rapport CIGREF « Economie des données personnelles »*, Paris 2015, p. 32.
34. Tribunal fédéral, *Communiqué de presse du TF du 5 avril 2017, en lien avec l'arrêt du 17 mars 2017 (2C_1000/2015)*, in : Tribunal fédéral (https ://www.bger.ch/), Lausanne 2017, p. « https://www.bger.ch/files/live/sites/bger/files/pdf/fr/2C_1000_2015_2017_04_05_T_f_09_47_53.pdf » (03/12/2018).
35. ATF 2C 893/2015 du 16 février 2017, consid. 11.1.
36. Message relatif à l'adhésion de la Suisse à la Convention de Vienne de 1969 sur le droit des traités et à la Convention de Vienne de 1986 sur le droit des traités entre Etats et organisations internationales ou entre organisations internationales du 17 mai 1989, FF 1989, p. 697.
37. Beyer Marcus, *Sicherheitsrisiko facebook, Twitter & Co.*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2010 10/1.
38. O'Brien David, *Privacy and Cybersecurity Research Briefing*, in : Berkman Klein Center Research Publication 2016/17, p. 4 ss.
39. Springer Paul J. (édit.), *Encyclopedia of Cyber Warfare*, Santa Barbara 2017, p. 15.

WannaCry en Mai 2017) [40].

Plus encore, comme le mentionne Yuval Noah Harari [41], la concentration actuelle des données personnelles de nature biologique ou génétique, combinée à la puissance de calcul des ordinateurs et aux technologies d'intelligence artificielle et d'apprentissage machine rendent désormais possible le « hacking » de l'être humain [42]. Les enjeux de la cysécurité réside pour lui dans dans la capacité des algorithmes d'avoir une connaissance plus fine d'une personne que la personne elle-même. Cet état de fait faciliterait ainsi les prédictions des choix et décisions individuelles ce qui pourrait aboutir à la manipulation des individus. L'enjeu de la protection des données in fine serait celui du déplacement du pouvoir des individus vers celui des algorithmes, aboutissant aussi à une délégation potentielle de responsabilité. 78

La CJUE et le Règlement européen tentent de maintenir un équilibre des rapports de force entre tous les acteurs à l'ère digitale. A la suite de l'arrêt Schrems [43], le Règlement place la personne humaine au coeur du dispositif de la protection des données [44] et rappelle la responsabilité des acteurs économiques dans le traitement des données personnelles, certaines étant plus sensibles que d'autres (données de santé, biologiques, génétiques...). La possibilité d'un contrôle a posteriori et d'une action civile en responsabilité (voir paragraphe 1294) est cruciale en ce qu'elle rappelle aux acteurs économiques que dernière les données personnelles collectées se trouvent une personne humaine, digne de respect et que sa vie privée a une valeur digne de protection. Le non-respect de la personne humaine à travers le traitement de ses données personnelles est punissable par des sanctions dissuasives des autorités de 79

40. Meyer Paul / Stauffacher Daniel, *WannaCry, the Geneva Digital Convention and the urgent need for Cyber Peace - A commentary by ICT4Peace*, in : ICT4Peace Foundation (https ://ict4peace.org/), Geneva 2017, p. « https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2017-Wannacry-GenevaDigitalConvention.pdf » (03/12/2019).
41. Harari Yuval Noah, *Homo Deus : A brief history of tomorrow*, 1e éd., New York 2018 ; Harari Yuval Noah, *21 Lessons for the 21st Century*, 1e éd., London 2018.
42. Harari Yuval Noah, *Conférence du 10 juillet 2019*, EPFL, Lausanne.
43. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :627, consid. 62.
44. Feral-Schuhl Christiane, *Comment les droits de la personne concernée sont-ils renforcés ?*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 222.

contrôle et le versement de dommages-intérêts par le juge (art. 83 RGPD, art. 82 RGPD).

III. L'intégration croissante de l'Europe de la protection des données

80 A l'ère digitale, l'enjeu est d'assurer un contrôle territorialisé d'un phénomène par nature dématérialisé [45]. Pour M.A Frison-Roche, « le digital est une monde de libertés dans lequel le droit n'a prise que de manière fragmentaire et dans lequel le principe de personne n'existe pas [46] ». L'enjeu est également de garantir aux entreprises soumises au droit européen une sécurité juridique maximale, c'est-à-dire une homogénéité, une stabilité, et une relative prévisibilité de la norme et de son interprétation. Cet impératif de sécurité juridique trouve son fondement dans l'interdépendance étroite qui unit les pays qui font partie de l'Union européenne. Cette interdépendance a renforcé la coopération des autorités nationales, et a rendu pertinente une intégration croissante de l'Europe de la protection des données [47].

81 Cette intégration se caractérise notamment par l'adoption des avis et des travaux du groupe de travail de l'Article 29 de la Commission européenne, constitué des autorités de protection européennes. Ce groupe a publié de nombreux avis facilitant l'interprétation des dispositions du Règlement et l'harmonisation de son application dans les États-membres. Il est également intervenu dans le cadre de contentieux avec des entreprises privées (voir la privacy policy de

45. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 21.
46. Frison-Roche Marie-Anne, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, in : MAFR (https ://mafr.fr/), Paris 2019, p. « https://mafr.fr/fr/article/lapport-du-droit-de-la-compliance-dans-la-gouverna/ » (07/03/2020).
47. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 20.

Google [48] ou de Microsoft [49] ou le rôle des autorités de contrôle [50]).

C'est dans cette double logique d'intégration et de sécurité juridique que s'inscrit le Règlement européen sur la protection des données. L'adoption du Règlement permet, dans toute l'Union, de garantir un niveau élevé de protection des données dans l'Union [51], l'application et l'interprétation d'un seul texte. Il s'agit d'un instrument de stabilité propice au développement de modèles d'affaires durables pour les entreprises [52]. 82

Cette intégration de l'Europe sur le plan de la protection des données dépend principalement de l'adhésion des entreprises à cette vision positive selon laquelle la protection des données constitue un avantage comparatif. Il s'agit également d'un enjeu de confiance pour les personnes concernées qui confient leurs données personnelles à des organisations dont elles attendent un traitement diligent. Le contexte des scandales post-Snowden, Wikileaks puis Facebook et Cambridge Analytica a renforcé tant la méfiance des personnes concernées que les contrôles a posteriori par les autorités de contrôle que par les personnes concernées elles-mêmes par l'intermédiaire du juge. 83

48. Article 29 Data Protection Working Party, *Letter from the Article 29 Working Party of the European Commission President to the CEO of Google with regards to Google Privacy Policy of 22 September 2014*, in : European Commission (https ://ec.europa.eu/), Brussels 2014, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf » (03/12/2018).
49. Article 29 Data Protection Working Party, *Letter from the Article 29 Working Party of the European Commission President to the CEO of Microsoft of 22 September 2014*, in : European Commission (https ://ec.europa.eu/), Brussels 2014, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf » (03/12/2018).
50. Article 29 Data Protection Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « http://ec.europa.eu/information_society / newsroom / image / document / 2016 - 51 / wp244 _ en _ 40857 . pdf » (27/10/2018).
51. Arrêt CJUE du 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI :EU :C :2019 :772, consid. 54.
52. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 20.

§2 Les modalités de contrôle *a posteriori*

84 Dans un États de droit, l'équilibre de tout système juridique repose sur l'équilibre des rapports de force en présence. Cet équilibre dépend notamment du respect de la norme juridique et des mesures de contrôle *a posteriori*. Le contrôle *a posteriori* repose sur trois acteurs : le citoyen, les autorités de protection et le juge [53].

I. Le citoyen

85 Le contrôle par le biais du citoyen est le contrôle démocratique par excellence. La jurisprudence européenne en est une illustration [54].

86 Les données personnelles étant rattachées à une personne et relevant pour partie de son intimité, les individus doivent avoir la plus grande maîtrise possible de leurs données et constituer à ce titre les premiers gardiens en la matière. Ce contrôle démocratique doit être relayé et consacré par le double contrôle des autorités de contrôle et du juge.

II. Le rôle des autorités de contrôle

87 En tant que régulateurs, les autorités de contrôle doivent définir un cadre éthique et réglementaire, au sein duquel les entreprises puissent déployer leurs traitements. Elles doivent aussi assurer le suivi des plaintes individuelles et sanctionner les manquements au Règlement.

88 L'autorisation des autorités de contrôle européennes revêt parfois un caractère essentiel. Ainsi, à la suite des révélations d'Edouard Snowden, concernant le transfert de données personnelles vers des autorités publiques étrangères (programme PRISM), le Parlement européen a décidé dans le projet de Règlement d'imposer à toute entreprise sollicitée par une autorité publique étrangère de soumettre ce transfert de données à l'autorisation des autorités de contrôle européennes des pays dont les résidents sont concernés.

89 L'idée est d'encadrer le transfert dans des conditions telles qu'elles ne peuvent générer une surveillance massive et indifférenciée des personnes physiques.

53. Geffaray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 22.
54. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :627, consid. 13.

III. Le juge

Le juge, pour sa part, doit intervenir pour trancher les litiges entre les régulateurs et les responsables de traitement, mais aussi entre les particuliers et les autorités de contrôle. 90

A titre d'exemple, nous pouvons citer l'arrêt Google Spain du 13 mai 2014 de la Cour de Justice de l'Union Européenne [55]. Selon cette jurisprudence, l'activité d'un moteur de recherche peut être considérée comme un traitement de données personnelles. Si la personne concernée est la seule à pouvoir activer son droit au déréférencement auprès du responsable du traitement d'un moteur de recherche, celui-ci agit ensuite sous le double contrôle de l'autorité de protection et du juge. L'autorité de protection a vocation à agir directement sur ces nombreuses demandes individuelles et le juge a vocation à trancher les cas les plus problématiques. L'effectivité des droits est ainsi assurée dans une complémentarité de droits et repose sur les échanges tripartites entre l'individu, les autorités de contrôle indépendantes et le juge, notamment communautaire [56]. Plus ces échanges sont constructifs, plus le contrôle A posteriori est efficace. 91

De l'engagement complémentaire des entreprises, des administrations, du citoyen, des autorités de protection des données, et du juge dépend l'effectivité de la protection des droits et l'équilibre entre droits et innovation. La construction d'un système juridique européen humaniste, c'est-à-dire centré sur la personne humaine dont les données sont traitées et favorisant dans le même temps la libre circulation des données, constitue un défi majeur à relever pour les États démocratiques à l'ère digitale. Au service du citoyen, avec les entreprises, sous le contrôle du régulateur et du juge européen [57]. 92

Le juge doit intervenir pour trancher les litiges entre les régulateurs et les responsables de traitement, mais aussi entre les particuliers qui n'auraient pas eu satisfaction et les autorités de contrôle. 93

La Cour de justice de l'Union européenne, joue un rôle clef dans cet 94

55. Arrêt CJUE du 13 mai 2014, *Google Inc contre Agencia Española de Protección de Datos (AEPD)*, C-131/12, ECLI :EU :C :2014 :317, consid. 79.
56. Geffray, *Comment assurer l'effectivité de la protection des droits à l'ère post-snowden ?*, p. 23.
57. Castets-Renard Céline (direct.), *Quelle protection des données personnelles en Europe ?*, 1e éd., Bruxelles 2015, p. 26.

recherche d'équilibre entre des intérêts divergents [58].

95 La problématique de la « compliance », de la place du droit et de la place du juge est une question centrale. Le Règlement propose une vision opérationnelle du droit de la « compliance » appliquée au droit de la protection des données. Il impose, à titre d'exemple, aux responsable du traitement et aux sous-traitants de prendre des mesures techniques et organisationnelles appropriées pour ne pas être tenus responsables en cas de contentieux (voir paragraphe 941).

58. Invalidation de la directive 2006/24/EC (Arrêt CJUE du 8 avril 2014, *Digital Rights Ireland contre Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.*, Aff. jointes C-293/12 and C-594/12,ECLI :EU :C :2014 :238 ; Arrêt CJUE du 21 décembre 2016, *Tele2 Sverige/Watson*, Aff. C-203/15, ECLI :EU :C :2016 :970).

Chapitre 2: Le contexte de l'élaboration du Règlement

Avant d'exister en tant que droit européen, le droit de la protection des données est apparu en Allemagne. En 1970, le canton de Hesse a élaboré pour la première fois au monde une loi sur la protection des données. En 1977, la première loi fédérale sur la protection des données est apparue en Allemagne suivie par la France en 1978 [59]. 96

Le modèle européen de protection des données place la personne et ses droits au cœur du système. Celui-ci est protégé, appliqué et en partie construit par le juge, notamment la Cour de Justice de l'Union européenne et par les autorités de protection des données. En témoignent deux arrêts de la Cour de Justice rendus entre avril et mai 2014, sur les thèmes de la rétention des données de connexion, l'indépendance des autorités de protection des données, et le droit de déréférencement [60]. 97

Le contenu du Règlement est le résultat de plus de quatre années de négociations, qui a fait l'objet d'une vaste littérature [61]. Les contextes 98

59. Patklom Thasanee, *Herausforderungen bei der Umsetzung des Datenschutzes für ein Schweizer Unternehmen*, 1e éd., Zürich 2018, p. 20.
60. Arrêt CJUE du 8 avril 2014, *Digital Rights Ireland contre Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI :EU :C :2014 :238, consid. 9 ; Arrêt CJUE du 13 mai 2014, *Google Inc contre Agencia Española de Protección de Datos (AEPD)*, C-131/12, ECLI :EU :C :2014 :317, consid. 4.
61. Pötters Stephan, *Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts*, in : Recht der Datenverarbeitung (RDV) 2015/1, pp. 10-16 ; Vasella David, *DSGVO : Stand und Fundstellen*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2016, pp. 28-29 ; Weber Rolf H., *EU - Datenschutz - Grundverordnung : Kernelemente und Ausstrahlungswirkung auf die Schweiz*, in : Jusletter IT (http :// jusletter-it.weblaw.ch/), Bern 2015, p. « http : / / jusletter - it . weblaw . ch / issues / 2015 / 24 - September - 2015 / eu - datenschutz - grund _ bd86ed7481 . html » (21/05/2019) ; Kern Markus, *Datenschutzrevision in der EU : Neuer Wein ? Neue Schläuche ?*, in : Digma-Zeitschrift für Datenrecht und Informationssicherheit 2013 13/1, pp. 30-33 ; Rossnagel Alexander / Richter Philipp / Nebel Maxi, *Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DS-GVO*, in : Zeitschrift für Datenschutz 2013 3/3, pp. 103-108 ; Rossnagel Alexander / Nebel Maxi / Richter Philipp, *Was bleibt vom Europäischen Datenschutzrecht ? Überlegungen zum Ratsentwurf der DS-GVO*, in : Zeitschrift für Datenschutz 2015/5, pp. 455-460 ; Ehmann Eugen, *Der weitere Weg zur Datenschutzgrundverordnung–Näher am Erfolg, als viele glauben*, in : ZD

politiques, historiques et économiques ont joué un rôle important sur le contenu du Règlement. D'où la nécessité d'examiner ces aspects.

§1 Le contexte historique et politique

I. Le processus législatif et les travaux préparatoires

99 Si le Conseil européen définit l'agenda politique de l'Union européenne, le processus législatif européen est à l'initiative de la Commission européenne. Celle-ci propose une nouvelle législation, qui est ensuite examinée par le Conseil de l'Union européenne, en charge de la négociation et de la législation européenne, en accord avec le Parlement européen.

100 Dès 2009, la Commission a lancé plusieurs études et consultations publiques sur le thème de la protection des données.

101 En 2012, la Commission européenne a proposé une réforme globale des règles en matière de protection des données en Europe pour accroître la maîtrise des utilisateurs sur leurs données personnelles, et pour réduire les coûts des entreprises [62].

102 En 2012, Vivian Reding a effectué le constat que la législation européenne en matière de protection des données datait de 1995 et ne correspondait plus à la réalité technologique. En 1995, moins de 1 pour cent des Européens utilisaient Internet, alors qu'en 2012, de grandes quantités de données à caractère personnel étaient transférées d'un continent à l'autre, en quelques fractions de seconde.

103 Elle insista sur le fait que « la protection des données à caractère personnel est un droit fondamental reconnu à tous les concitoyens, mais ceux-ci n'ont pas toujours le sentiment de maîtriser entièrement les données à caractère personnel les concernant ». Les propositions législatives ont pour objectif de renforcer la confiance

2015, pp. 6-12 ; Wagner Lorin-Johannes, *Datenschutz in der EU*, 1e éd., Wien 2015, pp. 1-280.

62. Commission Européenne, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises - Communiqué de presse du 25 janvier 2012*, in : Commission Européenne (http ://europa.eu/), Bruxelles 2012, p. « http : / / europa . eu / rapid / press - release_IP-12-46_fr.htm?locale=FR » (27/10/2018).

dans les services en ligne en informant mieux les utilisateurs de leurs droits et en ayant une plus grande maîtrise des informations qui les concernent. Pour la Commission européenne, un cadre juridique solide, clair et uniforme au niveau de l'UE contribuera à libérer le potentiel que possède le marché unique digital et à soutenir la croissance économique, l'innovation et la création d'emplois [63].

Le 25 janvier 2012, la Commission européenne a présenté le projet de réforme du droit de la protection des données lors d'une conférence de presse [64]. 104

Dans une note informelle, l'administration américaine a critiqué l'introduction de nouveaux instruments juridiques contraignants visant à accroître la protection des personnes concernées (notification des violations de données, droit à l'oubli, protection des données des enfants, règles pour les transferts transfrontaliers de données [65]. 105

L'Allemagne a également fortement réagi à l'annonce du projet de révision de la directive et de son remplacement par un Règlement. Le juge Johannes Masing du Tribunal fédéral constitutionnel a identifié le risque de non-application des droits fondamentaux en Allemagne et de remise en cause du rôle du Tribunal fédéral constitutionnel [66]. 106

Choisissant de suivre la procédure législative ordinaire de l'article 16, al. 2 du Traité sur le fonctionnement de l'Union Européenne (TFUE) [67] pour réformer la directive 95/46 CE, la Commission européenne a communiqué une version du projet au Parlement européen et au Conseil de l'Union européenne pour approbation (art. 107

63. *Ibidem.*
64. *Ibidem.*
65. European Digital Rights, *US lobbying against draft Data Protection Regulation*, in : EDRi (http ://www.edri.org/), Brussels 2011, p. « http://www.edri.org/US-DPR » (12/04/2019).
66. Vordermayer Markus, *Ein „Abschied von den Grundrechten"?*, in : Rescriptum (http ://www.rescriptum.org/), München 2012, p. « http://www.rescriptum.org/Aufsätze/2012_1_024_Vordermayer.pdf » (18/04/2019).
67. Union européenne, *Traité sur le fonctionnement de l'Union Européenne du 26 octobre 2012, C 326/ 49 - Journal officiel de l'Union européenne*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2012, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012E/TXT&from=DE » (02/04/2019).

294 TFUE).

108 Le Parlement européen a examiné le projet dans le cadre de réunions de commissions spécialisées [68]. La commission des libertés civiles, de la justice et des affaires intérieures (LIBE) a dirigé le projet de Règlement général sur la protection des données. Cette commission (LIBE) est responsable de la législation et du contrôle démocratique des politiques en matière de justice et des affaires intérieures. Elle garantit le plein respect au sein de l'Union européenne de la charte des droits fondamentaux et de la convention européenne des droits de l'homme ainsi que le renforcement de la citoyenneté européenne [69]. D'autres commissions ont également proposé des amendements et commenté le projet de texte. Les commentaires et propositions d'amendements reçus furent consolidés dans un document, qui fut communiqué au Parlement européen. Ce document reflétait la position officielle du Parlement européen sur le projet de réforme européenne en matière de protection des données.

109 Le Conseil de l'Union européenne a également examiné le projet. Le groupe de travail principal était le groupe DAPIX dédié à l'échange d'informations et à la protection des données (« Information Exchange and Data Protection »). Une fois sa version finalisée, le groupe DAPIX a communiqué le projet de Règlement général au Conseil de l'Union européenne. Ce projet reflétait la position officielle du Conseil de l'UE sur le projet de réforme européenne.

110 Le Parlement et le Conseil de l'UE ont ensuite entamé une discussion pour parvenir à un consensus sur le projet de Règlement (figure 2.1), en présence de la Commission européenne (procédure du Trilogue) [70].

68. Albrecht Jan Philipp, *Das neue EU-Datenschutzrecht-von der Richtlinie zur Verordnung*, in : Computer und Recht 2016 32/2, p. 1 ; Milt Kristiina, *La protection des données à caractère personnel*, in : Fiches techniques sur l'Union européenne (http ://www.europarl.europa.eu/), Bruxelles 2019, p. « http://www.europarl.europa.eu/ftu/pdf/fr/FTU_4.2.8.pdf » (22/05/2019).
69. Parlement européen, *Annexe VI relative aux compétences des commissions parlementaires permanentes, XVII Commission des libertés civiles, de la justice et des affaires intérieures*, in : Règlement intérieur du Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2019, p. « https://www.europarl.europa.eu/doceo/document/lastrules/RESP-LIBE_FR.html » (05/12/2019).
70. Albrecht, *Das neue EU-Datenschutzrecht-von der Richtlinie zur Verordnung*, p. 1.

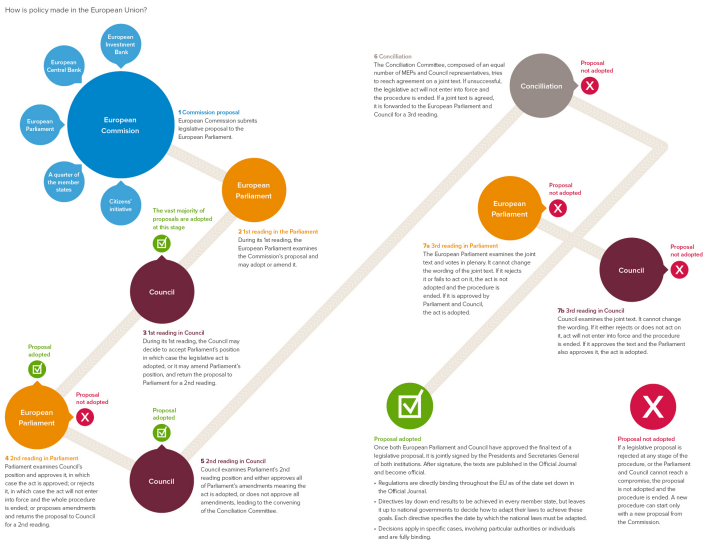

FIGURE 2.1 – Processus d'élaboration des politiques européennes. (Source : « https://royalsociety.org/ ».)

La réforme du droit européen de la protection des données a été longue et difficile, comme en atteste ce graphique. 111

Si le processus d'élaboration des politiques européennes est en soi complexe, l'élaboration du Règlement a été rendue particulièrement délicate du fait de la divergence des intérêts en présence. De nombreux groupes de pression (Think Tank, Lobbies indutriels (bancaire, pharmaceutique, informatique)), Lobbie de la police ou les représentants des consommateurs, tous ont pris part aux négociations [71]. 112

Le contrôleur européen de la protection des données (CEPD) a approuvé la révision du cadre juridique pour la protection des données dans l'UE afin de garantir une protection efficace et constante des individus dans une société de l'information globalisée fondée 113

71. ALBRECHT Jan Philippe, *La ruée vers les data*, in : Arte, p. « https://www.youtube.com/watch?v=UL2guT4FIYc » (30/10/2017) ; WEBER, *Datenschutz*, p. 614.

sur les technologies [72].

114 Il insista sur le contexte de la révision en faisant référence au développement technologique et à la mondialisation qui donne lieu à une « augmentation des traitements et des transferts internationaux de données transfrontalières ».

115 Il fit notamment référence à « la délocalisation de traitements de grandes quantités de données à l'échelle mondiale et à l'intensification des activités policières et judiciaires internationales en faveur de la lutte contre la criminalité organisée, à l'aide d'un échange massif d'informations à des fins répressives [73]».

116 L'entrée en vigueur du traité de Lisbonne [74] a marqué une nouvelle ère pour la protection des données. L'article 16 TFUE prévoit non seulement un droit individuel pour la personne concernée, mais fournit également une base juridique directe pour une solide législation en matière de protection des données à l'échelle de l'UE. Par ailleurs, l'abolition de la structure en piliers oblige le Parlement européen et le Conseil à garantir la protection des données dans tous les domaines du droit européen. En d'autres termes, elle permet la mise en place d'un cadre juridique global pour la protection des données qui soit applicable au secteur privé, au secteur public, tant dans les États membres que dans les institutions et organes de l'UE.

117 Enfin, la modernisation des instruments juridiques existants dans le domaine de la protection des données a eu pour effet de lancer un projet de révision de la convention 108 du Conseil de l'Europe et des lignes directrices de l'OCDE concernant la protection de la vie privée, dans un objectif d'harmonisation. L'adoption de normes internationales sur la protection des données à caractère personnel et de la vie privée contribue à l'élaboration progressive d'un instrument mondial contraignant sur la protection des données.

72. Le contrôleur européen de la protection des données, *Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » (2011/C 181/01)*, in : Journal officiel de l'Union européenne (https ://edps.europa.eu/), Bruxelles 2011, p. « https : / / edps . europa . eu / sites / edp / files / publication / 11 - 01 - 14_personal_data_protection_fr.pdf » (07/03/2019).

73. *Ibidem.*

74. Union européenne, *Traité sur l'UE*, C-326/13, 26 octobre 2012, version consolidée.

A. Le contenu de la réforme soumise par la Commission européenne

La réforme soumise par la Commission européenne le 25 janvier 2012 modernise les principes inscrits dans la directive de 1995 relative à la protection des données. Elle tend à harmoniser le droit de la protection des données dans l'UE, à garantir les droits des personnes concernées par le traitement de leurs données personnelles. Elle vise enfin à favoriser la libre circulation des données au sein de l'UE. 118

En 2012, la Commission européenne envisageait déjà un corpus unique de règles relatives à la protection des données valable dans toute l'Union. La réforme comprenait une communication exposant les objectifs de la Commission, ainsi que deux propositions législatives : un Règlement définissant un cadre général de l'UE pour la protection des données et une directive relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que des activités judiciaires connexes [75]. Cette directive applique les règles et principes généraux relatifs à la protection des données à la coopération policière et judiciaire en matière pénale. Les règles s'appliquent aux traitements aussi bien transfrontaliers que nationaux de données à caractère personnel. 119

Au niveau du contenu, le projet de réforme visait dès l'origine à responsabiliser les organisations procédant au traitement de données à caractère personnel, en créant de nouvelles obligations et responsabilités. 120

En contrepartie, le projet supprimait l'obligation de notifier l'ensemble des activités concernant la protection des données à des autorités de contrôle compétentes en la matière (cette obligation étant à l'origine de formalités administratives coûtant 130 millions d'EUR par an aux entreprises). Ceci est formalisé par le Règlement. 121

Le projet renforçait déjà les droits des personnes concernées [76]. La 122

75. Commission Européenne, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises*, p. « http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=FR » (27/10/2018).

76. Weber, *Datenschutz*, p. 617.

version finale prévoyait d'obtenir un consentement explicite pour certaines catégories de données faisant courir un risque élevé pour les droits de l'homme et les libertés fondamentales de la personne concernée. Le consentement pour utiliser des données personnelles devait déjà être beaucoup plus difficile à obtenir et à prouver pour les entreprises [77]. En outre, la Commission envisageait aussi dans l'avant-projet de faciliter l'accès des personnes concernées à leurs propres données ainsi que le transfert de données à caractère personnel d'un prestataire de services à un autre (droit à la portabilité des données). La concurrence entre prestataires de services devait s'en trouve renforcée. Un « droit à l'oubli numérique » fut créé, pour aider les citoyens à mieux gérer les risques liés à la protection des données en ligne : ce droit permet de requérir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation [78]. Il est la formalisation de la jurisprudence de la CJUE [79].

123 La Commission avait en outre déjà prévu que le Règlement aurait un champ d'application extraterritorial [80].

124 La réforme simplifiait les relations des entreprises et des personnes concernées avec les autorités compétentes. Elle prévoyait qu'une seule autorité nationale serait chargée de la protection des données dans le pays de l'UE où les entreprises ont leur établissement principal. De même, les citoyens pourraient s'adresser à l'autorité chargée de la protection des données dans leur pays, même lorsque leurs données sont traitées par une entreprise établie en-dehors du

77. Hofmann-Hafner Susanne / Borboën Yan / Colonna Vincent, *Fondamentaux du règlement général sur la protection des données et comment PwC peut vous aider*, in : PwC (https ://news.pwc.ch/), Geneva 2018, p. « https://news.pwc . ch / wp - content / uploads / 2016 / 08 / Fondamentaux - du - reglement - general_FR.pdf » (26/10/2018).

78. Commission Européenne, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises*, p. « http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=FR » (27/10/2018).

79. Arrêt CJCE du 13 mai 2014, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12, ECLI :EU :C :2014 :317.

80. Commission européenne, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises*, p. « http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=FR » (27/10/2018).

territoire de l'UE.

Dans son projet, la Commission européenne modifiait le statut des autorités nationales chargées de la protection des données. Elles devenaient des autorités de contrôle. Leurs compétences étaient renforcées afin qu'elles puissent mieux faire appliquer et respecter les règles de l'UE. Elles étaient habilitées à infliger des amendes aux entreprises qui enfreignaient les règles de l'Union relatives à la protection des données. Ces amendes pourraient atteindre 1 million EUR ou 2 % du chiffre d'affaires annuel global de l'entreprise. Le projet final portait le montant de l'amende à 20 millions EUR ou 4 % du chiffre d'affaires mondial. 125

En juin 2015, la Commission européenne a publié une version consolidée du projet de révision [81]. 126

Le projet de règlement était composé de 91 articles et 135 considérants, soit plus de 250 pages. 127

La version définitive du Règlement européen repose sur quelques principes fondamentaux, de manière analogue au droit suisse, dont le respect doit être démontré par le responsable du traitement en cas de litige. 128

Dans le communiqué de presse de la Commission européenne de 2015, le but du Règlement est d'harmoniser la législation sur la protection des données afin de renforcer le marché unique de l'UE [82]. La protection de l'individu contre un abus dans le traitement des données personnelles ne figure plus au premier plan. 129

B. Le Règlement : un texte de compromis

Le Règlement est un texte long et complexe. Il contient 173 considérants pour 99 articles. Il est plus complexe que la directive de 1995 qui fonde le droit communautaire de la protection des données de- 130

81. Conseil de l'Union Européenne, Doc 9398/15 du 1er juin 2015 ; Weber, *Datenschutz*, p. 314.
82. European Commission, *Stronger data protection rules for Europe*, in : European Commission (https ://ec.europa.eu/), Luxembourg 2015, p. « http : //europa.eu/rapid/press-release_MEMO-15-5170_fr.htm » (22/05/2019).

puis vingt ans [83].

131 Le processus législatif a duré plus de quatre ans et a fait l'objet de plus de 1000 amendements. Sous la pression des lobbies, le processus législatif a été interrompu au bout de 18 mois [84].

132 Les révélations de l'affaire PRISM faites par Edouard Snowden et l'invalidation par la Cour de Justice de l'Union européenne, le 6 octobre 2015, de la décision d'adéquation de la Commission européenne selon laquelle les États-Unis garantissent un niveau de protection adéquat des données à caractère personnel ont relancé le processus de négociation du Règlement au Parlement européen. Nous allons brièvement expliquer en quoi ces deux affaires ont joué un rôle fondamental dans le processus législatif du Règlement et dans son contenu.

C. Les révélations d'Edward Snowden

133 Les révélations d'Edward Snowden le 6 juin 2013, au sujet de la National Security Agency (NSA) américaine [85] et des moyens employés à un niveau mondial aux fins d'une surveillance illicite des communications électroniques (via téléphone mobile ou Internet) ont sensibilisé un large public à la question de la protection des données à caractère personnel dans le monde.

134 Cette affaire a fait émerger des questionnements concernant la portée des systèmes de surveillance aux États-Unis et dans les États membres de l'Union. Elle a soulevé des interrogations concernant la violation des normes juridiques et des droits fondamentaux de l'Union européenne [86] ainsi que des normes européennes en ma-

83. Falque-Pierrotin Isabelle, *Règlement européen sur la protection des données : Le règlement européen « Data protection » adopté le 27 avril 2016 consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés*, Cork 2016, pp. 1-759.

84. Albrecht Jan Philippe, *La ruée vers les data*, in : Arte, p. « https://www.youtube.com/watch?v=UL2guT4FIYc » (30/10/2017).

85. Privacy International, *Privacy International and nine other human rights organizations pursue landmark case at European Court of Human Rights directly challenging UK and US mass surveillance revealed by Edward Snowden*, in : Privacy International (http ://privacyinternational.org/), London 2016, p. « http : / / privacyinternational . org / press - release / 1316 / privacy - international - and - nine - other - human - rights - organizations - pursue - landmark » (27/10/2018).

86. Parlement européen, *Programme de surveillance de la NSA, organismes de*

tière de protection des données.

En particulier, s'est posée la question du degré de coopération et d'implication tant des agences de renseignements de certains États membres de l'Union européenne dans des programmes de surveillance américains que de certaines entreprises informatiques et de télécommunication privées. Des interrogations ont vu le jour concernant les frontières entre les activités répressives et les activités de renseignement avec pour effet que chaque citoyen est traité comme un suspect et fait l'objet d'une surveillance. La confiance à l'égard du respect de l'État de droit, et la confiance dans la sécurité des services et des communications informatiques ont été mises à mal [87]. 135

À la suite de ces révélations, le Congrès américain a adopté le US Freedom Act pour limiter les dispositions du Patriot Act [88]. 136

Des divergences politiques sont apparues entre les autorités chargées de la protection des données, incitant la Commission européenne à publier une communication sur la sphère de sécurité européenne en novembre 2013 concernant les citoyens de l'Union européenne et les entreprises établies sur son territoire [89]. Le projet de Règlement général sur la protection des données, proposé en 2012 par la Commissaire européenne Vivian Reding a quant à lui bénéficié de ce regain d'intérêt pour la sphère privée au sein des institutions européennes. Le processus législatif a ainsi été relancé en 2013. 137

surveillance dans divers États membres et incidences sur les droits fondamentaux des citoyens européens, débat du 11 mars 2014, in : Parlement européen (http ://www.europarl.europa.eu/), Bruxelles 2014, p. « http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-014&language=FR&ring=A7-2014-0139 » (27/10/2018).

87. Moraes Claude, *Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (A7-0139/2014)*, in : Parlement européen (http ://www.europarl.europa.eu/), Bruxelles 2014, p. « http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//FR » (27/10/2018).

88. Weber Rolf H. / Staiger Dominic, *Transatlantic Data Protection in Practice*, 1e éd., Zürich 2017, p. 47.

89. Commission européenne, *Communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire du 27 novembre 2013 - COM (2013) 847 final*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2013, p. « https://eur-lex.europa.eu/procedure/FR/1041465 » (21/03/2020).

D. L'invalidation de l'accord Safe Harbour par la Cour de Justice

138 La réussite du processus législatif européen en matière de protection des données vient également du fait que la Cour de Justice de l'Union européenne a invalidé le 6 octobre 2015, la décision de la Commission européenne selon laquelle les États-Unis d'Amérique garantissent un niveau de protection adéquat des données à caractère personnel [90].

139 Comment expliquer l'invalidation de l'accord Safe Harbor ?

140 L'affaire Schrems trouve son origine dans la demande d'un étudiant en droit autrichien, présentée auprès de l'autorité de contrôle irlandaise. Maximillian Schrems s'interrogeait sur la licéité des transferts de Facebook opérés entre l'Europe et les États-Unis, via son siège européen basé en Irlande. Maximillian Schrems demandait l'intervention de l'autorité de contrôle irlandaise pour interdire le transfert de données à Facebook vers les États-Unis, à la suite des prétendues activités des services de renseignements des États-Unis par la National Security Agency.

141 L'entreprise Facebook a donc été mise en cause par l'un de ses utilisateurs pour ne pas avoir respecté ses droits fondamentaux [91].

142 L'autorité de contrôle irlandaise a donné raison à l'entreprise Facebook. Elle a estimé que toute question relative au caractère adéquat de la protection des données à caractère personnel devait être tranchée en conformité avec la décision 2000/520 sur le Safe Harbour, et que dans cette décision, la Commission constatait que les États-Unis d'Amérique assuraient un niveau de protection adéquat de protection.

143 Max Schrems a interjeté appel de ce refus auprès de la High Court irlandaise. Celle-ci a demandé à la CJUE de se prononcer sur les questions préjudicielles suivantes :

— Est-ce qu'une autorité de contrôle indépendante chargée d'ap-

90. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :650, consid. 52.

91. Azoulai Loic / Van Der Sluis Marjin, *Institutionalizing personal data protection in times of institutional distrust : the Schrems Case*, in : Common Market Law Review 2016 53/5, p. « http://spire.sciencespo.fr/hdl:/2441/3n384hqii69kur2jo7dp0v1ta7 » (27/10/2018).

pliquer la législation sur la protection des données, saisie d'une plainte relative au transfert de données à caractère personnel vers un pays tiers, dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée, est ou non liée par la décision d'adéquation relative au Safe Harbor ?

— Est-ce que, dans le cas contraire, cette autorité peut mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission ?

144 La question posée à la CJUE était de déterminer dans quelle mesure les autorités de contrôle étaient liées par une décision d'adéquation concernant un pays tiers, ou si, au contraire, ces autorités devaient ou pouvaient mener leurs propres enquêtes, pour évaluer si ce pays tiers, qui bénéficie d'une décision d'adéquation, assurait toujours un niveau de protection adéquat des données transférées.

145 La CJUE a jugé qu'une décision d'adéquation ne pouvait pas priver les autorités de contrôle de leur pouvoir de contrôler les activités de transfert de données, malgré l'existence d'une décision d'adéquation s'appliquant dans l'UE. Le pouvoir d'enquête des autorités de contrôle n'est donc pas restreint par les décisions d'adéquation.

146 La CJUE a rappelé que seule la CJUE avait compétence pour invalider un acte de l'UE, tel qu'une décision d'adéquation. L'autorité de contrôle nationale ne dispose pas de cette prérogative et doit utiliser les voies de recours nationales pour effectuer un renvoi préjudiciel devant la CJUE, qui seule peut examiner la validité de la décision d'adéquation et invalider éventuellement celle-ci.

147 La CJUE a aussi défini ce qu'était un « niveau de protection adéquat ». Il s'agit d'un niveau de protection « substantiellement équivalent [92] » à celui de la directive et de la Charte dans l'UE, et « non pas identique ». Pour décider, la Commission vérifie si le pays tiers peut assurer effectivement un tel niveau de protection juridique du fait de son ordre juridique interne. Elle choisit donc le critère de la protection juridique.

148 Dans l'arrêt Schrems, la CJUE a constaté que les mesures de sécu-

92. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :627, consid. 73.

rité qui étaient en place dans l'accord Safe Harbor ne protégeaient pas suffisamment les droits des personnes. En faisant référence aux révélations d'Edward Snowden, la Cour constatait qu'il n'existait aucune protection suffisante contre des accès disproportionnés des autorités aux informations, concernant les données transmises aux États-Unis dans le cadre de l'accord Safe Harbor. Elle ajoutait qu'il n'existait pas non plus de protection juridique efficace contre de tels accès pour les personnes se trouvant hors des États-Unis [93].

149 L'accord Safe Harbor a donc été abrogé et remplacé par l'accord Privacy Shield (ou « accord de bouclier de protection de la vie privée »), qui fut adopté formellement le 12 juillet 2016 par la Commission européenne.

150 L'accord Safe Harbor était un programme d'adhésion volontaire mis en place par le Département du Commerce américain et la Commission européenne durant l'année 2000. Les entreprises américaines intéressées par l'adhésion à l'accord Safe Harbor devaient respecter un certain nombre de principes, basés sur le droit européen de la protection des données. Des sanctions étaient prévues en cas de manquement pour « misrepresentation » par la Federal Trade Commission.

151 L'invalidation de l'accord Safe Harbor a impacté plus de 4000 entreprises américaines, qui avaient adhéré à l'accord Safe Harbor [94].

152 Après l'invalidation du Safe Harbor par la CJUE, le groupe de travail de l'Article 29 de la Commission européenne s'est prononcé sur son contenu dans une publication du 13 avril 2016. Il a fait part de ses préoccupations importantes, concernant le volet commercial du Privacy Shield et l'accès, par les autorités publiques, aux données

93. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :627, consid. 89 ; Commission européenne, *Protection des données - Règles relatives à la protection des données à caractère personnel au sein et à l'extérieur de l'UE*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles s.a., p. « https://ec.europa.eu/info/law/law-topic/data-protection_fr » (27/10/2018).

94. Burton Cédric / Cadiot Sarah / De Boel Laura, *What's Next for U.S.-EU Data Transfers ? An Analysis of Recent Developments Following Schrems*, in : The WSGR Data Advisor (https ://www.wsgr dataadvisor.com/), s.l. 2015, p. « https://www.wsgrdataadvisor.com/2015/11/whats-next-for-u-s-eu-data-transfers-an-analysis-of-recent-developments-following-schrems/ » (26/10/2018).

transférées dans le cadre de l'accord Privacy Shield.

À la suite de cet arrêt, l'accord Safe Harbor a été jugé insuffisant par le Préposé fédéral à la protection des données suisse et a été officiellement abrogé par le Conseil fédéral [95]. La Suisse a conclu un accord « Privacy Shield » en janvier 2017 avec les Etats-Unis [96]. Pour que le nouveau cadre juridique « Privacy Shield » conclu en janvier 2017 entre la Suisse et les Etats-Unis, puisse se pérenniser et s'adapter à l'évolution des besoins, des évaluations annuelles ont été convenues avec les États-Unis et le Préposé fédéral à la protection des données. Ces évaluations seront menées par le SECO, assisté du Préposé fédéral à la protection des données, donnant lieu à un rapport annuel indépendant [97]. 153

E. L'accord « Privacy Shield »

Adopté le 12 juillet 2016, l'accord Privacy Shield encadre le transfert des données personnelles des citoyens européens vers des centres de données (data centers) situés aux États-Unis. Il repose sur un mécanisme volontaire de co-régulation et d'autocertification par les entreprises concernées. Les autorités américaines s'engagent à surveiller les pratiques des sociétés bénéficiant de cet accord, à corriger les abus et à sanctionner les entreprises fautives, y compris en matière pénale. 154

L'accord Privacy Shield vise à renforcer la protection juridique des personnes se trouvant hors des États-Unis, contre l'accès illégal des autorités américaines et des entreprises à ces informations. Le département d'État a créé un poste de médiateur pour traiter les plaintes provenant d'Europe. Mais cela ne saurait se confondre avec 155

95. Parlement suisse, *Suppression du Safe Harbor USA-UE en matière de protection des données. Quelles conséquences pour la Suisse ?*, in : Le Parlement suisse (https ://www.parlament.ch/), Berne 2015, p. « https : / / www . parlament . ch / fr / ratsbetrieb / suche - curia - vista / geschaeft ? AffairId = 20151068 » (27/10/2018).

96. PFPDT, *Swiss-US Privacy Shield : un nouveau cadre pour la transmission des données aux États-Unis*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa/swiss-us-privacy-shield--neuer-rahmen-fuer-datenuebermittlungen-.html » (27/10/2018).

97. PFPDT, *24ème Rapport d'activités sur la protection des données*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2017, p. « https : / / www . edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/25--taetigkeitsbericht-2017-2018.html » (27/10/2018).

le recours judiciaire qui est indépendant et a été exigé par la Cour de Justice.

156 Les services de renseignement et de police américains continueront d'intercepter et d'exploiter les données personnelles venues d'Europe, notamment dans les affaires de « sécurité nationale » (contre-espionnage, terrorisme, armes de destruction massive, etc.), « d'intérêt public » et de crime organisé. Elles pourront les garder cinq ans. La décision d'exécution de la Commission dresse la liste exhaustive des instances et des mesures techniques, administratives et judiciaires censées empêcher les Américains de répéter les pratiques révélées par Edward Snowden [98]. Des garanties sont offertes aux citoyens [99].

157 L'accord Privacy Shield a été reconnu par la Commission européenne comme offrant des garanties suffisantes pour transférer des données entre l'UE et les États-Unis, en vertu de la décision d'adéquation du 12 juillet 2016. Dès le 1er août 2016, les entreprises américaines ont pu confirmer leur adhésion à l'accord Privacy Shield.

158 Les principes de cet accord s'inscrivent dans le prolongement de l'accord Safe Harbor. De nouvelles restrictions et de nouveaux mécanismes de recours juridictionnels sont néanmoins apparus pour les citoyens européens. Le Privacy Shield intègre en outre des engagements du gouvernement américain concernant l'accès des autorités publiques américaines aux données personnelles en provenance de l'UE.

159 L'accord Privacy Shield fait apparaître sept nouveaux principes ainsi que seize principes additionnels.

— Obligation d'information détaillée : Les politiques de confi-

98. Commission européenne, *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (C(2016) 4176)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2016, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016D1250 » (03/06/2017).

99. Commission européenne, *La Commission européenne présente le paquet « bouclier de protection des données UE-États-Unis » : des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données - Communiqué de presse du 29 février 2016*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2016, p. « https : / / ec . europa . eu / commission/presscorner/detail/fr/IP_16_433 » (21/03/2020).

dentialité des entreprises adhérant au Privacy Shield doivent inclure treize types d'informations impératives.

— Droit d'opposition renforcé : Les citoyens européens doivent pouvoir s'opposer à la communication de leurs données à des tiers ou à une utilisation de ces données, pour une finalité «matériellement différente» de la finalité pour laquelle elles ont été collectées.

— Strict encadrement des transferts ultérieurs : les entreprises adhérant au Privacy Shield doivent encadrer les transferts ultérieurs de données vers d'autres entreprises comme leurs sous-traitants (sur une base contractuelle).

— Qualité des données et finalité du traitement : les entreprises certifiées doivent se limiter à traiter les données qui sont adéquates, pertinentes et non excessives pour les finalités du traitement et ne les traiter que pendant la durée n'excédant pas la durée nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées. Le projet initial du Règlement prévoyait à l'article 13 a que la personne concernée devait être informée si les données collectées étaient traitées pour d'autres finalités que celles de la collecte et si les données collectées allaient être transférées à des tiers, vendues et si elles étaient chiffrées. La proposition prévoyait une représentation des données à caractère personnel sous la forme de pictogrammes visuels, indiquant également si les exigences du Règlement étaient ou non remplies (croix rouge ou verte) [100]. Cette disposition ne figure plus dans la version définitive du Règlement.

— Renforcement des droits des citoyens européens : les personnes concernées en Europe peuvent demander l'accès aux données personnelles traitées les concernant ainsi que des informations à l'origine d'une décision produisant des effets juridiques à leur égard et qui a été prise sur le seul fondement d'un traitement automatisé de données (credit score [101]).

100. Fasnacht Tobias, *Die Einwilligung im Datenschutzrecht Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht*, thèse, Freiburg 2017, p. 153.

101. Bödi Richard, *Scoring als Methode zur Entscheidfindung*, in : Digma : Zeitschrift für Datenrecht und Informationssicherheit 2007 7/2, pp. 68-71.

— Moyens de recours des personnes concernées contre les entreprises américaines adhérant au Privacy Shield : les personnes concernées peuvent déposer une plainte directement auprès de l'entreprise, ou auprès des autorités de contrôle en Europe, qui travaillent en coopération avec les autorités américaines compétentes. Les personnes concernées peuvent également faire usage d'un mécanisme alternatif de résolution des conflits.

— Suppression des données : une entreprise américaine qui déciderait de ne plus adhérer au Privacy Shield doit supprimer les données collectées dans le cadre de son adhésion précédente ou s'engager à les utiliser dans le respect des principes du Privacy Shield.

160 Le site de l'Accord Privacy Shield indique que plus de 1750 entreprises américaines ont adhéré à l'accord Privacy Shield depuis le 1er août 2016 [102].

161 Pour le rapporteur du Règlement, Jan-Philipp Albrecht, les garanties offertes aux citoyens européens restent faibles [103] d'où les critiques postérieures de l'accord Privacy Shield. Il propose de privilégier des mesures de sécurité, incorporées en tant que mesures techniques et organisationnelles lors des transferts de données européennes vers les États-Unis.

162 L'accord Privacy Shield fait l'objet de deux recours en annulation près la CJUE de la part de Digital Rights Ireland [104] et de la Quadrature du Net (Arrêt CJUE, La Quadrature du Net et autres c. Commission, T-738/16). Les conclusions de l'avocat général sont attendues en décembre 2019.

II. L'effectivité du droit fondamental à la protection des données

163 Malgré l'espoir nourri par le Règlement et sa valeur contraignante dans l'UE, deux événements de l'année 2017 sont venus rappeler

102. Privacy Shield Framework, *Welcome to the Privacy Shield*, in : Privacy Shield Framework (https ://www.privacyshield.gov/), Washington D.C. s.a., p. « https://www.privacyshield.gov/welcome » (21/03/2020).
103. Albrecht Jan Philipp, *La ruée vers les datas*, in : Arte, Bruxelles 2016.
104. Arrêt CJUE du 22 novembre 2017, *Digital rights Ireland c. Commission*, T-670/16, ECLI :EU :T :2017 :838, consid. 20 ; Arrêt CJUE, *La Quadrature du Net et autres c. Commission*, T-738/16, ECLI :EU :T :2018 :520, consid. 1.

que l'effectivité du droit fondamental à la protection des données restait fragile et pouvait rapidement être remise en question.

A. Le cas d'espèce Wikileaks, du 7 mars 2017

Le 7 mars 2017, plus de 8761 documents publiés par Wikileaks ont confirmé l'utilisation par les services de renseignement américain (CIA-Center for Cyber Intelligence) et les services de renseignement britannique (GCHQ – Government Communication Headquarter) [105] de programmes de hacking pour infiltrer des objets connectés à Internet (iPhones, Android phones, télévisions, Whatsapp) et des systèmes d'exploitation (Microsoft, Mac et Linux). Ces révélations ont remis au cœur de l'actualité la question de la protection des données et rappelé qu'il s'agissait d'un droit fondamental garanti, au moins formellement, par la Charte des droits fondamentaux de l'Union Européenne [106]. Ces nouvelles révélations ont rappelé la crise de confiance des citoyens dans l'autorité de contrôle américaine et dans ses alliés, de même que dans les entreprises engagées dans les nouvelles technologies de l'information et des communications. 164

B. La suppression de la neutralité du Net, du 26 mars 2017

La politique européenne en matière de protection des données ne semble pas partagée de manière constante par les États-Unis. Trois mois après l'investiture du président américain Donald Trump à la Maison-Blanche, la chambre des représentants américaine a approuvé le 28 mars 2017, une résolution du Sénat, supprimant les règles favorables à la neutralité du Net, adoptées en octobre 2016 par la Federal Communications Commission à la demande du président Barack Obama. Cette disposition obligeait les fournisseurs de services internet (ou ISP) à demander aux utilisateurs leur consentement préalablement à toute collecte d'informations à caractère personnel (ex : informations de géo-localisation, informations financières, informations relatives aux mineurs, historique de na- 165

105. Privacy International, *Privacy International and nine other human rights organizations*, p. « http://privacyinternational.org/press-release/1316/privacy-international-and-nine-other-human-rights-organizations-pursue-landmark » (27/10/2018).

106. Union européenne, *Charte des droits fondamentaux de l'Union européenne (2012/C 326/02)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2012, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:12012P/TXT&from=FR » (27/10/2018).

vigation internet à des fins de marketing publicitaire). Désormais, les fournisseurs de services internet tels AT&T, Comcast Corp, et Verizon disposent du même statut juridique que d'autres acteurs comme Google ou Facebook. Ils ne sont pas obligés de demander aux utilisateurs leur consentement avant le traitement de leurs données personnelles. Cette décision, signée par le président américain Donald Trump, remet en cause le principe de neutralité de l'internet et fragilise la protection des données aux États-Unis [107].

166 La reconnaissance en octobre 2017 par Facebook, Google et Twitter de leur responsabilité dans la diffusion de fausses informations, sur mandat russe, pour influencer les élections américaines, a confirmé le besoin d'effectuer un contrôle des activités de ces acteurs économiques. Il n'est cependant pas très clair si un contrôle a priori ou a posteriori est le plus souhaitable.

C. La loi fédérale sur le renseignement en Suisse

167 La population suisse a accepté la loi sur le renseignement. Cette acceptation démontre que la population suisse privilégie la défense de la sécurité nationale à la défense du droit fondamental à la protection des données.

168 Ce renoncement à faire valoir son droit fondamental à la protection des données peut s'expliquer par la peur de la menace terroriste, qui justifierait l'atteinte à la sphère privée. La menace terroriste n'a cependant pas de caractère permanent et toute dérogation aux droits de l'homme et libertés fondamentales devrait être limitée dans le temps.

169 La loi fédérale sur le renseignement (LRens, R.S 121) a été largement acceptée par référendum avec 65.5% de voix, le 25 septembre 2016, et n'est pas limitée dans le temps.

170 La loi suisse sur le renseignement effectue cependant une pesée des intérêts en présence comme le requiert la CJUE et offre des garanties aux citoyens : les mesures extraordinaires qui sont à disposition du Service de Renseignement de la Confédération doivent être

107. Fung Brian, *Republicans voted to roll back landmark FCC privacy rules. Here's what you need to know*, in : The Washington Post (https ://www.washingtonpost.com/), Washington D.C. 2017, p. « https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/ » (27/10/2018).

autorisées par une instance de droit (notamment par le Tribunal administratif fédéral), avant que ce dernier ne puisse les mettre en pratique (art. 28). Pour certains cas, l'aval doit venir du Conseil fédéral. Une fois la mesure de recherche autorisée, le chef du DDPS décide s'il y a lieu de la mettre en œuvre après avoir consulté la Délégation pour la sécurité du Conseil fédéral (art. 29 et, pour l'exploration du réseau câblé, art. 39). La haute surveillance sur les activités du SRC sera attribuée au Parlement, plus précisément à la délégation des commissions de gestion (art. 77). Pour l'exploration radio, la loi prévoit des mesures de contrôle supplémentaires (art. 75). En cas d'urgence, l'autorisation peut cependant intervenir a posteriori.

171 Le principal argument du point de vue des droits humains à l'encontre de la nouvelle version de la Lrens concerne l'exploration du réseau câblé qui s'apparente à une forme de surveillance de masse non fondée sur des soupçons. De ce fait, il est possible de considérer, que sous cet aspect spécifique, il s'agit d'une ingérence disproportionnée dans la vie privée de nombreuses personnes. La question de l'adéquation de cette loi avec la jurisprudence de la CJUE [108]. se pose également.

172 Le processus législatif du Règlement est intervenu durant une période riche en innovations technologiques, à l'aube d'une révolution digitale [109].

§2 Le contexte technologique

173 Le Règlement a été élaboré dans le contexte d'une transition technologique. Celle-ci se caractérise par l'essor de plusieurs technologies digitales, dont les données à caractère personnelle sont la matière première [110]. L'accès aux données, leur utilisation et leur protection sont au cœur d'enjeux de pouvoir et d'enjeux commerciaux [111].

174 Si l'or jaune a joué un rôle historique central dans le fonctionne-

108. Arrêt CJUE du 21 décembre 2016, *Tele2 Sverige AB contre Postoch telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.*, C-203/15 21, ECLI :EU :C :2016 :970, consid. 15.
109. Harari, *Homo Deus*, p. 402.
110. Ross Alec, *The industries of the future*, 1e éd., London 2017, p. 152.
111. United States / Executive Office of the President / Podesta John, *Big data : seizing opportunities, preserving values*, Washington D.C. 2014.

ment du système monétaire international puis l'or noir (pétrole) dans le commerce international, l'or digital qu'est la donnée tient désormais une place stratégique dans l'essor économique et technologique des sociétés.

175 Le député européen Jan-Philippe Albrecht a d'ailleurs comparé la donnée au pétrole en précisant que la protection des données était comparable à l'émergence de la protection de l'environnement [112].

176 Le statut de droit fondamental consacré au droit de la protection des données par l'UE n'est pas reconnu dans tous les pays, comme un droit fondamental protégé constitutionnellement. En Asie, l'analyse et la valorisation économique des données personnelles constituent une priorité, au détriment de la protection des données personnelles [113].

177 Promettant des potentiels de valorisation gigantesques, la donnée fait désormais l'objet de moyens de collecte et d'analyse de grande envergure (Data Mining, Data Vizualization, Data Analytics, Data Scoring, Predictions) [114].

178 L'analyse des Big Data est source de nombreuses innovations technologiques et de nouveaux biens et services personnalisés. Elle crée un nouveau paradigme, pouvant remettre en cause la sphère privée des individus. Margo Seltzer, Professeur en informatique à l'université d'Harvard, indiqua en 2015, lors du Forum mondial de l'économie de Davos que « la vie privée telle que nous la connaissions dans le passé n'est plus possible. La façon dont nous la concevions auparavant, est dépassée [115]». Le XXIéme siècle apparaît comme une époque « post-privacy ».

179 En 2016, l'Office fédéral suisse de la communication a fait réaliser une étude sur la problématique du Big Data par la Haute École bernoise, intitulée « Big Data : atouts, risques et mesures néces-

112. Albrecht, *La ruée vers les data* (documentaire Arte).
113. Russell Stuart, *Panel Discussion "Developments and Challenges with the Data Economy"*, in : Big Data Summit (http ://www.bigdatasummit.co/) Melbourne 2017, p. « http://203.170.84.89/~idawis33/wordpress/program/BDS2017_Program.pdf » (27/09/2017).
114. Lemberger Pirmin, *Big data et machine learning : les concepts et les outils de la data science*, 2e éd., Malakoff 2016, p. 23.
115. *Idem*, p. 178, « Privacy as we knew it in the past is no longer feasible...How we conventionally think of privacy is dead ».

saires pour la Confédération [116]». La conclusion de cette étude précise qu'une intervention du législateur suisse serait nécessaire. Selon cette étude, il s'agit d'améliorer le fonctionnement du marché en donnant davantage de pouvoirs aux utilisateurs et en renforçant la réglementation et le contrôle des acteurs privés par l'Etat.

Le Règlement européen sur la protection des données réagit aux développements technologiques sans en faire mention directement, en vertu du principe de neutralité technologique. 180

Dans toutes les activités humaines, la mise à disposition en libre accès de données personnelles et leur combinaison avec des algorithmes nourrissent de nombreux espoirs dans les communautés scientifiques et le milieu de la recherche. 181

A titre d'exemple, la combinaison des Big Data et de données agricoles promet de réduire la pauvreté [117]. La combinaison des Big Data, du déchiffrage du génome humain et de l'industrie pharmaceutique promet le développement d'une médecine personnalisée (chaque médicament étant précisément adapté au génome du patient). La combinaison des Big Data et des outils de traduction promet l'élimination des barrières linguistiques et une plus grande compréhension et tolérance humaine entre des personnes aux langues et cultures différentes, grâce aux outils de traduction instantanée [118]. La combinaison des Big Data et des capacités d'apprentissage machine rend possible la reconnaissance faciale, vocale, ethnique, la reconnaissance d'objets [119]. Les traitements de données vocales (analyses, profilages) soulèvent le risque de l'usurpation d'identité et de 182

116. OFCOM, *Big Data : atouts, risques et mesures nécessaires pour la Confédération*, in : Le Conseil fédéral (https ://www.bakom.admin.ch/), Berne 2016, p. « https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/ofcom-infomailing/ofcom-infomailing-40/big-data--atouts--risques-et-mesures-a-prendre-pour-la-confedera.html » (21/03/2020).
117. Lemberger, *Big data et machine learning*, p. 159.
118. *Idem*, p. 160.
119. Jaggi Martin, *Fundamentals of AI*, in : AI Governance Forum (https :// ai-gf.com/), Geneva 2019, p. « https://ai-gf.com/ » (21/03/2020).

la discrimination [120].

183 L'ère digitale se caractérise par la mise à disposition d'un volume croissant de données à caractère personnel, et par l'émergence de nouvelles technologies fondées sur les données : objets connectés, clouds, intelligence artificielle, robotique, technologie Blockchain, FinTech, convergence entre la génétique, la nanotechnologie, l'informatique, la biotechnologie et les sciences cognitives. Il est fondamental de comprendre les interactions entre les données à caractère personnel et ces technologies, pour appréhender le Règlement dans sa globalité.

I. Les objets connectés

184 Un objet connecté échange des données à caractère personnel sur les réseaux de manière quasi permanente et instantanée, par l'intermédiaire d'une application Web ou mobile. Les failles de sécurité des objets connectés, peuvent être à l'origine d'un détournement de données à caractère personnel au profit de tiers non autorisés. L'utilisation malveillante des données interceptées, voire la prise de contrôle de l'objet connecté peuvent causer des dommages à leurs utilisateurs.

185 Dans une étude réalisée en 2014, la société Fortify, division d'Hewlet Packard dédiée à la cybersécurité, a constaté que sur dix objets connectés audités, 70 % ne cryptaient pas les données échangées avec le réseau, 80 % ne nécessitaient pas de mot de passe suffisamment complexe et 60 % n'offraient pas une interface Web suffisamment sécurisée [121].

186 Ainsi, le risque d'une perte de contrôle des données personnelles et le risque d'un profilage préjudiciable, est réel pour l'utilisateur d'objets connectés et d'applications mobiles. Pour faire face à ce risque, les autorités de contrôle pourraient diligenter des audits réguliers des applications pour tester si les serveurs qui stockent les

120. La CNIL s'est prononcée en juin 2019 en faveur d'un droit à la voix équivalent sonore du droit à l'image. Prise de position de la CNIL sur le droit à la voix : Vallet Félicien, *Les droits de la voix (2/2) - Quelle parole pour nos systèmes ?*, in : Laboratoire d'Innovation Numérique de la CNIL (https ://linc.cnil.fr/), Paris 2019, p. « https://linc.cnil.fr/les-droits-de-la-voix-22-quelle-parole-pour-nos-systemes » (27/06/2019).

121. Geoffray Sylvain, *HP publie un rapport alarmant sur la sécurité des objets connectés*, in : Aruco (https ://aruco.com/), s.l. 2014, p. « https://aruco.com/2014/07/hp-fortify-securite/ » (27/10/2018).

données collectées sont sécurisés de manière adéquate et si l'information qui est faite aux personnes concernées dans le traitement des données permet une prévention efficace.

La CNIL et 26 autres autorités compétentes membres du Global Privacy Enforcement Network (GPEN – réseau d'organismes agissant au sein de l'OCDE pour la protection de la vie privée) ont conduit un audit en ligne simultané de plus de 1 200 applications mobiles. Cet audit a démontré une carence manifeste dans l'information faite aux utilisateurs du traitement des données personnelles qui les concernent [122]. 187

II. Le marché des objets connectés

Le marché des applications et des objets connectés connaît une croissance fulgurante. L'institut Gartner table sur un parc de 8,4 milliards d'objets connectés dans le monde en 2017, soit une augmentation de 31 % par rapport à 2016. En 2020, près de 20,4 milliards [123]. En Janvier 2020 Thierry Breton, commissaire européen indiqua que « le volume mondial de données que nous traitons est de 35 zeta bites, c'est-à-dire 35 000 milliards de milliards de données. Et que ce volume double tous les 18 mois et qu'il atteindra 175 zeta bites dans cinq ans [124]». Si les données sont principalement stockées dans le Cloud et dans des centres de données, les données seront selon lui dans tous les objets connectés et la 5G jouera jouera un rôle clef dans ce déploiement [125]. 188

Au niveau global, la Chine, l'Amérique du Nord et l'Europe de l'Ouest sont les terres de prédilection des objets connectés. En 2017, ces trois zones rassemblent 67 % de l'internet des objets (IoT) selon 189

122. Maguire Michael, *2016 GPEN Privacy Sweep, Internet of Things : Participating Authorities' Press Releases*, in : Global Privacy Enforcement Network (https ://www.privacyenforcement.net/), s.l. 2016, p. « https://www.privacyenforcement.net/node/717 » (27/10/2018).
123. van der Meulen Rob, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, in : Gartner (https ://www.gartner.com/), Egham 2017, p. « https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 » (27/10/2018).
124. Grésillon Gabriel / Perrotte Derek / Barré Nicolas, *Thierry Breton : « Pour accéder au marché européen, il faudra accepter nos règles »*, in : Les Echos (https ://www.lesechos.fr/), Paris 2020, p. « https://www.lesechos.fr/monde/europe/thierry-breton-pour-acceder-au-marche-europeen-il-faudra-accepter-nos-regles-1161004 » (08/01/2020).
125. *Ibidem.*

l'Institut de prévision Gartner. La digitalisation de l'industrie en Europe a commencé et repose en partie sur les objets connectés [126]. Cette digitalisation devrait s'accélérer avec l'introduction de la 5G.

190 Les objets connectés sont présents dans des domaines très divers. Ils peuvent être portés par la personne (montres, vêtements, lunettes), dont les données à caractère personnel sont collectées ou bien se trouver dans son environnement (smart cities, immeubles, transports publics, parkings) et prélever des données à son insu. Dans cette seconde hypothèse, des senseurs et des capteurs connectés sont intégrés dans des objets du quotidien (objets connectés (smartphones, jeux pour enfants, véhicules, smart home, mobilier intelligents, trackers d'activité...). Ces objets connectés intègrent une application mobile, qui collecte, analyse, stocke et restitue une multitude de données en lien avec un utilisateur, son environnement, ses consommations, ses habitudes, son hygiène de vie ou encore sa santé [127].

III. Les applications

A. Le domaine médical

191 Dans le domaine de la santé (applications fitness, capteurs corporels) les objets connectés sont appréciés pour leur aspect ludique et motivant pour la pratique sportive. Ils peuvent favoriser le bien-être et la santé en général. Cependant, ils produisent une quantité considérable de données à caractère personnel. Ils présentent donc le risque d'une perte de contrôle des données et menace le droit fondamental à l'auto-détermination informationnelle [128]. Les données qui renseignent sur notre État de santé ou nos maladies sont qualifiées de particulièrement sensibles par la Loi fédérale suisse sur la protection des données (ci-après LPD) [129], et le Règlement [130] car leur transmission et leur traitement constituent une intrusion

126. Schweer Dieter / Sahl Jan Christian, *The Digital Transformation of Industry – The Benefit for Germany*, in : Abolhassan Ferri (édit.), *The Drivers of Digital Transformation : Why There's No Way Around the Cloud*, Cham 2017, pp. 23-31.
127. Berger Kurzen Brigitte, *E-health und Datenschutz*, thèse, Zürich 2004, pp. 1-229.
128. PFPDT, *24ème Rapport d'activités*, p. 27.
129. Loi fédérale sur la protection des données (LPD) du 19 juin 1992, FF 1992, p. 929 ss.
130. art. 9 RGPD.

massive dans la sphère privée [131]. Ces capteurs et applications fitness collectent des informations variées sur la santé des personnes concernées et rendent possible la création d'un profil personnalisé. Les données ainsi générées présentent un intérêt certain pour les acteurs économiques. Le fait que des tiers puissent avoir accès à des informations relatives à la santé des individus et les utiliser à des fins contraires à l'intérêt des personnes concernées peut avoir des effets néfastes majeurs [132].

Le séquençage du génome humain soulève également des questions de fond. Publié en 2003, le premier séquençage d'un génome humain (formé de 20 à 25 000 gènes) a pris dix ans, pour un coût de 3 milliards de dollars [133]. Aujourd'hui, quelques heures et un millier de francs suffisent, grâce aux techniques de «séquençage de prochaine génération» à haut débit. Ces techniques permettent aux généticiens de trouver des liens entre mutation de gènes et pathologies [134]. 192

Dans quel objectif ? Lorsqu'un patient est malade, lui administrer un traitement entièrement individualisé. Et lorsqu'il est en bonne santé, lui indiquer de quelles affections il pourrait souffrir à l'avenir, puis mettre en place avec lui des stratégies de prévention. 193

Comment ? Par le biais des objets connectés, qui collectent les données à caractère personnel. Ces données sont ensuite analysées par des robots ou par des algorithmes d'intelligence artificielle. IBM-Watson par exemple pourrait devenir l'interface privilégiée de la médecine du futur. Google, Apple ou Facebook, investissent également massivement dans ces technologies et disposent d'infrastructures pour analyser ces données médicales ainsi que de compétences sophistiquées en intelligence artificielle pour extraire du sens de ces données [135]. 194

Les systèmes de santé font face à une révolution inéluctable. Doit- 195

131. Härting Niko, *Datenschutz-Grundverordnung*, Köln 2016, p. 128.
132. PFPDT, *24ème Rapport d'activités*, p. 27.
133. Léchenet Alexandre, *Business, éthique, légalité... Le séquençage du génome en questions*, in : Le Monde (https ://www.lemonde.fr/), Paris 2014, p. « https://www.lemonde.fr/les-decodeurs/article/2014/08/18/le-sequencage-du-genome-comment-ca-marche_4472313_4355770.html » (27/10/2018).
134. *Ibidem.*
135. Lecrip, *E-santé et génétique : quand les Gafa s'emparent de notre ADN*, in : CRIP (https ://lecrip.org/), Nanterre 2016, p. « https://lecrip.org/2016/01/25/e-sante-genetique-gafa-semparent-de-adn/ » (27/10/2018).

elle être qualifiée de « triomphe de la médecine » comme le prétend le Dr Knock de Jules Romains pour qui « tout bien portant est un malade qui s'ignore » ? Le droit de ne pas savoir devrait-il être officiellement reconnu ?

196 Les traitements de données à caractère personnel sont au cœur des stratégies d'innovation des sociétés pharmaceutiques [136]. Bayer, Novartis, Genentech, Merck, Pfizer, Bristol-Meyers Squibb développent de nouveaux traitements personnalisés sur la base de l'analyse des données collectées.

197 Le marché des objets connectés dans le domaine de la lutte contre le diabète est un marché lucratif. L'Organisation Mondiale de la Santé indiquait dans son rapport d'avril 2016, que le nombre de personnes atteintes de diabète est passé de 108 millions en 1980 à 422 millions en 2014.

198 Dans ce domaine, Apple travaille au développement d'un lecteur de glycémie non invasif, intégrable au produit Apple Watch. La méthode est la même pour les personnes diabétiques de type 1 ou 2 ou gestationnel). Certains diabétiques ont préféré opter pour le lecteur Freestyle Libre, des laboratoires Abbott, qui s'implante sous la peau durant 15 jours. En scannant le code-barre du lecteur Freestyle avec le téléphone portable, l'utilisateur connaît son indice de glycémie, ce qui facilite la vie des diabétiques. D'autres laboratoires investissent dans l'implantation de capteurs pour mesurer la glycémie en continu. L'équipe de Google Life Science développe quant à elle étudie une lentille de contact capable de mesurer le taux de sucre dans le sang en continu. Le traitement des données sera donc effectué en continu.

199 En analysant les données de santé à caractère personnel, les compagnies d'assurance offrent des biens et des services personnalisés (médicaments personnalisés, dépistage des maladies, gestion des données médicales, relation avec le client).

200 Ainsi, les compagnies d'assurance évaluent-elles leur risque financier de manière précise grâce à la collecte de données personnelles

136. CNIL, *Objects Connectés*, in : Commission Nationale de l'Informatique et des Libertés (https ://www.cnil.fr/), Paris 2016, p. « https://www.cnil.fr/fr/thematique/internet-technologies/objets-connectes » (27/10/2018).

par le biais des objets connectés.

Les objets connectés dans le domaine de la santé, présentent l'avantage de donner accès à des données de santé mesurées à intervalle régulier, ce qui favorise le diagnostic et la prise de décision des médecins. Les médecins et les compagnies d'assurance sont ainsi mieux informés des comportements de santé du patient, tels que la quantité d'activité physique effectuée ou bien le type de médicaments pris. En étant mieux informés, les patients reçoivent des offres personnalisées spécifiques à leur situation. Pour les patients ayant des maladies graves, qui nécessitent parfois la prise de plus de plusieurs médicaments par jour, les outils de contrôle journalier permettront au médecin de vérifier que le traitement est bien pris et dans les bonnes quantités. A contrario, tout oubli pourrait-il être sanctionné par un non-remboursement des soins ou un renchérissement des primes ? Se poserait alors la question de la liberté de soin du patient, en plus de la disparition de son autonomie. 201

Pour Joël de Rosnay, la multiplication des données issues des différents capteurs que l'on peut porter sur soi, va permettre l'avènement d'un « tableau de bord de santé personnalisée [137] ». Selon lui, la médecine ne sera alors plus essentiellement basée sur l'aspect thérapeutique, mais sur la prévention quantifiable [138]. « Cette nouvelle approche de la santé pourrait aboutir à des programmes de maintenance de la santé prenant appui sur une médecine 4P, à savoir personnalisée, préventive, prédictive et participative. Il s'agit-là, de l'un des facteurs qui devrait profondément révolutionner l'industrie de la santé de demain [139]». 202

Il n'est pas exclu qu'à l'avenir, que ceux qui refuseront de voir leur activité surveillée pour s'assurer qu'ils prennent soin de leur santé paieront plus cher leur assurance, voire n'y accéderont plus. 203

Le montant de la prime d'assurance pourrait ainsi varier en fonction du contenu des données collectées, introduisant une obligation de monitoring de son État de santé ou de bien-être à intervalles réguliers voire en temps réel. Pour l'instant cette option est exclue en Suisse. Le conseiller fédéral Alain Berset s'est opposé en mai 2017 à une variation des primes d'assurance en fonction des données 204

137. De Rosnay Joël, *Je cherche à comprendre : les codes cachés de la nature*, 1e éd., Paris 2016, p. 26.
138. *Idem*, p. 80 ss.
139. *Idem*, p. 82.

collectées. Il a rappelé le principe d'égalité entre individus [140]. La CJUE viendra peut-être créer de nouveaux droits comme celui « de ne pas savoir » dans le domaine médical pour limiter les analyses et respecter la dignité de la personne humaine.

205 L'individualisation du risque suscite des craintes dans le domaine de la santé, car elle pourrait conduire à exclure certains individus du bénéfice d'une assurance, s'ils présentent un ratio risque/bénéfices désavantageux pour la compagnie d'assurance. Au niveau européen, la Commission pour la santé publique a indiqué en janvier 2017, dans sa proposition de résolution du Parlement européen, à l'intention de la commission des affaires juridiques [141], que « les compagnies d'assurance ou tout autre prestataire de service ne devraient pas être autorisés à utiliser des données issues des applications de santé électroniques dans le but de pratiquer des discriminations dans la fixation des prix, étant donné que cela irait à l'encontre du droit fondamental à l'accès au niveau de santé le plus élevé possible ».

206 En Suisse, le Préposé fédéral à la protection des données a ouvert en octobre 2017 une enquête concernant le programme de la société Helsana sur ces problématiques [142]. Le Préposé a rappelé à cette occasion que « le droit à l'autodétermination informationnelle est la règle pour toutes les prestations complémentaires facultatives qui impliquent un traitement de données. Chacun peut décider personnellement des services dont il veut bénéficier, ainsi que de la part de sphère privée qu'il est prêt à sacrifier en échange. Or, la valeur des données personnelles est souvent sous-estimée à cette occasion. Il en résulte que la quantité d'informations personnelles fournies est souvent plus grande que ne le demanderait effectivement le but

140. Berset Alain, *Berset plaide pour la numérisation de la santé*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2017, p. « https://www.tdg.ch/suisse/berset-plaide-numerisation-sante/story/31505261 » (27/10/2018).

141. Parlement européen, *Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*, in : Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2017, p. « https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_FR.html?redirect » (21/03/2020).

142. PFPDT, *Explications relatives aux capteurs fitness en lien avec les assurances*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/gesundheit/kranken--und-unfallversicherungen/erlaeuterungen-zum-einsatz-von-fitnesstrackern-im-versicherungsb.html » (27/10/2018).

poursuivi ».

La prolifération des capteurs et des dispositifs collectant des données à caractère personnel fait de la protection des données à caractère personnel un enjeu stratégique. 207

Les objets connectés facilitent la surveillance en temps réel des individus, car ils enregistrent et transmettent un volume massif de données partagées et analysées d'une manière unique et nouvelle [143]. Les données collectées par les objets connectés permettent d'atteindre un niveau de connaissance inédit des personnes physiques qui peut aboutir à un surveillance massive uniquement anticipée dans les romans de science-fiction [144]. Cet état de fait soulève la question de la liberté et de l'autonomie individuelle et incite à nous poser la question du sens du progrès et du contrôle de la technologie [145]. La reconnaissance d'une obligation de diligence (duty of care) des acteurs économiques et l'existence de recours effectifs pour les personnes concernées apparaissent comme des éléments indispensables pour offrir des garanties aux personnes concernées et rééquilibrer les rapports de force en présence. Cette approche s'inscrit dans le prolongement de la jurisprudence de la CJUE concernant le principe de proportionnalité et la pesée des intérêts. Les acteurs économiques doivent veiller en particulier à la licéité de la collecte des données, à l'information des personnes concernées, à la proportionnalité de la collecte et de la durée de rétention des données. Ce sont des éléments déterminants d'une gouvernance effective des données [146]. 208

Favoriser l'innovation tout en offrant des garanties pour les personnes concernées dans le domaine du respect des droits de l'homme et des libertés fondamentales deviennent des questions essentielles. 209

143. Maras Marie-Helen / Wandt Adam Scott, *Enabling mass surveillance : data aggregation in the age of big data and the Internet of Things*, in : Journal of Cyber Policy 2019.
144. Voir aussi le projet chinois et coréen de « Bright Internet » fondé sur la surveillance de masse des télécommunications par Internet, incluant l'internet des objets (protocole IPv6), justifiée par le principe de cybersécurité préventive, p. « http://brightinternet.org » (30/12/2019).
145. Fukuyama Francis, *La fin de l'homme : les conséquences de la révolution biotechnique*, Paris 2002, p. 33.
146. PFPDT, *Explications relatives aux capteurs fitness en lien avec les assurances*, p. 159.

B. Les bâtiments et villes « intelligentes »

210 L'exemple des villes intelligentes (ou «smart cities») est particulièrement pertinent dans une analyse de la protection des données. En effet, des données à caractère personnel sont massivement collectées dans les villes intelligentes. Les traitements qui en résultent permettent un monitoring en temps réel de l'activité urbaine ce qui facilite la délivrance des services et des biens aux citoyens. Les nombreux capteurs et objets connectés présents dans les « villes intelligentes » et les bâtiments promettent de révolutionner le mode de vie urbain [147].

211 Tout type de technologie est envisageable : des caméras de surveillance intégrant une technologie algorithmique de reconnaissance faciale, émotionnelle voir ethnique dans un objectif de sécurité. Des poubelles connectées à Internet et munies de capteurs favorisant la propreté des villes. Des capteurs multiples rendant possible le désengorgement des villes, leur sécurité et leur durabilité. Les technologies connectées peuvent aussi prendre la forme d'applications qui assistent les individus dans la recherche de places de parking [148], dans la gestion de la qualité de l'eau. Avec l'essor de l'internet des objets, des capteurs sont installés dans des objets connectés à internet au sein d'infrastructures publiques [149], sur ou à l'intérieur des bâtiments [150]. Ils collectent des données à caractère personnel, les transfèrent et les stockent dans des Clouds, parfois à

147. Nembrini Julien / Lalanne Denis, *Human-Building Interaction : When the Machine Becomes a Building*, in : Human-Computer Interaction - INTERACT 2017, pp. 348-369.
148. Stolfi Daniel H. / Alba Enrique / Yao Xin, *Predicting Car Park Occupancy Rates in Smart Cities*, in : Smart Cities 2017, pp. 107-117.
149. Botta Alessio, *Integration of Cloud computing and Internet of Things : A survey*, in : Future Generation Computer Systems 2016/56, pp. 684-700.
150. Verma Himanshu / Alavi Hamed S. / Lalanne Denis, *Studying Space Use : Bringing HCI Tools to Architectural Projects*, in : Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York 2017, pp. 3856-3866.

l'insu des personnes concernées [151].

Le projet de ville intelligente initié par l'entreprise Google au Canada [152] prévoit de construire de nouveaux quartiers sur 77 hectares en investissant 700 millions de francs. Ces villes intelligentes collectent des données personnelles par le biais de capteurs et de caméras et mesurent en temps réel les flux des piétons, la vitesse de circulation des piétons, le taux d'occupation des bancs publics, le niveau de propreté. Les bordures des routes pourront également se déplacer en fonction du trafic [153]. 212

La collecte des données via des capteurs ou des objets connectés contribue également à optimiser l'utilisation de l'espace à l'intérieur d'un bâtiment, à générer des économies énergétiques, et à améliorer le confort des occupants [154]. 213

Phénomène de mode ou réel changement de paradigme ? Certains envisagent la mise en œuvre de smart policy [155] et de nouvelles formes de démocraties [156]. 214

C. Le transport autonome et la circulation routière

Le transport autonome concerne toutes les formes de moyens de transport : le transport routier, ferroviaire, aérien et maritime, que 215

151. CNIL, *Smart city et données personnelles : quels enjeux de politiques publiques et de vie privée ?*, in : Commission Nationale de l'Informatique et des Libertés (https ://www.cnil.fr/), Paris 2017, p. « https://www.cnil.fr/fr/smart-city-et-donnees-personnelles-quels-enjeux-de-politiques-publiques-et-de-vie-privee » (27/10/2018) ; Future of Privacy Forum, *Shedding Light on Smart City Privacy*, in : FPF (https ://fpf.org/) Washington D.C. 2017, p. « https://fpf.org/2017/03/30/smart-cities » (25/06/2017) ; Alavi Hamed S., *Comfort : A Coordinate of User Experience in Interactive Built Environments*, in : Human-Computer Interaction – INTERACT 2017, pp. 247-257.
152. Project Sidewalk, p. « https://www.sidewalktoronto.ca » (29/06/2019).
153. Seydtaghia Anouch, *Google City, la ville intelligente futuriste qui inquiète*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2019, p. « https://www.letemps.ch/economie/google-city-ville-intelligente-futuriste-inquiete » (29/06/2019).
154. Brambilla Arianna, *"Our inherent desire for control" : a case study of automation's impact on the perception of comfort*, in : Energy Procedia 2017/122, pp. 925-930 ; Verma / Alavi / Lalanne, *Studying Space Use*, pp. 3856-3866.
155. Bostrom Nick / Roache Rebecca, *Smart policy : Cognitive enhancement and the public interest*, in : Contemporary Readings in Law and Social Justice 2010 2/1, p. 14.
156. Helbing Dirk, *Will Democracy Survive Big Data and Artificial Intelligence ?*, in : Helbing Dirk (édit.), *Towards Digital Enlightenment : Essays on the Dark and Light Sides of the Digital Revolution*, Cham 2019, p. 16.

les systèmes soient télépilotés, automatisés, connectés ou autonomes [157]. Les drones seront abordés dans une partie spécifique.

216 L'investissement dans les véhicules autonomes s'explique par la volonté d'améliorer la sécurité routière [158], « 90 % des accidents de la route pouvant être attribués à des erreurs humaines ». L'enjeu consiste donc à créer des algorithmes qui permettent d'éviter les accidents [159].

217 Comment appliquer la notion d'autonomie á des artefacts comme des robots ou des voitures autonomes ?

(a) Le premier concept de voiture autonome créé par Google.

(b) Le robot de livraison conçu par Starship Technologies (2015).

Figure 2.2 – Exemples de systèmes autonomes.

218 La mise en circulation des véhicules autonomes répond avant tout au souhait d'améliorer la sécurité routière [160]. « 90 % des accidents de la route pouvant être attribués à des erreurs humaine s». L'en-

157. Parlement européen, *Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*; Thayer Eric, *Adversarial Testing to Increase the Overall Security of Embedded Systems : A Review of the Process*, in : IEEE Control Systems 2017 37/2, pp. 104-108 ; Katsikas Sokratis K., *Cyber Security of the Autonomous Ship*, in : Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, New York 2017, pp. 55-56 ; Portouli Evangelia, *Public attitudes towards autonomous mini buses operating in real conditions in a Hellenic city*, in : IEEE Intelligent Vehicles Symposium (IV), Los Angeles 2017, pp. 571-576 ; Araki Brandon, *Multi-robot path planning for a swarm of robots that can both fly and drive*, in : IEEE International Conference on Robotics and Automation (ICRA), Singapore 2017, pp. 5575-5582.

158. Hilgendorf Eric / Seidel Uwe (édit.), *Robotics, autonomics, and the law : legal issues arising from the autonomics for industry 4.0 technology programme of the German federal Ministry for economic affairs and energy*, 1e éd., Baden-Baden 2017, p. 174.

159. *Idem*, p. 189

160. *Idem*, p. 174.

jeu consiste donc à créer des algorithmes qui permettent d'éviter les accidents [161]. Elle offre également des solutions alternatives au transport et à la livraison de marchandises comme le démontre l'activité de JD en Chine.

Deux exemples seront approfondis : les véhicules autonomes et les drones. 219

Cas 1 : les véhicules autonomes

Comment définir un véhicule autonome ? 220

La Suisse ne dispose pas encore de loi ni d'ordonnance spécifique aux véhicules autonomes. 221

Au niveau européen, il n'existe pas non plus de loi européenne spécifique aux véhicules autonomes. Le Parlement européen a cependant approuvé le rapport sur la robotique préparé par Mady Delvaux, en février 2017 [162]. Les députés européens ont souligné qu'un projet législatif était urgent et nécessaire pour clarifier les questions de responsabilité, en particulier pour les voitures sans conducteur. Ils ont appelé à un système d'assurance obligatoire et à un fonds supplémentaire pour garantir le dédommagement total 222

161. *Idem*, p. 189.

162. Parlement européen, *Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*, p. « https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_FR.html?redirect » (21/03/2020) ; Delvaux Mady, *Rise of the robots : Mady Delvaux on why their use should be regulated*, in : European Parliament News (http ://www.europarl.europa.eu/), Brussels 2017, p. « http://www.europarl.europa.eu/news/en/headlines/economy/20170109STO57505/rise-of-the-robots-mady-delvaux-on-why-their-use-should-be-regulated » (27/10/2018).

des victimes en cas d'accidents causés par ce type de voitures [163].

223 La proposition de résolution du Parlement européen ne définit pas les véhicules autonomes. Les annexes requièrent cependant de la Commission qu'elle développe une définition commune des véhicules autonomes qui tienne compte de la forme physique de l'enveloppe du robot, de la capacité d'apprentissage à travers l'expérience et l'interaction, de la capacité d'adaptation de son comportement et de ses actes à son environnement et de la capacité d'acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données avec l'environnement et l'analyse des données [164].

224 Le rapport du Parlement européen demande à la Commission de définir un ensemble unique de règles dans l'Union pour éviter l'apparition d'une « mosaïque de législations nationales qui entraverait le développement de véhicules autonomes, assurant un juste équilibre entre les intérêts des utilisateurs, des entreprises et d'autres parties concernées, tout en évitant la sur-réglementation [165] ».

225 Aux États-Unis, il faut distinguer la législation au niveau fédéral et au niveau des États fédérés [166].

226 Aux États-Unis, la chambre des représentants a approuvé à l'unanimité, en juin 2017, le projet de loi fédérale dédié aux voitures autonomes, intitulé « the Self-Drive Act [167] ». Ce projet vise à développer des normes de sûreté pour les véhicules autonomes. Il autorise

163. Parlement européen, *Robots et intelligence artificielle : les députés demandent des règles européennes en matière de responsabilité*, in : Parlement européen Actualité (http ://www.europarl.europa.eu/), Bruxelles 2017, p. « http : / / www . europarl . europa . eu / news / fr / press - room / 20170210IPR61808/robots-les-deputes-veulent-des-regles-europeennes-en-matiere-de-responsabilite » (30/10/2017) ; Parlement européen, *Projet de rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)) du 31 mai 2016*, in : Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2016, p. « https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_FR.pdf?redirect » (29/12/2019).

164. Delvaux, *Rise of the robots*, p. 14.

165. *Ibidem.*

166. United States Senate, *Laws and Regulations*, in : US Senate (https ://www.senate.gov/), Washington D.C. s.a., p. « https://www.senate.gov/reference/reference_index_subjects/Laws_and_Regulations_vrd.htm » (08/11/2017).

167. United States Congress, *The Self-Drive Act (H.R. 3388)*, in : US Congress (https ://www.congress.gov/), Washington D.C. 2017, p. « https : / / www.congress.gov/bill/115th-congress/house-bill/3388/text » (30/09/2017).

les constructeurs à tester 100 000 véhicules sur les routes américaines, même si ces véhicules ne remplissent pas les critères de sûreté actuels. Ce projet de loi impose aux constructeurs de véhicules autonomes de préparer un plan relatif à la protection de la vie privée, qui spécifie comment les données seront collectées, utilisées, partagées, et stockées par les véhicules autonomes. La compétence est donnée au département fédéral du commerce [168] pour juger des violations en matière de protection des données. Ce projet de loi doit être discuté puis approuvé par le sénat américain, avant d'être signé par le Président américain pour devenir Loi [169].

Le département américain du transport et de la sûreté des infra- 227
structures routières nationales (U.S. Dept. of Transportation and the National Highway Traffic Society) a également adopté en 2014 le standard de la « Society of Automotive Engineers (SAE International) ».

Le schéma ci-dessous (figure 2.3) présente les différents niveaux 228
d'autonomie des véhicules autonomes tels que définis par la « Society of Automotive Engineers ».

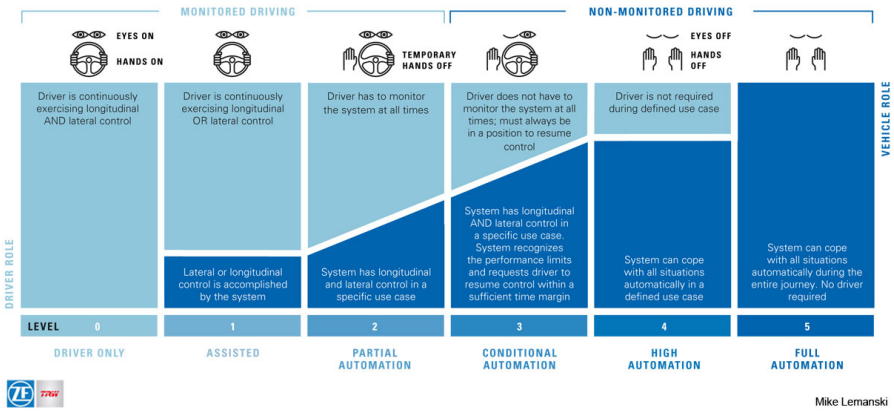

FIGURE 2.3 – Les différents niveaux d'autonomie des véhicules autonomes tels que définis par la "Society of Automotive Engineers". Source : Université de Birmingham.

168. Section 5 of the Federal Trade Commission Act.
169. GRIGORIAN Christopher H. / ENGLUND Nicholas / HAAKE Jack G., *Self Drive Act Passes the House as Senate Prepares Its Own Bill*, in : The National Law Review (https ://www.natlawreview.com/), Chicago 2017, p. « https://www.natlawreview.com/article/self-drive-act-passes-house-senate-prepares-its-own-bill » (27/10/2018).

229 En fonction de leur degré d'autonomie, les véhicules autonomes présentent la caractéristique de pouvoir s'affranchir de toute supervision [170]. Pour un observateur extérieur au véhicule, il est cependant difficile de savoir sur quel mode opère le véhicule (autonome, ou contrôlé) [171].

230 Aux États-Unis, les constructeurs s'interrogent sur les aspects juridiques de l'utilisation de véhicules de niveau 3. Que se passera-t-il si le conducteur n'est pas capable de reprendre le contrôle de son véhicule en cas d'accident ? Par conséquent, certains constructeurs comme Ford envisagent d'automatiser leurs véhicules au niveau 4 directement [172].

231 Le délai de réaction du conducteur en cas de reprise de contrôle imprévue du véhicule a également fait l'objet d'une mention spécifique dans le rapport Mady du Parlement européen, car il revêt une importance capitale.

232 Le développement de véhicules de plus en plus autonomes fait émerger une nouvelle problématique dénommée « dilemme du contrôle [173] ». Il s'agit de déterminer l'auteur d'un accident lorsque le véhicule est un véhicule autonome.

233 Lors du Sommet de Genève dédié à l'intelligence artificielle qui s'est tenu le 22 septembre 2017, l'avocat Me Bensoussan a démontré qu'une voiture autonome peut décider seule de percuter une voiture A au lieu d'une voiture B, lors d'un accident inévitable, sur le seul critère du nombre de passagers des voitures A et B. Doit-elle être qualifiée d'auteur de l'accident ?

234 À ce jour le département fédéral américain définit les normes de sûreté et de sécurité des véhicules traditionnels (air bag, ceinture de sécurité, assurance, permis de conduire...). Cependant, ces régle-

170. Fagnant Daniel J. / Kockelman Kara, *Preparing a nation for autonomous vehicles : opportunities, barriers and policy recommendations*, in : Transportation Research Part A : Policy and Practice 2015/77, pp. 167-181.

171. Richards Neil M. / Smart William D., *How should the law think about robots ?*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot law*, 1e éd., Cheltenham 2016, pp. 3-22.

172. HALO Attorneys, *Self Driving Cars - More Questions Than Answers*, in : HALO Attorneys (https ://www.halo-attorneys.com/), Las Vegas 2020, p. « https://www.halo-attorneys.com/self-driving-cars/new-rules-of-the-road.html » (21/03/2020).

173. Hilgendorf / Seidel, *Robotics, autonomics, and the law*, p. 187.

mentations ne sont pas applicables aux voitures autonomes, à leur design et au contrôle de leur fonctionnement. Comment estimer la qualité des différents modèles de voitures autonomes ? Toutes n'ont pas les mêmes standards en termes de respect de la vie privée, sûreté, sécurité, fiabilité, commodité.

L'État du Nevada [174] et l'État de Californie disposent de législations spécifiques aux véhicules autonomes. 235

L'État du Nevada définit un véhicule autonome comme un « véhicule équipé d'un système de conduite automatisé, conçu pour fonctionner avec un niveau d'automatisation de niveau 3, 4 ou 5 sur l'échelle définie par la Society of Automotive Engineers [175] ». 236

L'État du Nevada est le premier à avoir adopté une réglementation en la matière. Les véhicules seront marqués d'une plaque d'immatriculation rouge durant les phases de test. Si la technologie est approuvée, la couleur de la plaque d'immatriculation deviendra verte. (les plaques d'immatriculation américaines classiques sont grises). Les véhicules devront impérativement contenir 2 personnes, l'une pouvant prendre le contrôle du véhicule si besoin. Chaque véhicule contiendra un système de boîte noire destiné à enregistrer les données collectées par les senseurs, si bien que les informations seront disponibles jusque 30 secondes avant une collision. 237

L'État de Californie définit un véhicule autonome [176], comme un «véhicule équipé d'une technologie constituée d'un équipement et de logiciels qui procèdent à la conduite avec ou sans personne phy- 238

174. Assembly Committee on Transportation, *AB69 Law, An Act relating to transportation : revising requirements for the testing or operation of an autonomous vehicle on a highway within this State ; authorizing the use of driver-assistive platooning technology ; authorizing the use of a fully autonomous vehicle to provide transportation services in certain circumstances by persons licensed by the Department of Motor Vehicles, Nevada Transportation Authority or Taxicab Authority ; providing for the regulation of autonomous vehicle network companies ; providing penalties ; and providing other matters properly relating thereto*, in : NELIS (https ://www.leg.state.nv.us/), Las Vegas 2017, p. « https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/4750/Overview » (27/10/2018).

175. *Idem*, p. 4.

176. State of California, *Autonomous Vehicles in California*, in : California DMV (https ://www.dmv.ca.gov/), Sacramento 2019, p. « https://www.dmv.ca.gov/portal/wcm/connect/caa2f466-fe0f-454a-a461-f5d7a079de49/avexpressterms_31017.pdf?MOD=AJPERES » (10/12/2019).

sique contrôlant le véhicule en continu [177]. La notion de « Dynamic driving task » se réfère à toutes les fonctions en temps réel requises pour faire fonctionner un véhicule routier, à l'exclusion des destinations finales et intermédiaires, et incluant, sans limite, la détection d'objets et d'événements, la reconnaissance et la classification, la réponse à des objets et à des événements, la planification de manœuvres... [178]».

239 Les véhicules autonomes sont insérés dans un environnement ouvert, évolutif et complexe, soumis à de fortes variations [179]. Ils sont en interaction avec des humains situés à l'intérieur et à l'extérieur du véhicule autonome [180]. Ils pourront également interagir avec des agents autonomes à l'avenir.

240 Le Parlement européen de même que les États-Unis souhaitent modifier certains accords internationaux tels que la convention de Vienne sur la circulation routière du 8 novembre 1968 et la convention de La Haye du 4 mai 1971 sur la loi applicable en matière d'accidents de la circulation routière.

241 La transition vers des véhicules autonomes aura des répercussions dans les domaines suivants : la responsabilité civile (responsabilité et assurance), la sûreté et la sécurité routière, tous les sujets concernant l'environnement (par exemple efficacité énergétique, utilisation de technologies et de sources d'énergie renouvelables), la gestion et la protection des données (accès aux données, protection des données personnelles et de la vie privée, partage des données, etc.), la gestion des infrastructures de TIC (par exemple couverture dense de moyens de communications efficaces et fiables), et la gestion des ressources humaines (création et destruction d'emplois, formation

177. « *Vehicule Code* » par. 227.02, Section 38750 ; Cf. la version anglaise : "vehicle equipped with technology that is a combination of both hardware and software that performs the dynamic driving task with or without a natural person continuously controlling the vehicule".

178. Voir la version anglaise : "All of the real time functions required to operate a vehicle in on-road traffic, excluding selection of final and intermediate destinations, and including without limitation : object and event detection, recognition, and classification ; object and event response ; maneuver planning...".

179. Strowel Alain, *Robots et gouvernance des données : avons-nous besoin de nouveaux droits et devoirs ?*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https : / / www . isdc . ch / fr / evenements / prochains - evenements/droit-robot » (21/03/2020).

180. *Ibidem.*

des conducteurs de poids lourds à l'utilisation de véhicules automatisés, etc.) [181].

La responsabilité

Le Parlement européen estime que la responsabilité civile pour les dommages causés par les véhicules autonomes est une question essentielle qui mérite d'être analysée et à laquelle il importe de répondre au niveau de l'UE afin de garantir le même niveau d'efficacité, de transparence et de cohérence dans la mise en œuvre de la sécurité juridique dans chaque État membre, dans l'intérêt des citoyens, des consommateurs et des entreprises. 242

Compte tenu de la multiplicité des acteurs, la clarification du régime de responsabilité en cas de dommage est au coeur des enjeux de confiance du secteur automobile. Afin d'indemniser les victimes potentielles en cas d'accident, un régime de responsabilité strict est envisagé en parallèle d'un régime fondé sur la gestion du risque. Le régime de responsabilité strict nécessite de rapporter uniquement la preuve des dommages causés, la relation de causalité entre le dommage causé et le fonctionnement dommageable du véhicule autonome. 243

La Corée du Sud a adopté un modèle de responsabilité stricte, sans faute pour la circulation routière des véhicules autonomes. Ce régime de responsabilité s'applique également aux robots dans ce pays. 244

En revanche, le Parlement européen retient que l'approche fondée sur la gestion du risque ne se concentre pas sur la personne qui a agi de manière négligente, mais sur la personne capable, dans certaines circonstances, de réduire au minimum les risques et de gérer les répercussions négatives. 245

Il souligne que la responsabilité doit être imputable à un humain et non au véhicule autonome. 246

Il demande à la Commission une proposition de loi dans un horizon de 10 à 15 ans. Compte tenu des développements rapides de l'innovation dans ce domaine (des taxis autonomes étant prévus par exemple à Paris en 2018), les lignes directrices et les codes de 247

181. Ford Martin, *Rise of the robots : technology and the threat of a jobless future*, New York 2015, p. xiii.

conduite joueront un rôle clef.

248 Le Royaume-Uni a adopté en 2018 le « *U.K. Automated and Electric Vehicles Act* » selon lequel le conducteur doit être responsable quelle quoi soit la faute durant la conduite autonome et sera indemnisé par la compagnie d'assurance. La compagnie pourra se retourner contre le fabricant de véhicules autonomes et les autres parties prenantes au litige pour obtenir le remboursement du coût du dommage.

249 Dans les systèmes juridiques romano-germaniques, le droit de la responsabilité lie en général la responsabilité à un comportement humain, qui a pour effet de provoquer le dommage (lien de causalité). Dans le même temps, la responsabilité personnelle pour la mise en danger d'autrui constitue une des raisons principales à l'engagement de la responsabilité d'une personne.

250 La question de la responsabilité est complexe pour les véhicules autonomes, car ce n'est pas une personne qui décide, mais une machine « intelligente » sur la base d'un algorithme programmé par un individu ou un groupe d'individus. Les décisions sont donc prises sur une base automatisée, dont la logique dépend directement du design, du modèle de l'algorithme et des données d'entraînement. Avant toute mise sur le marché, la performance d'un système algorithmique devrait être contrôlée avec de nouvelles données.

251 La question de l'identification de l'auteur du dommage aux personnes et aux biens, et celle de la responsabilité des agents autonomes prennent une importance majeure á l'ère digitale. Le degré d'autonomie varie en outre d'un véhicule à l'autre ce qui aura des répercussions sur le régime de responsabilité. Pour des raisons de facilité, la responsabilité stricte a été adoptée comme une solution par défaut, pour compenser les difficultés d'allocation de la responsabilité et garantir l'indemnisation des victimes en cas d'accident.

252 La jurisprudence montre que les données deviennent essentielles à la compréhension d'un accident et à la preuve de la responsabilité du dommage. En 2017, un accident mortel s'est produit avec une voiture autonome (Tesla modèle S, avec un système Autopilote) suite à manœuvre d'un camion. Les caméras n'ont pas fait la distinction entre le véhicule et le ciel, car il y avait beaucoup de lumière. Cependant, la boîte noire (Event Data Recorder) a révélé

que le conducteur n'a laissé ses mains sur le volant que 25 secondes pendant les 37 minutes précédant l'accident. Des avertissements avaient été envoyés au conducteur par le système d'Autopilote [182].

En 2017, seuls Audi et Tesla proposent des véhicules autonomes en Suisse [183]. Volvo effectue des tests en Suède [184]. Aux États-Unis, les acteurs Tesla et Google (Waymo) ont déjà mis en circulation des véhicules autonomes [185]. 253

En France, des tests de circulation ont débuté le 2 octobre 2017 dans le cadre d'un partenariat entre Renault, la métropole de Rouen et la région Normandie, d'un montant de près de 10 millions d'euros pour trois ans. Ces tests ont permis, à quatre voitures autonomes d'effectuer en toute autonomie trois boucles totalisant 10 kilomètres. Ce projet vise à rendre possible la commande d'un véhicule autonome en temps réel par l'intermédiaire de son smartphone. 254

Cependant, comme en atteste le cas Flynn v. FCA US LLC (3 :15-CV-00855-SMY-RJD), la sécurité des véhicules connectés à internet doit être améliorée. Certains véhicules Fiat-Chrysler peuvent être hackés et contrôlés à distance, par le biais du UConnect système. Aucun dommage n'a été reporté dans ce cas, mais un recours collectif a été effectué par des acheteurs contestant le prix du véhicule, trop élevé selon eux, car correspondant à un niveau de sécurité qui ne reflétait pas la réalité. Le procès est prévu en octobre 2019 dans l'Illinois (« Southern District of Illinois ») [186]. 255

Le régime de responsabilité devant s'adapter à des menaces multi- 256

182. Waters Richard, *US agency criticises Tesla over fatal crash*, in : Financial Times (https ://www.ft.com/), London 2017, p. « https : / / www . ft . com / content/a040c84a-97d1-11e7-a652-cde3f882dd7b » (27/10/2018).
183. Meunier Nicolas, *Audi A8, un pas de plus vers la voiture autonome*, in : Challenges (https ://www.challenges.fr/), Paris 2017, p. « https : / / www . challenges . fr / automobile / nouveautes / audi - a8 - un - pas - de - plus - vers - la-voiture-autonome_486469 » (27/10/2018).
184. Test Site Sweden, *DriveMe*, in : Test Site Sweden (https://www.testsitesweden.com/), Lindholmen s.a., p. « https://www.testsitesweden.com/en/projects-1/driveme » (10/12/2019).
185. Guizzo Erico, *How google's self-driving car works*, in : IEEE Spectrum Online 2011 18/7, pp. 1132-1141.
186. International Telecommunication Unit, *Cybersecurity and Artificial Intelligence : How to allocate Liability between the stakeholders ?*, in : WSIS Forum (https://www.itu.int/), Geneva 2019, p. « https://www.itu.int/net4/wsis/forum/2019/Agenda/ViewSession/186 » (08/04/2019).

formes en plein évolution (« fake sensors », « virus ransomwares », « absence d'analyse contextuelle des systèmes de reinforcement learning »), les assureurs pourraient récompenser les entreprise qui adoptent des mesures de sécurité efficaces en diminuant leur niveau de primes afin de les encourager [187].

257 Dans l'UE, le Cybersecurity Act offre la possibilité d'une certification dans le domaine de la cybersécurité, afin de démontrer sa conformité ex-ante avant la mise en circulation du véhicule. Ceci constitue une avancée majeure dans le domaine de la sécurité des véhicules autonomes.

258 Le 8 avril 2019, la Commission européenne a publié des lignes directrices intitulées : « Building Trust in Human-Centric Artificial Intelligence » afin de poser le cadre juridique de la confiance dans les systèmes d'intelligence artificielle, à la base des véhicules autonomes.

Un régime d'assurance robotique

259 Le Parlement européen recommande la création d'un régime d'assurance « robotique » applicable aux véhicules autonomes. Celui-ci devrait tenir compte de toutes les responsabilités potentielles d'un bout à l'autre de la chaîne. De manière similaire aux véhicules à moteur, ce régime d'assurance pourrait être complété par un fonds, afin de garantir un dédommagement financier des victimes en cas d'accident.

260 Le rapport Mady demande au secteur de l'assurance de développer de nouveaux produits et de nouvelles offres, adaptés aux progrès de la robotique.

261 La Commission va examiner les points suivants :

a) la mise en place d'un régime d'assurance obligatoire, lorsque cela est justifié et nécessaire pour certaines catégories de robots. Les fabricants ou les propriétaires de robots devront ainsi contracter une police d'assurance couvrant les dommages potentiels causés par les robots ;

b) la mise en place d'un fonds de compensation, dont la fonction principale serait de garantir un dédommagement même

187. *Ibidem.*

lorsque les dommages ne sont pas couverts par une assurance ;

c) la possibilité pour le fabricant, le programmeur, le propriétaire ou l'utilisateur de contribuer à un fonds de compensation ou de contracter conjointement une assurance afin de garantir la compensation des dommages causés par un robot et de bénéficier en conséquence d'une responsabilité limitée ;

d) le choix entre la création d'un fonds général pour tous les robots autonomes intelligents ou la création d'un fonds individuel pour chaque catégorie de robot, ainsi que le choix entre un versement forfaitaire lors de la mise sur le marché du robot et des versements réguliers tout au long de la vie du robot ;

e) la création d'un numéro d'immatriculation individuel, inscrit dans un registre spécifique de l'Union, afin de pouvoir toujours associer un robot au fonds dont il dépend ; ce numéro permettrait à toute personne interagissant avec le robot de connaître la nature du fonds, les limites en matière de responsabilité en cas de dommages matériels, les noms et les fonctions des contributeurs et toute autre information pertinente ; et

f) l'introduction d'un instrument adéquat destiné aux consommateurs qui souhaitent demander conjointement une réparation, de la part des entreprises productrices responsables, des dommages découlant du mauvais fonctionnement de machines intelligentes [188].

Protection des données et véhicules autonomes

En parallèle des questions relatives à la détermination du régime de responsabilité et du schéma d'assurance applicable, la problématique de la protection des données à caractère personnel (accès aux données, protection des données, vie privée, partage des données) se pose pour les véhicules autonomes. 262

Les voitures autonomes sont dotées de capteurs qui collectent des données à caractère personnel. Un schéma synthétique présente ci-dessous (figure 2.4) les spécificités des véhicules autonomes. 263

La figure précédente illustre l'étendue des traitements de données par les voitures autonomes. En Septembre 2018, Google a signé un 264

188. Delvaux, *Rise of the robots*, point 59.

accord avec le groupe Nissan-Renault-Mitsubihi pour intégrer le système d'exploitation Android dans les 10 millions de véhicules produits par les trois marques. La firme offrira tous les logiciels embarqués, de la vidéo de You Tube à la commande vocale, de la cartographie à la climatisation de l'habitacle, mais aussi des instru-

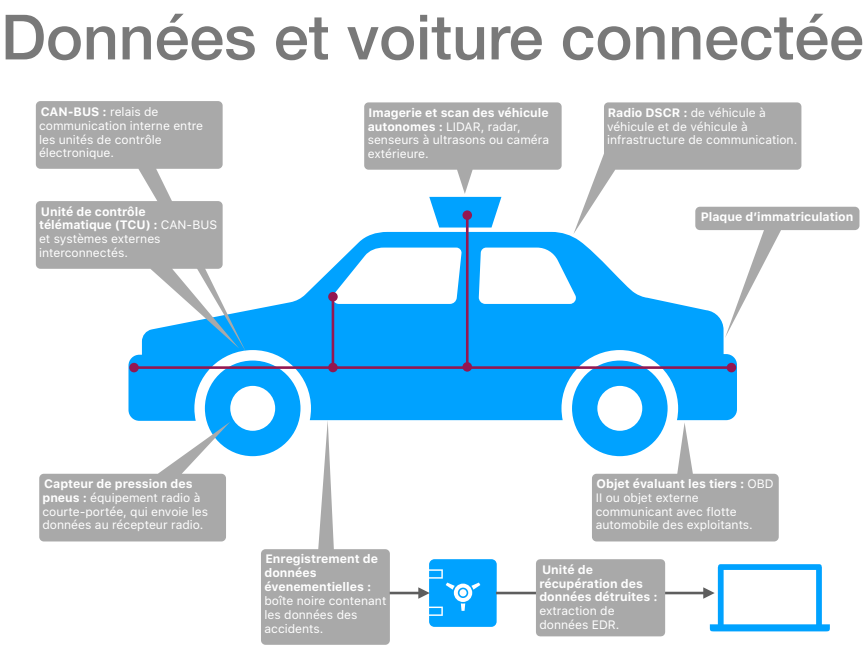

Figure 2.4 – Données collectées par les voitures autonomes.

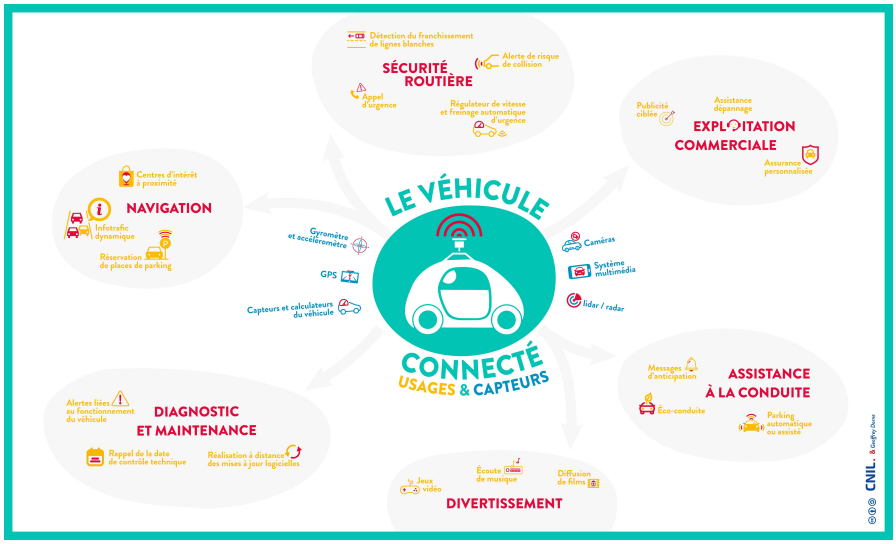

Figure 2.5 – Véhicule connecté, usages et capteurs. Source : CNIL.

ments utiles à la conduite. Elle pourra recueillir des informations importantes sur les conducteurs et continuer ainsi à utiliser toutes les informations privées [189].

Les données peuvent être traitées de manière illicite, à l'insu de leurs utilisateurs. En l'absence de contrôle *a posteriori*, tenant compte de la nature du traitement de données personnelles (collecte de données vocales, visuelles (données oculaires (regard) pour évaluer l'état de fatigue du conducteur), données sur le style de conduite, données de santé...), avant d'autoriser le véhicule à circuler, seule une action civile *a posteriori*, une fois le dommage constaté, est envisageable. Le législateur devrait imposer une analyse des risques tenant compte de la protection des données et de considérations éthiques lors de la délivrance d'une autorisation de mise en circulation du véhicule autonome. Afin de s'assurer de la licéité des traitements de données personnelles, les parties prenantes que sont les constructeurs, assureurs, exploitants de flottes de véhicules, autorités locales, etc, doivent être particulièrement vigilantes sur l'existence et la validité du consentement demandé et sur l'information des personnes concernées. 265

Il n'est pas exclu que les données personnelles relatives au comportement de conduite du conducteur et à sa vigilance [190] soient transférées en temps réel à la compagnies d'assurance du conducteur. En contrepartie, la prime d'assurance serait ajustée avec des bonus ou des malus en fonction de la qualité de la conduite [191]. 266

Le schéma ci-dessous (figure 2.5) présente les différents échanges de données entre le véhicule autonome et des sources externes [192]. 267

Anticipant cette évolution et afin de soutenir l'ensemble des parties prenantes, la CNIL a élaboré des lignes directrices pour une utilisation responsable des données collectées par les véhicules autonomes. Parmi ces données à caractère personnel figurent les don- 268

189. Fontanel / Sushcheva, *La puissance des GAFAM*, p. 9.
190. Zhu Zhiwei / Ji Qiang, *Eye and gaze tracking for interactive graphic display*, in : Machine Vision and Applications 2004 15/3, pp. 139-148.
191. Boshell Paige M., *The Power of Place : Geolocation Tracking and Privacy*, in : Business Law Today (https ://businesslawtoday.org/), Chicago 2019, p. « https : / / businesslawtoday . org / 2019 / 03 / power - place - geolocation - tracking-privacy/ » (19/06/2019).
192. CNIL, *Véhicules connectés : un pack de conformité pour une utilisation responsable des données*, in : Commission Nationale de l'Informatique et des Libertés (https ://www.cnil.fr/), Paris 2017, p. 1.

nées relatives aux trajets effectués, aux dates des contrôles techniques, au nombre de kilomètres ou au style de conduite.

269 L'autorité de contrôle française a sensibilisé les acteurs économiques du secteur automobile sur les principes de transparence et de loyauté de la collecte. Elle considère ainsi que l'effectivité de ces principes nécessite a minima une information des personnes concernées et le recueil de leur consentement [193].

270 Dans le même esprit que le Règlement européen, la CNIL est favorable à une approche de protection des données dès la conception (« Privacy by Design ») pour les véhicules autonomes. Elle propose trois modèles afin de respecter la protection des données.

271 Le premier scénario propose que les données à caractère personnel collectées dans le véhicule restent dans le véhicule sans transmission au fournisseur de services. Les données sont donc conservées localement. De solides garanties en matière de vie privée sont offertes par ce scénario. Le traitement des données s'effectue directement dans le véhicule aux fins d'afficher des conseils de conduite directement sur le tableau de bord.

272 Le second scénario propose une transmission des données collectées par le véhicule pour fournir un service à la personne. Citons par exemple le cas d'un contrat « pay as you drive » souscrit auprès d'une compagnie d'assurance.

273 Le troisième scénario transmet les données collectées à l'extérieur du véhicule pour déclencher une action automatique dans le véhicule. Citons l'exemple de l'envoi d'informations de géolocalisation (Info trafic) pour bénéficier d'un nouvel itinéraire en cas d'accident [194].

274 Du fait de l'enregistrement continu des données et de l'interaction avec d'autres agents sur la route, les voitures autonomes connec-

193. CNIL, *Véhicules connectés*.

194. Une démarche similaire a été conduite par l'industrie américaine en janvier 2017. Un guide à destination des utilisateurs de voitures autonomes a été publié pour les sensibiliser à la question de la protection des données : Future of Privacy Forum, *FPF and NADA Launch Guide to Consumer Privacy in the Connected Car*, in : FPF (https ://fpf.org/) Washington D.C. 2017, p. « https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car/ » (22/06/2017) ; CNIL, *Véhicules connectés*.

tées collectent plus de données que les boîtes noires [195].

Les données collectées par les boîtes noires rendent plus aisées l'amélioration des voitures pour les constructeurs (données sur batteries ou injection) [196]. Pour les assureurs, elles facilitent la personnalisation des contrats d'assurance afin d'offrir des contrats basés sur l'usage (durée et conduite) et sur le concept « Pay as you drive ». L'accès aux données permet le déclenchement d'alertes automatiques facilitant la mise à disposition de services d'assistance. Pour les gestionnaires de l'infrastructure routière, l'accès aux données rend possible une supervision de l'utilisation de l'infrastructure, ce qui favorise sa gestion. Pour les concessionnaires et garagistes, les données facilitent l'entretien des véhicules. Pour les fournisseurs de services, les données de géo-localisation achetées donneront lieu à des publicités personnalisées pour des restaurants et des magasins. 275

Une des questions essentielles est de définir qui contrôle les données collectées traitées par les véhicules autonomes et à qui elles appartiennent : au constructeur du véhicule ? à son propriétaire ? au fournisseur du dispositif du traitement des données ? (GPS, smart phone...), à l'assureur ? Quid des données relatives au bien-être physiologique des passagers (ex : données de santé) [197] ? 276

Une autre question essentielle est de savoir comment le système doit réagir, si les données collectées révèlent une détérioration de l'état de santé des passagers à court ou à long terme [198] ? Si les données sont disponibles pour une analyse, de quelles garanties bénéficient les passagers, et quels sont les devoirs des constructeurs ? Quelles sont les conséquences en termes de responsabilité civile et pénale du constructeur, par exemple en cas de décès du passager ? Le transfert automatique de telles données de santé vers un Cloud serait-il licite [199] ? 277

La collecte de données en grande quantité en vue d'une analyse et de prédictions et la création de profils de comportements de conduite soulèvent également des questions éthiques et juridiques [200]. Comment concilier en particulier ce modèle d'affaire avec le prin- 278

195. Strowel, *Robots et gouvernance des données.*
196. *Ibidem.*
197. Hilgendorf / Seidel, *Robotics, autonomics, and the law*, p. 191.
198. *Ibidem.*
199. *Ibidem.*
200. *Idem*, p. 192.

cipe de minimisation des données et de limitation des finalités [201] ? Quelles règles s'appliquent en cas de transfert données en-dehors de l'UE ? Le consentement de la personne concernée est-il requis et si oui, quelle est sa validité ?

279 Le contrôle des données dépend également de la technologie. Si la boîte noire est située dans le véhicule, il n'en est pas de même des données qui sont transférées dans un Cloud, potentiellement dans une autre juridiction que celle de l'enregistrement du véhicule.

280 Si les données sont analysées par des algorithmes prédictifs sur des plate-formes computationelles, alors des services personnalisés pourront être offerts aux passagers (par exemple : visite d'un restaurant conforme à son régime alimentaire, magasins en lien avec ses centres d'intérêts). La question se pose de savoir, quelle pourrait être la responsabilité du constructeur ou du loueur de véhicule, si les recommandations effectuées par le véhicule au conducteur contribuent à nuire à sa santé. Sa responsabilité pourrait-elle être engagée ? A titre d'exemple, est-il envisageable que le véhicule autonome recommande à un passager alcoolique une pause dans un pub ou dans un magasin vendant des produits alcoolisés [202] ?

281 Que se passera-t-il lorsque le véhicule autonome franchira la frontière entre deux pays et que les droits applicables ne seront pas similaires [203] ? L'ordinateur doit-il être programmé pour se conformer aux différents systèmes juridiques ? Faut-il régler la question du contrôle des données et de leur propriété par la loi ou régler cette question par contrat ? Dans cette dernière hypothèse, une évolution des contrats entre le constructeur et l'acheteur de données pourrait donner lieu à un accord de licences de données (personnelles et non personnelles) [204] ? Diana Marina Cooper partage cette vision relative à l'évolution contractuelle [205].

201. *Idem*, p. 192.
202. Hilgendorf / Seidel, *Robotics, autonomics, and the law*, p. 192 ; voir aussi le concept de « *machines morales* », Wallach Wendell / Allen Colin, *Moral Machines : Teaching Robots Right from Wrong*, 1e éd., New York 2008, p. 5.
203. Hilgendorf / Seidel, *Robotics, autonomics, and the law*, p. 191.
204. Strowel, *Robots et gouvernance des données*.
205. Cooper Diana Marina, *The application of a "sufficiently and selectively open license" to limit liability and ethical concerns associated with robotics*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016, pp. 163-185.

Sécurité des données

La recherche concernant l'accroissement de la robustesse des systèmes d'intelligence artificielle aux attaques adversariales constitue une priorité, en particulier pour les réseaux de neurones d'intelligence artificielle. La question de la sécurité des réseaux et de leur robustesse aux attaques adversariales [206] est également cruciale du fait de l'essor des objets connectés à Internet. 282

Depuis quelques années, l'Internet des objets s'est développé à un rythme sans précédent, se frayant un chemin dans tous les secteurs. Cependant, avec la demande croissante de ces dispositifs, l'un des principaux défis à relever pour les sécuriser est l'absence de normes de sécurité complètes. Les données collectées par les objets connectés à Internet étant transférées vers un Cloud, la question de la sécurité des Clouds est également fondamentale. La technologie de sécurité du cloud computing. Elle englobe un ensemble de politiques, de contrôles, de processus et de technologies qui fonctionnent ensemble pour protéger les systèmes, les données et l'infrastructure basés sur le cloud. 283

Une solution de cybersécurité émergente collecte, enregistre et stocke une grande quantité de données provenant des activités des points d'extrémité du réseau internet. Elle permet de surveiller en permanence les points d'accès, ce qui facilite les vérifications en cas d'incident [207]. 284

Un autre exemple d'applications entrainant des risques de sécurité est la possibilité de créer de fausses vidéos qui semblent très réelles. Ce processus est appelé « Deep Fake ». Des technologies d'Intelligence artificielle ont été conçues pour créer et détecter les fausses vidéos, par exemple au MIT [208]. Ces vidéos peuvent être utilisés pour influencer voire manipuler le public par le biais ou non d'un 285

206. Michalon Gilles / Auger Gerard, *Method for the transmission of data among mobile bodies or autonomous vehicles*, in : United States Patent 1994, p. « https://patents.google.com/patent/US5307509A/en » (26/10/2018) ; Petit Jonathan / Shladover Steven E., *Potential Cyberattacks on Automated Vehicles*, in : IEEE Transactions on Intelligent Transportation Systems 2015 16/2, pp. 1-11.
207. Darktrace, p. « https://www.darktrace.com/fr/ » (07/01/2020).
208. Day Suzanne, *MIT art installation aims to empower a more discerning public*, in : MIT News (http ://news.mit.edu/), Boston 2019, p. « http://news.mit.edu/2019/mit-apollo-deepfake-art-installation-aims-to-empower-more-discerning-public-1125 » (31/12/2019).

personnage influent (homme politique ou célébrité). Faceboook a annoncé l'interdiction des Deepfake sur le réseau social [209].

286 Dans l'éventualité d'une attaque, l'infraction ne sera punissable et l'auteur condamnable, qu'en présence d'une loi pénale.

Considérations éthiques

287 La question des considérations éthiques relatives aux valeurs encodées dans les algorithmes des véhicules autonomes est désormais reconnue comme essentielle [210]. L'IEEE a publié des lignes directrices sur ce thème en 2018 et 2019, afin d'encourager l'Ethics-by-Design.

288 L'Allemagne a également publié des recommandations éthiques dans ce domaine [211]. Elle fait figure de pionnière.

289 Ces recommandations indiquent que la préservation de la vie humaine doit toujours avoir la priorité sur la vie animale et sur les objets, et que toutes les vies humaines ont la même valeur [212]. La voiture autonome ne doit donc faire aucun choix, même parmi les passagers.

290 Aux États-Unis, le Massachusstet Institute of Technology a développé « une plate-forme compilant différentes perspectives humaines sur les décisions morales prises par les machines intelligentes comme les voitures autonomes ». Cette plate-forme présente les dilemnes moraux où une voiture sans conducteur doit choisir le moindre des deux maux, tuer deux passagers ou cinq piétons. L'utilisateur peut

209. McCabe David / Alba Davey, *Facebook Says It Will Ban 'Deepfakes'*, in : The New York Times (https ://www.nytimes.com/), New York 2020, p. « https://www.nytimes.com/2020/01/07/technology/facebook-says-it-will-ban-deepfakes.html » (07/01/2020).

210. Larousserie David, *Le dilemme macabre des voitures autonomes*, in : Le Monde (https ://www.lemonde.fr/), Paris 2016, p. « https://www.lemonde.fr/sciences/article/2016/06/23/tuer-un-pieton-ou-sacrifier-le-passager-le-dilemme-macabre-des-voitures-autonomes_4956924_1650684.html » (27/10/2018).

211. Ethik Kommission, *Automatisiertes und Vernetztes Fahren*, in : Bundesministerium für Verkehr und digitale Infrastruktur (https ://www.bmvi.de), Berlin 2017, p. « https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/084-dobrindt-bericht-der-ethik-kommission.pdf » (07/11/2017).

212. Seydtaghia Anouch, *Qui les voitures autonomes devront-elles tuer et protéger ?*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/economie/voitures-autonomes-devrontelles-tuer-proteger » (27/10/2018).

choisir quel résultat lui semble le plus acceptable et créer de nouveaux scénarios [213]». Le projet vise à « rassembler des avis sur des choix difficiles afin d'analyser les préférences des utilisateurs ».

Impact environnemental des véhicules autonomes

Certains s'interrogent sur l'impact environnemental de cette technologie [214], qui incite à investir dans de nouvelles infrastructures routières et dans de nouveaux véhicules. 291

Aspects philosophiques

L'émergence des véhicules autonomes pourrait amener à remettre en question le droit de conduire, si le nombre d'accidents de la route venait à chuter considérablement avec l'introduction des véhicules autonomes. 292

La question qui se poserait serait la suivante : « Est-ce moralement défendable de conduire soi-même son propre véhicule ? » 293

Accepter qu'un individu prenne des risques en conduisant lui-même son propre véhicule (et fasse prendre des risques aux autres usagers du domaine public) alors que ces risques seraient évitables en renonçant à la conduite, sera peut-être demain difficilement défendable. Cela reviendrait cependant à sacrifier la liberté de conduire sur l'autel de la sécurité. 294

Après avoir examiné le développement des voitures autonomes, nous allons analyser le cas des drones. 295

213. Noothigattu Ritesh, *A voting-based system for ethical decision making*, in : Thirty-Second AAAI Conference on Artificial Intelligence 2018, pp. 1587-1594.

214. Alavi Hamed S., *Is Driverless Car Another Weiserian Mistake ?*, in : Proceedings of the 2017 ACM Conference Companion Publication on Designing Interactive Systems, New York 2017, pp. 249-253.

Cas 2 : les drones

296 Les drones sont des objets connectés à internet en pleine expansion [215]. Ils sont notamment utilisés pour réaliser des livraisons [216], des opérations de surveillance [217], des travaux agricoles [218]. De nombreuses applications en matière civile sont possible [219]. Dans le domaine du transport, plusieurs projets de véhicules autonomes conçus à partir de drones, sont en cours de réalisation dans le but de désengorger les centres-villes [220]. La société Airbus propose par exemple un prototype de taxi volant [221]. La problématique des drones et du respect de la vie privée a fait l'objet d'une analyse approfondie de Robin Gavroy [222]. Les drones peuvent en effet géo-localiser et identifier tout individu du fait de son téléphone portable. Conçus pour

215. PFPDT, *Vidéosurveillance par des drones dans le domaine privé*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne s.a., p. « https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/technologien/videoueberwachung/videoueberwachung - mit - drohnen - durch - private / videoueberwachung - mit-drohnen-durch-private.html » (27/10/2018).
216. McFarland Matt, *Amazon's delivery drones may drop packages via parachute*, in : CNN Business (https ://money.cnn.com/), Washington D.C. 2017, p. « https : / / money . cnn . com / 2017 / 02 / 14 / technology / amazon - drone - patent/index.html » (27/10/2018).
217. Radio Télévision Suisse, *Les frontières suisses surveillées par des drones*, in : RTS (https ://www.rts.ch/), Genève 2006, p. « https : / / www . rts . ch / info / suisse / 980114 - les - frontieres - suisses - surveillees - par - des - drones . html » (27/10/2018).
218. Tribune de Genève, *Des drones au service des agriculteurs*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2016, p. « https : / / www . tdg . ch / suisse/drones-service-agriculteurs/story/17274017 » (27/10/2018).
219. Technidrones, *Les domaines d'application des drones civiles*, in : Technidrones (http ://techni-drone.com/), Dardilly s.a., p. « http://techni-drone.com/services/les-domaines-dapplications/ » (04/12/2018) ; Cf. aussi l'utilisation des drones par JD, concurrent d'Amazon en Chine : Liu Richard, *How e-commerce giant JD.com uses drones to deliver to far-out areas in China*, in : CNBC (https ://www.cnbc.com/), New Jersey 2017, p. « https://www.cnbc.com/video/2017/06/18/how-e-commerce-giant-jd-com-uses-drones-to-deliver-to-far-out-areas-in-china.html » (27/10/2018) ; Araki, *Multi-robot path planning for a swarm of robots that can both fly and drive*, pp. 5575-5582.
220. Zagni David, *Drones et voitures volantes : le ciel, nouvel horizon du transport individuel*, in : Les Echos (https ://www.lesechos.fr/), Paris 2017, p. « https : / / www . lesechos . fr / idees - debats / cercle / cercle - 167746 - le - ciel - nouvel - horizon - du - transport - individuel - 2073748 . php # Xtor = AD - 6000 » (27/10/2018).
221. Rozières Grégory, *Comment Airbus imagine nos transports du futur*, in : Le Huffington Post (https ://www.huffingtonpost.fr/), Paris 2016, p. « https://www.huffingtonpost.fr/2016/08/20/airbus-transport-futur_n_11605840.html » (27/10/2018).
222. Gavroy Robin, *Les drones et le droit au respect de la vie privée : Big Brother a-t-il le droit de voler en Belgique ?*, thèse, Louvain 2016, pp. 1-75.

un usage civil, les drones peuvent également être conçus à des fins militaires. Le risque de double usage (« dual-use ») est particulièrement élevé pour ces technologies.

D. Les robots intelligents

« Dans moins de 120 ans, tous les emplois humains seront effectués par des robots dotés d'une intelligence artificielle [223]. C'est en tout cas ce qu'affirment plusieurs experts des universités d'Oxford et de Yale [224]». « Ils prédisent que des robots travailleront dans le commerce d'ici 2031, qu'ils écriront des best-sellers et remplaceront les chirurgiens d'ici 2050 [225]». Joseph Weizenbaum met ainsi en garde la société : l'exercice de certains métiers par des machines tels que juge ou aide-soignant pourrait présenter un risque majeur pour la dignité humaine [226]. 297

Si une certaine prudence s'impose par rapport à ces prédictions nihilistes et absolues, les faits confirment effectivement une augmentation des ventes de robots de plus de 30 pour cent en 2018. Elles représentaient un marché de 16,2 milliards de dollars, en 2017 en hausse de 21 pour cent [227]. Le nombre annuel de demandes de brevets dans le domaine de la robotique a quant à lui triplé au cours des dix dernières années [228]. 298

Comment définir un robot ? 299

Le Parlement européen dans sa Résolution, 16/2/2017, souligna la nécessité d'une "définition acceptée par tous des notions de « ro- 300

223. Reisberg Anthony, *Intelligence artificielle : faut-il craindre un obscurantisme éclairé ?*, in : Le Club des Juristes (https ://www.leclub desjuristes.com), Paris 2019, p. « https://www.leclubdesjuristes.com/wp-content/uploads/2019/06/Intelligence-artificielle-faut-il-craindre-un-obscurantisme-%C3%A9clair%C3%A9-Anthony-Reisberg-1.pdf » (22/03/2020).
224. Frey Carl Benedikt / Osborne Michael A., *The future of employment : How susceptible are jobs to computerisation ?*, in : Technological forecasting and social change 2017/114, pp. 254-280.
225. *Idem*, p. 254 ; Reisberg, *Intelligence artificielle*, p. 1.
226. Reisberg, *Intelligence artificielle*, p. 1.
227. Garreau Marion, *2017, année record de ventes de robots industriels dans le monde*, in : L'Usine Nouvelle (https ://www.usinenouvelle. com/), Antony 2018, p. « https://www.usinenouvelle.com/article/2017-annee-record-de-ventes-de-robots-industriels-dans-le-monde.N757124 » (22/03/2020).
228. Parlement européen, *Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*, Introduction, point C.

bot » et d' « intelligence artificielle » (IA) qui soit flexible et n'entrave pas l'innovation".

301 De la même façon que pour les véhicules autonomes, le Parlement européen requiert une définition commune des différentes catégories de robots autonomes, qui tienne compte des caractéristiques suivantes :

- acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données avec l'environnement (interconnectivité) ;
- capacité d'échange et analyse de ces données ;
- capacité d'auto-apprentissage à travers l'expérience et les interactions (critère facultatif) ;
- existence d'une enveloppe physique, même réduite ;
- capacité d'adaptation de son comportement et de ses actes à son environnement ; et
- non vivant au sens biologique du terme [229].

302 Les robots intelligents sont donc des machines, capables d'agir sur leur environnement et de prendre des décisions. Ils sont capables de se mouvoir, de parler, de manipuler des objets ou d'exécuter des opérations selon un programme fixe, modifiable ou adaptable [230].

303 Du fait de la convergence entre la robotique et l'intelligence artificielle, le thème des robots intelligents sera également examiné au point 335.

304 Les robots collectent des données et les transfèrent vers des Clouds. La protection des données dans le cadre de l'utilisation des robots constitue un thème fondamental [231] qui soulève de nombreuses questions juridiques [232]. Cela s'explique par le fait que « les robots ont la capacité de percevoir, de traiter, et d'enregistrer le monde autour de d'eux. Les activités de surveillance constitue le second usage le plus

229. Delvaux, *Rise of the robots*, Principes généraux, p. 6.
230. Dictionnaire Larousse, p. « https://www.larousse.fr/encyclopedie/divers/robot/88768 » (29/12/2019).
231. Jarvis Ray, *Intelligent Robotics : Past, Present and Future*, in : International Journal of Computer Science and Applications 2008 5/3, pp. 23-35.
232. Calo Ryan, *Robots and Privacy*, in : Social Science Research Network (SSRN) Scholarly Paper (https ://papers.ssrn.com/), Rochester 2010, p. « https : // papers.ssrn.com/abstract=1599189 » (27/10/2018).

répandu des robots. Cela indique l'impact des robots sur la sphère privée [233]».

On distingue traditionnellement les robots : 305

— Supervisés : les données sont évaluées par des experts humains (tuteurs donnant les solutions correctes)

— Non-supervisés : l'algorithme d'apprentissage découvre par lui-même la structure des données

— À l'apprentissage « par renforcement » : apprentissage par l'expérience dans des situations variées

— À l'apprentissage « profond » (deep learning) : apprentissage automatique avec modélisation des données, notamment pour la reconnaissance d'objets et de personnes [234]. Ainsi pour tous les robots se pose la question du mode de décision, déterministe ou par apprentissage.

La norme ISO 8373 définit le robot intelligent comme « le robot 306
capable d'exécuter des tâches par détection de son environnement et/ou par interaction avec des sources extérieures et adaptation de son comportement [235]».

Il existe plusieurs catégories de robots : certains sont liés à la bio- 307
logie, d'autres sont dédiés à la construction de véhicules automobiles, certains sont dédiés à la gestion automatique des entrepôts, d'autres à la gestion des tâches ménagères, certains sont des drones militaires (drones), d'autres sont créés pour l'exploration de l'espace, pour la mobilité (véhicules autonomes), la chirurgie ou encore les loisirs (jouets pour enfants). Tous collectent des données,

233. "Its not hard to imagine why robots raise privacy concerns. Practically by definition, robots are equipped with the ability to sense, process and record the world around them. The fact that surveillance is the second most common use of robots indicate the magnitude of the impact of robotics on privacy", in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016, p. 176.
234. Strowel, *Robots et gouvernance des données.*
235. ISO, *Norme ISO 8373*, in : ISO (https ://www.iso.org/), Genève 2012, p. « https://www.iso.org/obp/ui//#iso:std:iso:8373:ed-2:v1:fr » (22/03/2020).

certaines à caractère personnel [236]».

308 Quel est l'État de l'art concernant les robots intelligents ?

309 Sur la base des informations transmises par Prof. Auke Jan Ijspeert [237]. Directeur du laboratoire de biorobotique de l'École polytechnique fédérale de Lausanne, lors de la conférence sur le droit et les robots qui s'est déroulée à l'Institut suisse de droit comparé le 28 septembre 2017, les biorobots intelligents développés en Suisse visent principalement à reproduire le comportement des animaux. Ainsi des robots volant, nageant, marchant ont été conçus sur le modèle du lézard, de la salamandre ou du chat [238]. Des robots humanoïdes sont également développés, mais uniquement dans un but de réadaptation fonctionnelle pour des patients atteints de myopathie ou de paraplégie [239] Il s'agit d'exosquelettes.

310 Il semble qu'aucune intégration de robots humanoïdes avec une intelligence artificielle ne soit effectuée en Suisse [240]. Aux États-Unis, en revanche, les fonds privées favoriseraient cette évolution [241]. La convergence de la biologie et de l'intelligence artificielle soulève de nombreuses questions éthiques et juridiques et nécessite d'encadrer la recherche dans ce domaine. Le principe de liberté de la recherche n'autorisant pas tout. Les chercheurs eux-mêmes sont demandeurs d'un cadre éthique [242]. A notre connaissance, seule la Corée du Sud a légiféré dans ce domaine [243]. L'OCDE vient cepen-

236. Institut Suisse de Droit Comparé, *Quand le droit rencontre les robots*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https://www.isdc.ch/fr/evenements/prochains-evenements/droit-robot » (21/03/2020).
237. Ijspeert Auke, *Biorobotics Laboratory (EPFL)*, Lausanne s.a., p. « https://biorob.epfl.ch/people/ijspeert » (29/09/2017).
238. *Ibidem.*
239. Ijspeert Auke, *De la biologie à la robotique et de la robotique à la biologie*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https://www.isdc.ch/fr/evenements/prochains-evenements/droit-robot » (21/03/2020).
240. Bouri Mohamed, *Exosquelettes d'assistance à la marche : une opportunité pour les activités quotidiennes*, in : Conférence de l'Institut Suisse de Droit Comparé, sur le droit et les robots du 28 septembre 2017 (https ://www.isdc.ch/), Lausanne 2017, p. « https : / / www . isdc . ch / fr / evenements/prochains-evenements/droit-robot » (21/03/2020).
241. *Ibidem.*
242. *Ibidem.*
243. Republic of Korea, *Intelligent Robots Development and Distribution Promotion Act*, in : Statutes of the Republic of Korea (http ://elaw.klri.re.kr/), Seoul 2008, p. « http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=39153&type=

dant de publier des principes directeurs pour l'IA et la Commission européenne aussi. Il y a donc une prise de conscience de la Communauté internationale de la nécessité de mettre en place un cadre éthique pour le développement de l'IA.

Des chercheurs de l'université de Oxford au Royaume-Uni ont lancé une initiative visant à créer un code éthique relatif à la robotique et à l'intelligence artificielle [244]. Cette initiative bénéficie du soutien du Future of Life Institute, qui encourage le développement responsable des robots intelligents. Prof. Luciano Floridi, Oxford University, propose quant à lui un « moral code » c'est-à-dire l'idée que le code intègre de valeurs morales. 311

À ce jour les robots humanoïdes les plus connus sont Nao, Pepper [245] et Bina 48 [246]. Nao et Pepper sont des robots humanoïdes développés par la société SoftBank Robotics qui sont capables de reconnaître certaines émotions. Ils détectent les émotions faciales, le champ lexical et le ton employé. Nao a été développé avec une vision éducative [247], ludique et avec l'objectif d'assister les personnes âgées, tandis que Pepper est utilisé à des fins commerciales. Bina 48 est une intelligence artificielle avec un visage. Elle représente l'intelligence artificielle la plus développée à ce jour pour Me. Bensoussan, avocat au barreau de Paris, spécialiste des robots, du fait de sa capacité langagière [248]. Selon Me. Bensoussan, les prochaines générations de robots auront à la fois capacité empathique, de raisonnement logique et la capacité d'interagir avec les humains. 312

Il apparaît légitime de réfléchir aux implications éthiques de ce type d'innovations et à leurs applications. Il semble raisonnable de se poser la question de savoir dans quelle mesure une interdiction de 313

lawname&key=robot » (29/09/2017).

244. Wooldridge Mike / Millican Peter / Boddington Paula, *Towards a Code of Ethics for Artificial Intelligence Research*, in : Oxford University (https ://www.cs.ox.ac.uk/), Oxford 2015, p. « https://www.cs.ox.ac.uk/efai/towards-a-code-of-ethics-for-artificial-intelligence/ » (29/09/2017).
245. Softbank Robotics, *Robots Nao et Pepper*, in : Softbank Robotics (https://www.softbankrobotics.com/), Paris s.a., p. « https://www.softbankrobotics.com/emea/index.php/fr/nao » (08/12/2019).
246. Bina Rothblatt, *Démonstration de l'intelligence artificielle Bina 48*, p. « https://www.youtube.com/watch?v=KYshJRYCArE » (28/09/2017). Il s'agit d'un cerveau artificiel et d'un visage.
247. Nao est utilisé par exemple dans des programmes avec des enfants autistes (Autism Solution for Kids).
248. Bensoussan Alain, *Etats généraux de l'intelligence artificielle du 22 septembre 2017*, Genève 2017.

l'intégration de l'intelligence artificielle dans des bio-robots serait justifiée.

314 Lors de la conférence internationale sur l'intelligence artificielle, qui s'est déroulée en août 2017, en Australie, une lettre a été signée par plus de 116 industriels et académiques spécialisés en robotique et en intelligence artificielle pour demander aux Nations-Unies l'interdiction des armes létales autonomes (les «killer robots») [249].

315 Les robots intelligents utilisés à des fins militaires acquièrent des informations, les traitent et interviennent sur les réseaux auxquels ils sont reliés, dans le cadre de cyber-guerre. Ils sont capables de capacités d'apprentissage autonomes du fait de technologies de machine-learning [250]. L'utilisation de tels robots, dans le cadre militaire soulève plusieurs questions en lien avec le respect du droit humanitaire, le risque de prolifération des armes, le risque de perte de contrôle des armes autonomes, voire celui de la dilution de responsabilité des États [251].

316 Pour Jean-Pierre Maulny, Directeur adjoint de l'Institut des relations internationales et stratégiques (IRIS), « c'est d'abord autour du degré d'autonomie des armes autonomes que doit s'articuler le débat. Il faut trouver un équilibre entre les risques et les avantages liés à la diminution – voire l'absence – de contrôle humain sur ces armes, comme on cherche à le faire pour les voitures sans conducteur par exemple. Dans le cas d'outils de guerre, il n'est pas envisageable d'accepter une autonomie totale, même en prétendant avoir confiance dans « nos » machines parce que nous les avons

249. Future of Life Institute, *Autonomous Weapons : An Open Letter from AI and Robotics Researchers*, in : Future of Life Institute (https ://futureoflife.org/), Allston 2015, p. « https : / / futureoflife . org / open - letter - autonomous-weapons/ » (28/09/2017).

250. Kerr Ian / Szilagyi Katie, *Asleep at the switch ? How killer robots become a force multiplier of military necessity*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016, p. 333 ss.

251. United Nations, *Disarmament in Geneva*, in : United Nations (https ://www.un.org/), Geneva s.a., p. « https://www.un.org/disarmament/geneva / ccw / background - on - lethal - autonomous - weapons - systems/ » (28/09/2017).

programmées [252]».

Les technologies évoluent très vite dans ce domaine. Les États-Unis investissent dans des interfaces cerveau-machines afin que des soldats puissent interagir et contrôler des systèmes uniquement avec leur cerveau [253]. 317

Les questions éthiques et juridiques autour des robots commencent à être abordées en doctrine [254] et Ian Kerr [255]. 318

En février 2017, le Parlement européen a voté une résolution, sur le statut juridique des robots, se fondant sur le rapport préparé par Mary Delvaux [256]. Il a recommandé à la Commission européenne de reconnaître aux robots autonomes le statut de personne électronique, ayant des droits spécifiques et des obligations. 319

Cette personnalité électronique s'appliquerait aux robots capables de prendre des décisions autonomes ou qui intéragissent avec des tiers [257]. En matière de responsabilité, la future législation européenne sur les robots prévoit un régime de responsabilité stricte [258], nécessitant uniquement la preuve de l'occurrence du dommage et 320

252. IRIS, *Jean-Pierre Maulny*, in : IRIS (http ://www.iris-france.org/), Paris s.a., p. « http://www.iris-france.org/chercheurs/jean-pierre-maulny/ » (29/09/2017).
253. DAPRA, *Six Paths to the Nonsurgical Future of Brain-Machine Interfaces*, in : Defense Advanced Research Projects Agency (https :// www.darpa.mil/), Arlington County 2019, p. « https://www.darpa.mil/news-events/2019-05-20 » (09/06/2019).
254. Veruggio Gianmarco / Operto Fiorella / Bekey George, *Roboethics : Social and Ethical Implications*, in : Siciliano Bruno / Khatib Oussama (édit.), *Springer Handbook of Robotics*, Cham 2016, pp. 2135-2160.
255. Calo / Froomkin / Kerr, *Robot Law*, p. 10.
256. Affaires juridiques et parlementaires, *Règles européennes de droit civil en robotique*, in : Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2016, p. « http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_FR.pdf » (20/06/2017).
257. Parlement européen, *Robots : les députés de la commission des affaires juridiques demandent des règles européennes*, in : Parlement européen Actualité (http ://www.europarl.europa.eu/), Bruxelles 2017, p. « https://www.europarl.europa.eu/news/fr/press-room/20170110IPR57613/robots-vers-des-regles-europeennes » (22/03/2020).
258. Parlement européen, *Le Parlement européen soulève des questions éthiques sur les robots et l'intelligence artificielle*, in : Parlement européen - Multimedia Centre (https ://multimedia.europarl.europa.eu/), Bruxelles 2017, p. « https://multimedia.europarl.europa.eu/fr/european-parliament-raises-ethical-questions-on-robots-and-artificial-intelligence_NB01-PUB-170111INT_ev » (27/10/2018).

l'établissement d'un lien de causalité entre le comportement dommageable du robot et le dommage subi par la tierce partie victime du dommage.

321 Un système d'assurance obligatoire est proposé pour contraindre les producteurs ou les propriétaires de robots à souscrire une police assurance, indemnisant les personnes concernées pour les dommages causés par les robots. Un fond de compensation viendrait en outre garantir la compensation d'un dommage causé par les robots qui ne dispose pas d'une couverture d'assurance.

322 Les robots capables de causer des blessures corporelles sérieuses sont conçus sur la base des principes développés par Isaac Asimov [259].

323 Le Parlement européen a proposé l'élaboration d'un code de conduite relatif aux robots dédiés aux chercheurs et aux designers pour s'assurer qu'ils fonctionnent conformément aux standards légaux et éthiques et que les robots respectent la dignité humaine. Il est en effet prévisible que les sociétés délégueront de façon croissante les procédures de décisions à des robots (de type Watson) [260]. Les auteurs considèrent que les robots intelligents assumeront probablement de façon croissante des fonctions de contrôle, en étant reconnus comme des « experts » [261]. La question de fond concerne l'évaluation du risque associé à la délégation de la prise de décision et à la renonciation du contrôle humain eu égard aux avantages que les robots experts pourront offrir à l'avenir [262]. Comment maintenir la confiance des acteurs humains dans le fonctionnement de ces

259. Asimov Isaac / Hodgson Jeffrey, *Robot visions*, 3e éd., London 1990, pp. 1-496 ; Asimov Isaac, *The Naked Sun*, London 2018, "*1)* A robot may not injure a human being, or, through inaction, allow a human being to come to harm, *2)* A robot must obey the orders given it by human beings except where such a orders would conflict with the First Law, and *3)* A robot must protect its own existence as long as such protection does not conflict with the First or Second Law".

260. "It is not difficult to imagine a smooth and simple logic that would lead a society like ours to delegate increasingly significant decision-making to future Watson-like robots", Millar Jason / Kerr Ian, *Delegation, relinquishment and responsibility : The prospect of expert robots*, in : Calo Ryan / Froomkin A. Michael / Kerr Ian (édit.), *Robot Law*, 1e éd., Cheltenham 2016, p. 124.

261. *Ibidem.*

262. *Idem*, p. 126.

robots lorsque le contrôle humain a été supprimé ?

Le Parlement européen prévoit en outre un système d'enregistrement des robots intelligents. Si ce projet est adopté, l'industrie sera tenue de déclarer le nombre de robots intelligents utilisés, le montant des contributions sociales épargnées du fait de l'utilisation de telles machines en lieu et place des êtres humains, et le montant des revenus générés du fait de l'utilisation des robots et de l'intelligence artificielle [263]. 324

Le Comité juridique européen a également demandé à la Commission de considérer la création d'une agence européenne dédiée à la robotique et à l'intelligence artificielle, pour mettre à disposition des autorités publiques une expertise technique, éthique et réglementaire. 325

Si la résolution fut acceptée par 393 votes contre 123 (dont 85 abstentions), la Commission européenne ne sera cependant pas tenue de suivre les recommandations du Parlement. Le cas échéant, elle devra, en revanche, justifier les raisons de son refus. 326

La question de la taxation des robots a été écartée du projet. La nouvelle forme de capacité contributive des robots pourrait cependant justifier la taxation des robots [264]. Il s'agit d'une décision politique, qui pourrait se justifier si les robots remplaçaient massivement les collaborateurs humains. A contrario, cette décision de taxation pourrait freiner les investissements et ralentir la croissance économique, donc la création de richesses et la capacité distributive des États. 327

Une réflexion autour de l'usage des robots, de la fiscalité [265] et d'une domiciliation fiscalement avantageuse est en cours en Suisse. La Suisse pourrait trouver un nouveau marché dans l'offre de domiciliation de robots. 328

La collecte massive de données à caractère personnel, voir de données sensibles (données médicales ou données relatives à des mineurs) [266] par des robots, nécessite de sensibiliser les utilisateurs de 329

263. *Idem*, p. 126.
264. Oberson Xavier, *Taxer les robots ? L'émergence d'une capacité contributive électronique*, in : AJP/PJA 2017, pp. 232-239.
265. *Ibidem.*
266. Paro, *PARO Therapeutic Robot*, in : Paro (www.parorobots.com), Tokyo s.a.,

ces services au fait que la protection des données est un droit fondamental au sein de l'Union-Européenne ainsi qu'en Suisse.

330 Cette étude étant dédiée à la protection des données, la question de l'octroi ou non d'une personnalité juridique spécifique aux robots ne sera pas abordée. Cependant, il importe de mentionner que cette doctrine est actuellement très vive. L'Arabie saoudite, a accordé au robot Sophia, conçu par l'industriel Hanson Robotics, la nationalité saoudienne fin octobre 2017. L'Estonie veut accorder un statut légal à l'intelligence artificielle [267]. En France, l'avocat Me Bensoussan propose la création de nouveaux droits, comme celui du droit au silence des puces et du droit á l'effacement des traces pour l'internet des objets [268]. Il est notable de relever que la responsabilité en cas de dommage causé par un robot incombe en premier lieu, à l'utilisateur du robot, « sauf preuve contraire [269] ». Selon cette charte, le cabinet Bensoussan place la charge de la preuve sur l'utilisateur du robot. Or, cette solution juridique n'est pas favorable à la protection des personnes concernées, qui seront a priori rarement dans une position de se défendre de manière effective face aux propriétaires des robots. Lors du sommet sur l'intelligence artificielle à Genève, qui s'est tenu en septembre 2017 à Genève, Me. Bensoussan expliqua que les robots vont progressivement être dotés d'une intelligence supérieure à l'intelligence humaine, d'empathie et de capacités imaginatives, ce qui est confirmé par la littérature [270]. « La mixité entre les hommes et les robots logiciels et

p. « www.parorobots.com »(15/12/2019) ; Toyota, *Partner Robot*, in : Toyota (http ://www.toyota-global.com/), Toyota City s.a., p. « http://www.toyota-global.com/innovation/partner_robot/ » (02/05/2017).

267. Garessus Emmanuel, *Les robots obtiendront leur propre statut juridique*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https : / / www. letemps . ch / economie / robots - obtiendront - propre - statut - juridique » (27/10/2018).

268. Bensoussan Alain / Barbry Éric, *La vie privée des objets*, in : Annales des Mines - Réalités industrielles 2013 2013/2, p. 65.

269. Bensoussan Alain, *Charte des droits et obligations des robots*, in : Lexing - Alain Bensoussan Avocats (https ://www.alain-bensouss an.com/), Paris 2015, p. « https://www.alain-bensoussan.com/wp-content/uploads/2014/10/Charte-droits-des-robots-Version-5.pdf » (29/09/2017), art. 6.

270. Pascanu Razvan, *Agents that imagine and plan*, in : Deepmind (https ://deepmind.com/), London 2017, p. « https://deepmind.com/blog/agents-imagine-and-plan/ » (28/09/2017) ; Bostrom Nick, *Superintelligence : paths, dangers, strategies*, Oxford 2017, p. 1 ; Heylighen Francis, *Return to Eden ? Promises and Perils on the Road to a Global Superintelligence*, in : Goertzel Ben / Goertzel Ted (édit.), *The End of the Beginning : Life, Society and Economy on the Brink of the Singularity*, 1e éd., Los Angeles 2015, pp. 243-305.

autonomes » constituera selon lui, l'enjeu du XXIème siècle. L'interaction homme-machine voire « la symbiose » homme-machine du fait des implants cutanées nous apparaissent des éléments importants, qui requièrent dans un premier temps un questionnement éthique et philosophique plus qu'un cadre juridique. Les technologies transcraniennes et les implants neuronaux apparaissent particulièrement problématiques. Ils visent l'amélioration des performances cognitives, la modification des neurones et rendent pertinente la réflexion autour d'un droit fondamental á l'intégrité neuronale [271].

Me. Bensoussan est favorable à la reconnaissance d'une personnalité juridique aux robots. Cette approche ne fait pas l'humanité. Elle est particulièrement contestée par le milieu scientifique, par exemple par le Prof. Joshua Bengio, qui fut récipiendaire du Prix Turing en 2018) [272]. 331

Le Professeur Bertil Cottier, notamment, se réfère aux travaux de Serge Tisseron pour rappeler que les robots resteront toujours des machines [273]. Pour ce spécialiste de l'étude des relations entre les hommes et les robots, les données personnelles sont centrales dans la relation Hommes-Robots [274], Il insiste sur le caractère artificiel de l'empathie des robots, qui trouve son fondement dans les données à disposition de l'intelligence artificielle du robot [275]. Cette doctrine est également partagée par Neil. M. Richards et William 332

271. Platypusneuro, *Are you ready to become human 2.0 ?*, in : Platypusneuro (https ://www.platypusneuro.com/), San Diego s.a., p. « https : / / www . platypusneuro.com/about » (14/12/2019) ; Emondi Al, *Next-Generation Nonsurgical Neurotechnology*, in : Defense Advanced Research Projects Agency (https ://www.darpa.mil/), Arlington County s.a., p. « https : / / www . darpa . mil / program / next - generation - nonsurgical - neurotechnology » (13/01/2020) ; Orwell George, *Nineteen eighty-four*, Boston 1987, p. 335.
272. Association for Computing Machinery, *Fathers of the Deep Learning Revolution Receive ACM A.M. Turing Award*, in : ACM (https : //acm.org/), New York 2018, p. « https://awards.acm.org/about/2018-turing » (14/12/2019).
273. Vincent Catherine, *Serge Tisseron : « Les robots vont modifier la psychologie humaine »*, in : Le Monde (https ://www.lemonde.fr/), Paris 2018, p. « https: //www.lemonde.fr/idees/article/2018/07/12/serge-tisseron-les-robots-vont-modifier-la-psychologie-humaine_5330469_3232.html » (15/12/2019).
274. Tisseron Serge, *« Parce que les objets sont au coeur de nos économies affectives »*, in : IERHR (http ://ierhr.com/), Paris s.a., p.« http://ierhr.com/ » (29/09/2017).
275. Tisseron, *Alice cares : Vers l'empathie artificielle*, in : IERHR (http ://ierhr.com/), Paris 2016, p. « http://ierhr.com/alice-cares-vers-lempathie-artificielle » (29/09/2017).

D. Smart [276].

333 Le débat sur la personnalité robot, ses droits, ses obligations et la protection des données collectées n'en est qu'à ses débuts. La reconnaissance, le 15 mars 2017, de la personnalité juridique au Fleuve Wanganui, en Nouvelle-Zélande par le Parlement néo-zélandais, et du statut de personne morale à deux fleuves indiens (le Gange et la rivière Yamuna) par une cour de justice en Inde viendra encore compliquer le débat [277].

334 A ce jour, il apparaît prématuré de reconnaître la personnalité juridique aux robots, compte tenu de l'absence de caractère «naturel» ou biologiquement sensible des robots. Cette réflexion mériterait des développements, qui dépassent le cadre de cette étude.

335 Le Dr. Serge Tisseron, psychiatre et directeur de l'Institut international des relations hommes-robots considère avec raison qu'il s'agit uniquement d'un problème d'interaction homme-machine entre trois composantes : les données, l'IA et le terminal qu'est le robot. Le robot interagit avec l'IA qui l'habite et avec toutes les données qui permettent à l'IA de fonctionner. L'être humain interagit avec un objet qui a son autonomie propre. Selon Serge Tisseron, les robots ne s'intéressent à l'homme et n'ont besoin des hommes que pour renforcer leurs apprentissages (pour lesquels ils sont récompensés) et pour gagner en autonomie. Serge Tisseront prévoit le développement d'une empathie artificielle entre les robots et les hommes qu'il qualifie « d'illusion de l'empathie [278]».

E. Les risques des objets connectés

336 L'utilisation mal contrôlée ou non sécurisée d'un objet connecté peut nuire à la vie privée des individus [279] et confronter les utilisateurs à diverses problématiques, comme la surveillance de leur vie

276. "Robots, even sophisticated ones are just machines. They will be no more than machines for the foreseeable future and we should design our legislation accordingly", Richards / Smart, *How should the law think about robots ?*, p. 20.
277. Ropert Pierre, *En Inde et en Nouvelle-Zélande, le fleuve reconnu comme un être vivant*, in : France Culture (https ://www.france culture.fr/), Paris 2017, p. « https://www.franceculture.fr/environnement/en-inde-et-en-nouvelle-zelande-le-fleuve-reconnu-comme-un-etre-vivant » (29/09/2017).
278. Présentation de Serge Tisseront, Geneva Summit on AI, 22 Septembre 2017.
279. Bensoussan / Barbry, *La vie privée des objets*, pp. 61-65.

privée [280], le détournement des données à des fins de ciblage publicitaire, à des fins d'escroquerie, d'usurpation d'identité, de harcèlement. Les objets connectés prennent en outre la forme d'objets d'apparence anodine (poupées, robots, babyphones...), ce qui n'incite pas à la vigilance. Même éteint, l'objet connecté peut capter des données personnelles. A contrario, une fois éteint, la personne concernée peut ne plus avoir la possibilité d'accéder aux données pour les supprimer [281].

Les objets et applications connectés impliquent le traitement de 337
données qui se rapportent à des personnes physiques identifiées ou identifiables et qui répondent donc à la qualification de « données personnelles » au sens du Règlement.

Malgré l'existence d'un droit à l'autodétermination informationnel, 338
consacré à l'article 13, al. de la Constitution suisse, les personnes dont les données sont collectées ignorent souvent en pratique que des données ont été collectées, analysées, voire transférées à titre gratuit ou à titre onéreux à des tiers, pour des finalités inconnues. Lors du Sommet Geneva AI, qui a eu lieu en septembre 2017 à Genève, Me. Bensoussan avait soulevé la problématique de l'absence de droit de propriété sur la donnée.

La reconnaissance d'un droit de propriété des données présenterait 339
un intérêt en matière pénale. En effet, le vol, c'est-à-dire la soustraction de la chose d'autrui nécessite que la chose soit la propriété d'une personne. Or, la donnée échappe à la propriété à ce jour, donc au vol d'un point de vue juridique.

Du fait de l'existence du droit à l'autodétermination informa- 340
tionnelle [282] en Suisse, la pertinence d'un droit de propriété apparaît cependant discutable. Ce droit permet n effet de « déterminer qui utilise des informations nous concernant, qui les propage et à quelles fins [283] ».

En Suisse, l'université de Zürich a soulevé la question de l'oppor- 341
tunité de reconnaître un droit de propriété applicable aux données à caractère personnel, lors d'une conférence dédiée à la protection

280. Orwell, *Nineteen eighty-four*, p. 273.
281. CNIL, *Objects Connectés*, p. « https://www.cnil.fr/fr/thematique/internet-technologies/objets-connectes » (27/10/2018).
282. art. 13, al. 2 de la Constitution suisse.
283. Astrid Epiney, Interview à la RTS, 2013.

des données le 29 mars 2017 [284].

342 De façon générale, il s'agit d'offrir aux utilisateurs la garantie que les données qui les concernent ne seront pas traitées sans fondement juridique (consentement, contrat, loi, intérêt légitime...).

343 L'utilisation des objets connectés nécessite une vigilance toute particulière des utilisateurs et une sensibilisation du public par les autorités nationales compétentes et le système éducatif.

344 Le Forum économique mondial a inscrit le thème des objets connectés en lien avec le développement de l'intelligence artificielle à l'agenda de la conférence du mois de décembre 2016. Il ressort des discussions que les utilisateurs privilégient l'accès à des services personnalisés offerts par les objets connectés ou les applications qu'ils installent, à la protection des données. L'aversion au risque varie cependant considérablement d'un pays à l'autre en fonction de la confiance accordée à leur État. Par exemple, les États du Nord de l'Europe sont beaucoup plus enclins au partage de leurs données que les Etats du Sud. Les aspects pratiques liés à l'utilisation et à la convivialité des nouveaux outils l'emportent sur les risques auxquels les consommateurs s'exposent lors de la communication de leurs données personnelles [285].

IV. La technologie Blockchain

345 Lors du Forum FinTech qui a eu lieu à Paris en janvier 2017, est apparue l'idée qu'un objet connecté pouvait être lié à un contrat intelligent programmé dans une Blockchain.

346 Qu'est-ce que la Blockchain ?

347 La première Blockchain est apparue en 2008 avec la monnaie numérique bitcoin [286], développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto. Elle en est l'architecture sous-

284. ITSL, *Data Ownership - Conférence du 29 mars 2017*, in : University of Zürich (http://www.dsi.uzh.ch/), Zürich 2017, p. « http://www.dsi.uzh.ch/dam/jcr:3b4398c3-e208-41f7-bb54-4b1c72c3b3ac/Flyer-Dateneigentum_EN.pdf » (23/10/2017).

285. Moore Andrew / Russell Stuart, *The State of Artificial Intelligence*, in : WEF (https ://www.weforum.org/), Davos 2016, p. « https://www.youtube.com/watch?v=VBceREwF7SA » (10/03/2017).

286. Narayanan Arvind, *Bitcoin and cryptocurrency technologies : a comprehensive introduction*, 1e éd., Princeton 2016, p. 176.

jacente [287].

Si Blockchain et bitcoin ont été construits ensemble, aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc.) envisagent l'utilisation de la technologie Blockchain pour d'autres utilisations que la monnaie numérique, bien que des questions de sécurité demeurent non résolues [288]. 348

La Blockchain est une technologie de stockage et de transmission d'informations, transparente et fonctionnant sans organe central de contrôle [289]. Par extension, une Blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne [290]. 349

Une Blockchain publique peut être assimilée à un grand livre comptable public, anonyme et infalsifiable. Pour le mathématicien Jean-Paul Delahaye, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible [291] ». 350

La Blockchain supprime les intermédiaires [292]. Elle dispose d'une forme d'organisation décentralisée [293] et permet de nouer des relations d'affaires [294]. 351

Constituent des « applications Blockchain » les applications organisées de manière décentralisées et distribuées, créées sur la base d'un registre virtuel, nommé « Distributed Ledger ». Les données 352

287. Blockchain France, *Qu'est-ce que la blockchain ?*, in : Blockchain France (https ://blockchainfrance.net/), Paris 2015, p. « https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/ » (27/10/2018).
288. Delahaye Jean-Paul, *Une épée de Damoclès sur le Bitcoin*, in : Complexités (http ://www.scilogs.fr/), s.l. 2016, p. « http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/ » (27/10/2018).
289. Tapscott Don / Tapscott Alex, *Blockchain Revolution : How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 1e éd., London 2016, p. 6.
290. *Ibidem.*
291. Delahaye Jean-Paul, *Travaux de recherche*, in : LIFL (http ://www.lifl.fr/), Lille s.a., p.« http://www.lifl.fr/~jdelahay/ » (01/06/2017).
292. De Rosnay, *Je cherche à comprendre*, p. 85.
293. Tapscott / Tapscott, *Blockchain Revolution*, p. 33.
294. *Idem*, p. 293.

peuvent y être stockées de manière publique, décentralisée et distribuée immuablement.

353 La Blockchain permet l'enregistrement d'un droit sur la Blockchain et la garantie d'une traçabilité de l'historique des transactions. Toute transaction est signée par une clef-signature, dite private key, laquelle constitue un identifiant unique pour l'individu l'utilisant.

354 Il est possible d'opérer des transactions de manière décentralisée, rapide et à moindre coût sur la base de la Blockchain, raison pour laquelle cette technologie est intéressante dans le domaine financier. Actuellement, la technologie fondée sur la Blockchain est la plus souvent utilisée pour la création et la mise en circulation de monnaies cryptographiques (bitcoin). Il est également possible, en plus des monnaies cryptographiques, de représenter d'autres droits dans une Blockchain, les tokens.

355 Le tableau ci-dessous (figure 2.6) présente le fonctionnement de la technologie Blockchain.

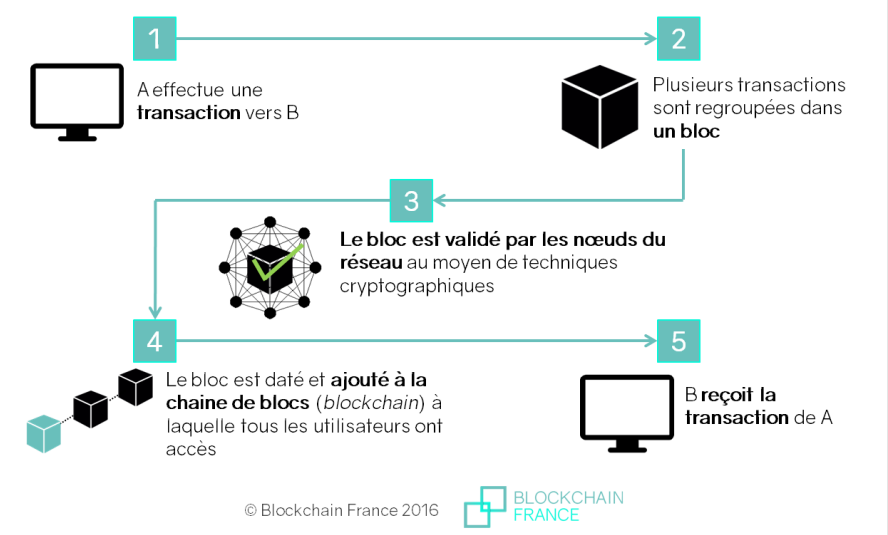

Figure 2.6 – Description du fonctionnement de la technologie Blockchain. Source : Blockchain France (2016).

356 Thomas Puschmann, directeur du laboratoire Fintech Innovation de l'Université de Zurich, considère que la convergence entre la Blockchain et d'autres technologies comme le cloud ou les objets

connectés va modifier en profondeur le monde économique [295].

La Blockchain permet d'exécuter des contrats intelligents [296], comme par exemple les contrats de leasing. Ceux-ci sont enregistrés sur la Blockchain sur laquelle les paiements sont effectués et reliés au véhicule. D'autres applications sont envisageables comme la passation de contrats dans le domaine du droit civil (mariage) [297] et du droit public (contrat social) [298]. Des documents tels que des passeports peuvent également être créés par ce biais [299]. Enfin, les actes notariés pourraient également à l'avenir être passés par le biais de la Blockchain. 357

Cette nouvelle technologie constitue une forme de registre des transactions numériques, ineffaçable, infalsifiable qui permet de réduire les coûts tout en améliorant la qualité et la vitesse des services. Le dessin ci-dessous (figure 2.7) présente un exemple de transaction financière via la technologie Blockchain. 358

Dans le domaine médical, la Blockchain permet de tracer le cycle de vie d'un vaccin de son lieu de production jusqu'à sa délivrance au patient. En matière minière, le processus d'extraction des mi- 359

295. Puschmann Thomas, *Swiss FinTech Innovation Lab*, in : University of Zürich (http ://www.uzh.ch/), Zürich 2019, p. « http://www.fintech.uzh.ch/en.html » (15/12/2019).

296. Buterin Vitalik, *A Next Generation Smart Contract & Decentralized Application Platform*, in : Etherium White Paper (https ://cryptorating.eu/), s.l. 2014, p. « https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf » (08/12/2019) ; Gasteiger Daniel, *Co-Founder de la société Nexussquared*, p. « http://www.nexussquared.co/about-us/team/ » (01/06/2017).

297. Ruben Alexander, *The First Blockchain Wedding*, in : Bitcoin Magazine (https ://bitcoinmagazine.com/) Nashville 2014, p. « https://bitcoinmagazine.com/articles/first-blockchain-wedding-1411842604/ » (30/07/2017) ; Von Hannes Bauer, *Risikofeststellung Dateneigentum*, in : Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, 3e éd., Leipzig 2019, p. 26.

298. Bitnation, *Governance 2.0, Sans frontière, décentralisée, volontaire*, p. « https://bitnation.co/main/?la=fr » et « http://www.nasdaq.com/article/bitnation-launches-worlds-first-blockchain-based-virtual-nation-constitution-cm584980 » (30/07/2017). Voir aussi le concept de *Democracy by Design*, « http://www.publicdeliberation.net/cgi/viewcontent.cgi?article=1329&context=jp » (01/04/2017) et l'article de Helbing Dirk sur ce sujet : Helbing Dirk / Pournaras Evangelos, *Society : Build digital democracy*, in : Nature News 2015 527/7576, pp. 33-34.

299. Hickey Matt, *Open Source Project Could Replace Traditional Passports With Bitcoin Tech*, in : Forbes (https ://www.forbes.com/), New Jersey 2014, p. « https://www.forbes.com/sites/matthickey/2014/10/31/open-source-project-could-replace-traditional-passports-with-bitcoin-tech/ » (27/10/2018).

nerais (ex : le diamant) peut également être rendu transparent, du stade de l'extraction minière jusqu'à la vente du produit fini auprès d'un joaillier. En matière fiscale, la Chine a décidé de recourir à la technologie Blockchain pour prélever les impôts et envoyer des factures [300].

360 Cependant, la Blockchain soulève plusieurs questions juridiques. Comment définir la notion de token ou de cryptomonnaie ? Quels droits de propriété sont liés aux données [301] et au token [302] ? Un smart contrat est-il assimilable à un contrat ? Quel est le régime de responsabilité en cas d'accident et de quels recours disposent les personnes concernées ? Comment concilier Blockchain et le droit

300. Ledger Insights, *China's Shenzhen district uses blockchain for $1 billion of tax invoices*, in : Ledger Insights (https ://www.ledger insights.com/), Limassol 2019, p. « https://www.ledgerinsights.com/china-shenzhen-blockchain-tax-invoices/ » (15/12/2019).

301. Mayer Anna, *Diskussionsansätze in der Debatte um die Regulierung von Dateneigentum : Ein Vergleich zwischen Deutschland und Japan*, in : Stiftung Datenschutz (édit.), *Dateneigentum und Datenhandel*, 3e éd., Leipzig 2019, p. 222.

302. Müller Luka, *BCP Framework for Assessment of Crypto Tokens*, in : MME Legal (https ://www.mme.ch/), Zürich 2017, p. « https://www.mme.ch/en/magazine/magazine-detail/url_magazine/conceptual_framework_for_blockchain_crypto_property_bcp/ » (10/10/2017).

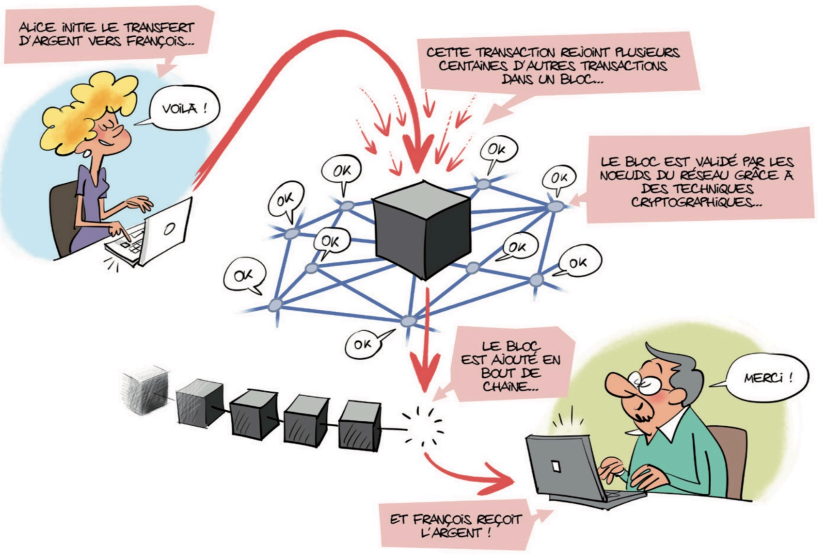

Figure 2.7 – Exemple d'une transaction entre deux personnes. Source : Livre blanc sur la Blockchain, Juin 2017.

à l'oubli ? La Blockchain peut-elle être assimilée à un registre de fichiers ? Y-a-t-il un besoin de régulation de la Blockchain et si oui, quelle place donner aux normes ISO [303] ?

« Le nombre d'offres initiales d'achat de tokens (ICO, Initial Coin Offering) a augmenté de façon notable, réalisées ou proposées en Suisse [304]». 361

Plus de USD 1,6 milliards ont été levés ces six derniers mois, dans le cadre des Initial Coins Offering, qui correspondent à des appels publics de fonds à des fins entrepreunariales sous une forme numérisée, utilisant uniquement la technologie Blockchain [305]. 362

A l'initiative de l'Australie, l'Organisme International de Standardisation ISO pourrait développer des standards spécifiques pour la Blockchain [306]. Le G20 est également appelé à réfléchir au mode de gouvernance de la Blockchain [307]. 363

Le contrôle de la Blockchain et son impact en terme de protection des données et de sécurité doivent être méticuleusement examinés [308]. L'attaque 51 a démontré l'existence de défauts de conception et soulevé la problématique du contrôle de la Blockchain [309]. 364

303. Polrot Simon, *Panorama des enjeux juridiques de la Blockchain*, in : Blockchain Partner (https ://blockchainpartner.fr/), Paris 2017, p. « http : / / blockchainpartner . fr / wp - content / uploads / 2017 / 05 / Enjeux - juridiques - de-la-blockchain-Blockchain-Partner.pdf?utm_source=Sociallymap&utm_medium=Sociallymap&utm_campaign=Sociallymap » (30/07/2017).
304. FINMA, *FINMA is investigating ICO procedures*, in : FINMA (https ://www.finma.ch/), Bern 2017, p. « https : / / www . finma . ch / en / news / 2017 / 09/20170929-mm-ico/ » (10/10/2017).
305. Müller, *BCP Framework for Assessment of Crypto Tokens*.
306. ISO, *ISO/TC 307 - Blockchain and distributed ledger technologies*, in : ISO (https ://www.iso.org/), Sydney 2016, p. « https://www.iso.org/committee/6266604.html » (27/07/2017).
307. Maupin Julie, *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All*, in : G20 Insights (https ://www.g20 - insights.org/), Berlin 2018, p. « https://www.g20-insights.org/policy_briefs/g20-countries-engage-blockchain-technologies-build-inclusive-transparent-accountable-digital-economy/ » (27/10/2018).
308. Zyskind Guy / Nathan Oz / Pentland Alex 'Sandy', *Decentralizing Privacy : Using Blockchain to Protect Personal Data*, in : IEEE Security and Privacy Workshops, San Jose 2015, pp. 180-184.
309. Jacob Marc, *Panorama de la cybercriminalité du CLUSIF : l'industrie du malware ne connait pas la crise !*, in : Global Security Mag (https://www.globalsecuritymag.fr/), Paris 2017, p. « https://www.globalsecuritymag.fr/Panorama-de-la-cybercriminalite-du,20170111,68200.html » (09/06/2017) ; Terruzi

A ce jour, 52 % de la puissance de calcul est détenue par quatre pools chinois. S'ils s'allient, ils détiendront un contrôle absolu de la technologie Blockchain et contrôleront les données échangées sur celle-ci (montants financiers inclus) [310]. C'est pourquoi de nombreuses chaines Blockchains privées voient le jour.

V. Le Cloud Computing

365 Le marché du Cloud Computing (informatique en nuage) est estimé à 131 milliard de dollars en 2017 contre 111 milliard en 2012 (en croissance de 18.5%) [311].

366 Pourquoi ? Les services de Cloud computing offrent des solutions de stockage des données sur des serveurs distants et accessibles par internet. Les serveurs de stockage sont appelés des « Datacenters » ou « centre de données [312]». Des algorithmes enregistrent exactement où sont rangées les données sur les serveurs et les restituent sur demande. Chaque centre de données nécessite un vaste espace et consomme beaucoup d'électricité [313]. Ils consomment également beaucoup d'eau pour refroidir les serveurs. Le coût environnemental lié á la gestion des centres de données représente un défi pour les sociétés du fait du réchauffement climatique. Pour rentabiliser leurs infrastructures, les opérateurs louent leurs capacités de stockage à des entreprises détenant de nombreuses données [314].

367 Le Cloud Computing évolue vers des plateformes duales intégrant le stockage des données et leur analyse sur la base d'algorithmes d'intelligence artificielle : les plateformes computationnelles.

368 La sécurité des services de Cloud Computing est au coeur d'enjeux

David / Chiron Nathan, *Combien ça coûterait une attaque 51% ?*, in : Blockchain Café (http ://blogchaincafe.com/), Paris 2016, p. « http://blogchaincafe.com/combien-ca-couterait-une-attaque-51 » (09/06/2017).

310. MEDEF, *Livre blanc : « Blockchain pour les entreprises »*, in : CIGREF (http ://www.cigref.fr/), Paris 2017, p. « http://www.cigref.fr/wp/wp-content/uploads/2017/06/Livre-blanc-Blockchain-pour-entreprises.pdf » (30/07/2017).

311. Gasiorowski-Denis Elizabeth, *Adopter le nuage en toute confiance*, in : ISO News (https ://www.iso.org/), Genève 2015, p. « http://www.iso.org/cms/render/live/fr/sites/isoorg/contents/news/2015/01/Ref1921.html » (27/10/2018).

312. Pinaud Florence, *#MaVieSous algorithmes*, 1e éd., Paris 2018, p. 72.

313. *Ibidem.*

314. *Ibidem.*

stratégiques pour les organisations.

Au niveau européen, les aspects juridiques de l'utilisation du Cloud computing font polémiques [315]. Les questions principales concernent le contrôle des données par les utilisateurs et la transparence du traitement des données dans un service de Cloud [316]. Il s'agit de questions en lien avec la confiance numérique. 369

La Suisse se positionne en troisième position en matière de Datacenters dans le monde [317]. De nouveaux centres de données Microsoft et Google sont prévus en 2019, en Suisse. 370

Les Clouds Google « offrent des services de calcul, de gestion de données, de développement d'applications, de stockage, d'analyse de données, ainsi que des outils de collaboration et de mise en réseau. La sécurité est assurée par une puce dédiée dans les serveurs pour détecter et empêcher l'exécution de codes nuisibles. Les données restent sous le contrôle des clients, de même que le choix de la localisation du stockage des données (région suisse et/ou autres régions). Ils offrent enfin des capacités d'analyse de données et de 371

315. Von Lewinski K. / Herrmann C., *Cloud vs. Cloud–Datenschutz im Binnenmarkt*, in : Zeitschrift für Danetschutz 2016 6/10, p. 467 ; Nägele Thomas / Jacobs Sven, *Rechtsfragen des Cloud Computing*, in : ZUM : Zeitschrift für Urheber- und Medienrecht/Film und Recht 2010 54/4, p. 281 ; Kroschwald Steffen, *Kollektive Verantwortung für den Datenschutz in der Cloud– Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing*, in : Zeitschrift für Datenschutz 2013/3, p. 388 ; Molnár-Gábor Fruzsina / Korbel Jo, *Verarbeitung von Patientendaten in der Cloud - Die Freiheit translationaler Forschung und der Datenschutz in Europa*, in : Zeitschrift für Datenschutz (ZD) 2016 6/6, p. 274.

316. Hilgendorf / Seidel, *Robotics, autonomics, and the law*, p. 121 ; Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing - Adopted on 1st July 2012 (WP 196)*, in : European Commission (https ://ec.europa.eu/), Brussels 2012, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf » (04/12/2018), pp. 6-7.

317. Trevor Mark / Inglis Keith / Heard Andrew, *Data Centre Risk Index*, in : Cushman and Wakefield (http ://www.cushmanwakefield .com/), London 2016, p. « http://www.cushmanwakefield.com/en/research-and-insight/2016/data-centre-risk-index-2016 » (27/10/2018).

machine learning intégrées à ces services [318]».

372 La loi fédérale sur la protection des données du 19 juin 1992 a permis à la Suisse d'obtenir, le 26 juillet 2000, une décision d'adéquation avec la directive 95/46 du 6 octobre 1995. Ce type de décision de la Commission européenne constate qu'un pays non membre de l'UE offre un « niveau adéquat » de protection des données personnelles compatible avec celui garanti dans l'Union Européenne. Cette décision d'adéquation permet à l'UE le transfert licite des données personnelles depuis l'UE vers la Suisse et constitue un critère d'évaluation des garanties apportées par un pays concernant la protection des données personnelles traitées par un pays.

373 La promotion des Datacenters est assurée sous le label « VigiSwiss ».

374 L'objectif de Vigiswiss est de promouvoir l'hébergement des données dans les Datacenters du pays, en vue de conserver et de protéger les données confidentielles à l'échelle mondiale, des gouvernements, organisations, entreprises et des particuliers. Pour se voir certifier par l'association, les adhérents (fournisseurs et intégrateurs) s'engagent à se conformer aux différents principes stipulés dans une charte.

375 Les membres de Vigiswiss sont Abissa Informatique (Renens), Cd-Rom (Le Noirmont), ColoBâle (Bâle-Campagne), Data 11 (Soleure), Deltalis (Uri), DNkast (Le Bouveret), Safe Host (Plan-les-Ouates) et Edificom (Lausanne).

376 Les membres de Vigiswiss s'engagent également à ne pas héberger des données illégales en se conformant au code de conduite des hébergeurs suisses [319]. Aucun contenu illégal ne doit être hébergé, qu'il s'agisse de données enfreignant les droits d'auteur ou du contenu condamnable sur le plan pénal (terrorisme, pédopornographie, racisme, diffamation, etc.). Enfin, les membres de Vigiswiss

318. Chavanne Yannick / Schneider Olivier, *Le cloud suisse de Google est ouvert*, in : ICT Journal (https ://www.ictjournal.ch/), Lausanne 2019, p. « https : //www.ictjournal.ch/articles/2019-03-12/le-cloud-suisse-de-google-est-ouvert » (09/06/2019).

319. Chavanne Yannick, *Une nouvelle association veut promouvoir l'hébergement des données en Suisse*, in : ICT Journal (https ://www.ict journal.ch/), Lausanne 2016, p. « https://www.ictjournal.ch/news/2016-02-15/une-nouvelle-association - veut - promouvoir - lhebergement - des - donnees - en - suisse » (21/05/2019).

ou un organisme indépendant effectuent un audit deux fois par an.

En 2016, la plate-forme datacentermap.com dénombrait 70 centres en Suisse, dont deux seraient certifiés TIER IV. « Cette certification atteste de la disponibilité et de la maintenabilité extrême d'un centre » selon Christian Neuhaus, porte-parole de Swisscom. Plus de 25 % des données numériques européennes seraient stockées en Suisse selon le rapport Telegeography [320]. Plus de 200 000 personnes sont employées en Suisse dans ce domaine, soit quatre fois plus que l'industrie horlogère [321]. 377

Le marché de l'informatique en nuage est très concentré. Les revenus d'Amazon, Microsoft, IBM et Google devraient représenter 69,1 % du marché de l'informatique en nuage en 2020, contre 7,8 % pour Alibaba Cloud, numéro un mondial de la vente en ligne, qui tire sa force de la croissance du commerce électronique chinois. Selon le cabinet de recherche Equancy, les chinois disposent de plus de 563 millions téléphones portables (soit plus que ceux des États-Unis, de l'Inde, du Brésil et de la France réunis), dont 400 millions sont clients chez Alibaba. Le chiffre d'affaires du groupe est donc supérieur à celui réalisé par l'ensemble des acteurs du commerce électronique aux États-Unis. 378

Après l'ouverture de quatre nouveaux centres de données en 2016 au Moyen-Orient (Dubaï), en Europe, en Australie et au Japon, pour un milliard de dollars, le groupe Alibaba Cloud se prépare à ouvrir quatre nouveaux centre de données hors de Chine. Ils s'inscrivent dans un programme d'investissement de trois milliard de dollars en infrastructures sur cinq ans [322]. 379

L'informatique en nuage présente l'avantage de pouvoir stocker une grande quantité de données et de mettre à disposition de nom- 380

320. Martin Claire / Galliker Dominik, *La Suisse : un coffre-fort numérique*, in : Swisscom Magazine (https ://magazine.swisscom.ch/), Berne 2017, p. « https://magazine.swisscom.ch/securite-des-donnees-infrastructure/la-suisse-un-coffre-fort-numerique/ » (04/12/2018).

321. Bühler Tiphanie, *Les coffres forts de vos données sensibles*, in : Brainserve (https ://www.brainserve.ch/), Crissier 2016, p. « https://www.brainserve.ch/brainserveweb2/wp-content/uploads/2016/01/201601-PME_Magazine-Datacenters.pdf?516c84 » (04/07/2017).

322. Loukil Ridha, *Alibaba va étendre son cloud mondial avec quatre nouveaux datacenters d'ici 2018*, in : L'Usine Digitale (https ://www. usine-digitale.fr/), Antony 2017, p. « https : / / www . usine - digitale . fr / article / alibaba - va - etendre - son - cloud - mondial - avec - quatre - nouveaux - datacenters - d - ici - 2018.N594138 » (01/04/2019).

breuses applications à des utilisateurs multiples en vue d'une utilisation à la demande. Au lieu d'être stockées sur les disques durs ou mémoires, les données sont disponibles sur des serveurs distants et accessibles par internet.

381 Les données et les applications sont sauvegardées et disponibles sur le Cloud. Elles ne sont plus stockées localement.

382 L'informatique en nuage est disponible à partir des ordinateurs, des smartphones, des tablettes et les services requis sont accessibles de n'importe quel endroit au monde.

383 Les Datacenters qui stockent les données sont des sites physiques sur lequels se trouvent regroupés des ordinateurs, des systèmes de stockage et des équipements de télécommunications [323].

384 L'usage de l'informatique en nuage et des supports de stockage physiques actuels est limité dans le temps. L'ADN semble être la solution pour le stockage des données à l'avenir. Des chercheurs de l'Ecole polytechnique fédérale de Zurich ont « encodé » 83 Ko de données provenant de manuscrits du Moyen- âge, sur un fragment d'ADN, et l'ont inséré dans une minuscule capsule de silice (de 150 nanomètres de diamètre) [324]. Ils ont ensuite simulé un vieillissement accéléré, démontrant qu'au bout de 2000 ans de stockage, les données numériques devraient toujours être intactes.

385 En étant conservées à -18 degrés, la durée de conservation augmente encore pour être portée à des centaines de milliers d'années. L'ADN permet d'augmenter l'espace de stockage jusqu'à 300 000 To contre 5 To pour un disque dur classique [325].

386 Un schéma synoptique de l'informatique en nuage peut être représenté ainsi [326].

323. Soyez Fabien, *L'ADN et le quartz pour stocker nos données pour l'éternité*, in : Techniques de l'Ingénieur (https ://www.techniques-ingenieur.fr/), Saint-Denis 2016, p. « https://www.techniques-ingenieur.fr/actualite/articles/ladn-quartz-stocker-nos-donnees-leternite-33538/ » (21/05/2019).
324. Jacobs Angelika, *Data-storage for eternity*, in : ETH (https ://ethz.ch/), Zürich 2015, p. « https://www.ethz.ch/en/news-and-events/eth-news/news/2015/02/data-storage-for-eternity.html » (02/05/2017).
325. Soyez, *L'ADN et le quartz pour stocker nos données pour l'éternité.*
326. *« Cloud computing »*, in : Wikipedia, Terminologie, sémantique, p. « https://fr.wikipedia.org/wiki/Cloud_computing » (01/06/2017).

Quelles répercussions le stockage des données à caractère personnel peut-il avoir sur la protection des données et la sécurité des données à caractère personnel ? La protection des données stockées dans des Clouds est au cœur d'enjeux de confiance [327] et soulève de 387

327. Hashem Ibrahim Abaker Targio, *The rise of "big data" on cloud computing : Review and open research issues*, in : Information Systems 2015/47, pp. 98-115.

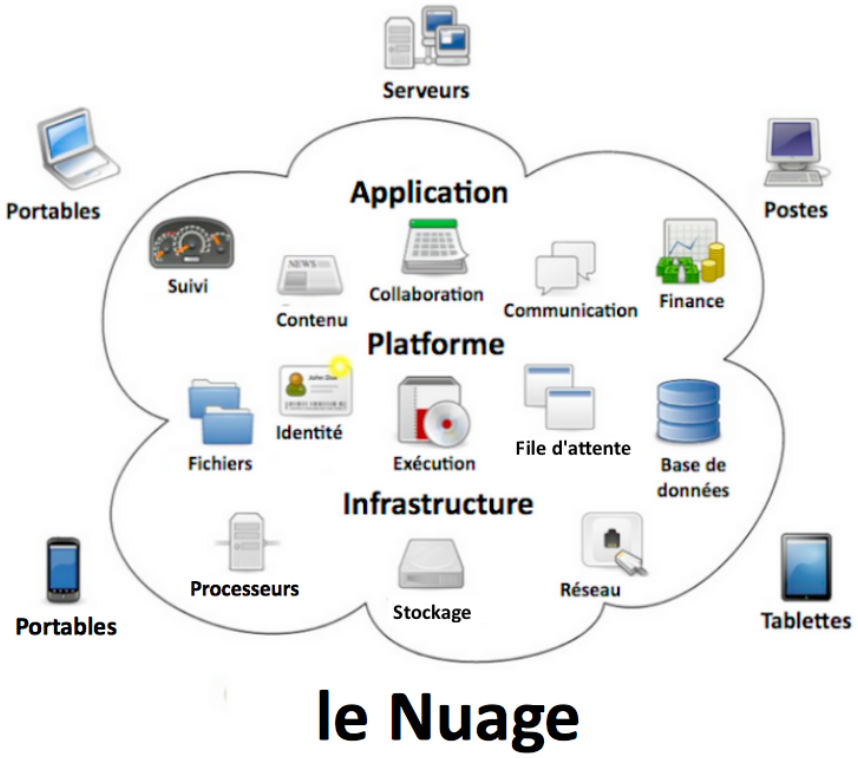

Figure 2.8 – Schéma synoptique de l'informatique en nuage. Source : Wikipedia.

nombreuses questions juridiques [328] et de sécurité [329].

388 Les responsabilités et obligations juridiques en matière de protection des données répondent au schéma suivant : le client (responsable du traitement) détermine les finalités et les moyens du traitement des données à caractère personnel, alors que le fournisseur de services (sous-traitant) n'agit que sur instructions du client pour traiter effectivement les données.

389 Cependant, les rôles de chaque partie ne sont pas toujours aussi clairement répartis dans le Cloud Computing. Le fournisseur de services en nuage peut prendre des décisions essentielles concernant les moyens et les conditions de traitement des données à caractère personnel. Il peut par exemple décider de l'endroit où les données sont stockées, avoir recours à des sous-traitants et décider des mesures de sécurité.

390 Le contrôle des données personnelles peut en outre être partagé entre l'utilisateur et le fournisseur de services.

391 Si la répartition des obligations et des responsabilités entre les utilisateurs et les fournisseurs de service en nuage n'est pas définie avec précision par contrat, il existe le risque d'une dilution de responsabilité en matière de protection des données. Concrètement, cela signifie que la protection des données serait dans ce cas précis, insuffisante pour offrir des garanties de protection effectives à

328. Métille Sylvain, *L'utilisation de l'informatique en nuage par l'administration publique*, in : AJP/PJA 2019/6, pp. 609-621 ; Métille Sylvain, *L'informatique en nuage au sein d'une étude d'avocats*, in : Plaidoyer 2013 31/3, pp. 39-43 ; Sobati Moghadam Somayeh / Darmont Jérôme / Gavin Gérald, *Enforcing Privacy in Cloud Databases*, in : Big Data Analytics and Knowledge Discovery 2017, pp. 53-73.

329. Katal Avita / Wazid Mohammad / Goudar R. H., *Big data : Issues, challenges, tools and Good practices*, in : Sixth International Conference on Contemporary Computing (IC3), Noida 2013, pp. 404-409 ; Chang Victor / Ramachandran Muthu, *Towards Achieving Data Security with the Cloud Computing Adoption Framework*, in : IEEE Transactions on Services Computing 2016 9/1, pp. 138-151 ; Agarwal Sonali / Tarbotton Lee Codel Lawson, *System and method for preventing data loss using virtual machine wrapped applications*, in : United States Patent 2017, p. « https://patents.google.com/patent/US9552497B2/en » (26/10/2018) ; Usman Muhammad / Ahmad Jan Mian / He Xiangjian, *Cryptography - based secure data storage and sharing using HEVC and public clouds*, in : Information Sciences 2017/387, pp. 90-102.

l'utilisateur.

Les informations à caractère personnel traitées dans le nuage sont généralement acheminées par - et sont stockées dans - diverses juridictions à travers le monde. Dans de nombreux pays où l'information est traitée ou stockée, la législation en matière de protection des données diffère de celle de l'UE et n'offre pas toujours un degré de protection équivalent. Cela engendre un risque que l'information soit accessible sans restriction ou éventuellement utilisée de manière abusive, sans que les particuliers ne soient capables d'exercer leurs droits de protection des données comme ils auraient pu le faire au titre du droit de l'UE. 392

Les fournisseurs de services en nuage doivent, dès lors, garantir par le biais d'un contrat avec l'utilisateur ou de règles d'entreprise contraignantes, que tous les transferts d'informations vers des juridictions non européennes ou dont le droit n'est pas jugé équivalent au droit de l'UE, rempliront des exigences spécifiques en matière de protection des données afin de fournir des sauvegardes adéquates. La Suisse présente l'avantage d'avoir une législation en matière de protection des données qui soit reconnue comme équivalente à la législation européenne ce qui rend licite les transferts de données entre l'UE et la Suisse. 393

Les autorités répressives peuvent avoir la capacité de demander aux fournisseurs de services en nuage qui opèrent dans leur juridiction l'accès aux informations stockées dans le nuage. Le fournisseur de services en nuage peut alors être confronté à des obligations juridiques contradictoires. 394

Idéalement, en vertu des termes du contrat, les utilisateurs doivent être informés de ces demandes d'accès. Le CEPD a recommandé que les informations ne soient transmises aux organismes répressifs que dans le cadre de procédures claires définies dans des accords internationaux ou bilatéraux. De telles procédures sont à l'étude, mais, dans de nombreux cas, ne constituent pas encore des accords officiels. 395

VI. Le Big Data

Les nouveaux modèles économiques reposent sur la collecte, l'analyse et la transmission d'importants volumes de données. (Big Data) Ils facilitent la personnalisation de biens et des services et les gains 396

de productivité [330].

397 La notion de Big Data se réfère à une grande quantité de données provenant de sources diverses et qui sont saisies et enregistrées grâce à des systèmes de traitement à très haut débit, en vue de permettre leur exploitation et leur analyse sans but prédéterminé et sans limite de temps [331]. Ces procédures de traitement intensives ont été rendues possibles par les progrès technologiques, qui ont permis d'accélérer considérablement l'enregistrement et l'exploitation d'immenses quantités de données, tout en réduisant fortement le coût de ces opérations [332].

398 La technologie algorithmique permet aujourd'hui d'analyser et d'interconnecter facilement de très grandes quantités de données. Corrélations, similitudes, liens ou divergences sont ainsi mis en évidence facilement [333]. Ces données sont analysées et permettent de reconstituer les modes de comportements et les préférences des individus.

399 Les Big Data se caractérisent par 4 éléments :

400 Ce sont de grandes quantités de données (Volume), traitées à grande vitesse (Velocity). Elles se caractérisent aussi par la diversité ou l'hétérogénéité (Variety) des données [334].

401 Les données peuvent être corrélées et provenir de sources différentes qui n'étaient pas interconnectées jusqu'ici. C'est ainsi qu'il est possible de mettre en relation des données enregistrées dans un smartphone (ex : nombre de pas), avec des données externes provenant de réseaux sociaux, de moteurs de recherche, de feuilles d'avis officielles ou de portails de données ouvertes gérés par des autorités publiques. Enfin, les Big Data produisent une plus-value (Value) du fait de l'analyse des données [335].

402 Les Big Data présentent la spécificité de pouvoir utiliser des informations non structurées (contenu d'emails, de chats, de conversations téléphoniques) et hétérogènes en les reliant et en les exploi-

330. PFPDT, *24ème Rapport d'activités.*
331. Delort Pierre, *Le big data (Que sais-je ?)*, 2e éd., Paris 2018, pp. 29-47.
332. *Ibidem.*
333. *Ibidem.*
334. *Ibidem.*
335. *Ibidem.*

tant commercialement [336].

Si les Big Data ouvrent de nouvelles perspectives pour la recherche fondamentale, grâce à la mise à disposition libre et gratuite de données de grande dimension (OpenData), elles peuvent aussi menacer l'autodétermination informationnelle et la sphère privée. C'est précisément le cas lorsque les données traitées sont utilisées à des fins de profilage commercial ou de discriminations entre individus. Par exemple, des Big Data collectées par une compagnie d'assurance pourraient servir demain à servir de fondement au refus de conclure un contrat d'assurance, si l'analyse des données donnait lieu à une forte probabilité de survenance ultérieure d'une maladie incurable. 403

Tobias Fasnacht [337] suggère qu'à intervalles réguliers, la personne concernée reçoive une copie des données à caractère personnel traitées par le responsable du traitement et que la validité de son consentement soit vérifiée auprès de la personne concernée. Il envisage également la création d'une entité «tiers de confiance» située entre la personne concernée et le responsable du traitement chargée de l'administration du consentement de la personne concernée [338]. La technologie Blockchain pourrait être employée, pour que la personne concernée gère son consentement en direct, dans le respect de l'article 27 du code civil suisse. En pratique, cette solution, paraît cependant peu réaliste, du fait des volumes de données considérés. 404

Dans le domaine politique, les algorithmes d'analyse de données massives pourraient être utilisés par des services de renseignements pour identifier des risques géopolitiques, ou pour pratiquer une surveillance permanente et multiforme des citoyens, à leur insu. L'œuvre de fiction écrite par Georges Orwell dans son livre 1984, est techniquement réalisable au XXIème siècle. L'émergence des technologies du Big Data et de l'internet des objets rendent cette 405

336. *Ibidem.*
337. Fasnacht Tobias, *Die Revision der Datenschutzkonvention des Europarates : Implikationen für die Schweiz*, in : Schweizerisches Jahrbuch für Europarecht = Annuaire suisse de droit européen 2011, p. 228 ss.
338. Delort, *Le big data*, p. 271.

fiction réaliste [339].

406 L'usage des données personnelles soulèvent ainsi des questions éthiques [340] et sociétales [341] du fait du volume de données à caractère personnel, collectées et interconnectées pour dresser des profils de personnalité. Collectées et exploitées de manière systématique et structurée, les Big Data représentent une opportunité commerciale, mais aussi un risque pour la sphère privée des individus et le respect des droits de l'homme [342].

407 Les analyses prédictives peuvent en particulier constituer des barrières à l'entrée et être la source de discriminations [343]. Lors de décisions prises sur une base uniquement automatisée, un contrôle humain est donc essentiel.

408 Les applications des Big Data sont multiples : réseaux sociaux (analyse de personnalité et des opinions politiques), santé (diagnostics médicaux approfondis), transports (analyse des déplacements), élections (analyses des votes), marketing (études de marché automatisées, analyses web en vue d'étendre et d'optimiser des campagnes de marketing en ligne, reconnaissance faciale, vocale, digitale...), prévention (délits, crimes), détection (fraude dans le domaine des transactions financières, lutte contre blanchiment d'argent), recherches par quadrillage ou par profilage pour le compte de services de renseignement ou de police.

409 Avec l'augmentation des capacités de scoring, le risque d'erreur dans l'attribution des scores augmente. Dans le domaine des crédits, les systèmes de scoring sont fondés sur les données collectées par d'autres établissements de crédit. Ainsi, si une personne ne détient pas de crédit, elle ne sera pas en mesure de recevoir un score, puisqu'il n'existe aucun historique donc aucun donnée concernant cette personne. Cela résulte en pratique à des discriminations, qui

339. Applied Machine Learning Day (30-31 January 2017), in : Ecole Polytechnique Fédérale de Lausanne (https://www.epfl.ch/), Lausanne 2017, p. « http://memento.epfl.ch/event/applied-machine-learning-days/ » (28/06/2017).
340. Mittelstadt Brent Daniel / Floridi Luciano, *The Ethics of Big Data : Current and Foreseeable Issues in Biomedical Contexts*, in : Science and Engineering Ethics 2016 22/2, pp. 303-341.
341. Cuquet Marti, *Societal impacts of big data : challenges and opportunities in Europe*, in : arXiv preprint (http ://arxiv .org/), s.l. 2017, p. « http://arxiv.org/abs/1704.03361 » (28/10/2018).
342. Weber / Staiger, *Transatlantic Data Protection in Practice*, p. 101.
343. *Ibidem.*

sont infondées [344].

L'utilisation des Big Data s'est développée dans le domaine judiciaire aux États-Unis. Ces données contribuent activités de prévention, facilitent l'identification des criminels [345] tout en présentant un risque accru de stigmatisation pour certaines communautés [346]. 410

En application du principe de proportionnalité, les données doivent être si possible anonymisées. Cette option est prévue dans la loi suisse [347]. Le Préposé fédéral a insisté sur ce point dans son rapport d'activités présenté devant l'Assemblée fédérale en Juin 2017 : « Le Préposé fédéral doit s'assurer que les données collectées soient anonymisées d'une façon qui exclut, avec une probabilité suffisante, toute identification rétroactive, au moyen des technologies actuelles ». 411

L'anonymisation des données personnelles rend difficile pour le responsable du traitement la mise en œuvre effective du droit à l'oubli ou du droit à la suppression des données. 412

Ceci d'autant plus lorsque les données ont été transférées à des sous-traitants. En cas de violation de l'art. 17 RGPD, une amende pourra être prononcée (art. 83. al. 5 RGPD) [348]. 413

Chaque personne étant unique, l'anonymisation des données personnelles est rarement irréversible. Une étude scientifique du MIT est venue démontrer en 2015 que même anonymisées, l'identification de la personne concernée est possible du fait de la seule interconnexion de métadonnées [349]. Selon le Règlement e-privacy, la collecte et l'utilisation des « *métadonnées de communications électroniques* » sera licite seulement avec le consentement de la personne concernée. Du fait du caractère unique des comportements humains, la ré-identification est possible [350]. 414

Prof. Yves-Alexandre De Montjoye a prouvé que 4 paramètres suf- 415

344. *Idem*, p. 103.
345. *Idem*, p. 105.
346. *Idem*, p. 106.
347. art. 9, al. 2 LTrans, et art. 19, al. 1 LPD.
348. Paal Boris P. / Pauly Daniel A., *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, 1e éd., München 2018, p. 225.
349. de Montjoye Yves-Alexandre, *Unique in the Crowd : The privacy bounds of human mobility*, in : Nature Scientific Reports 2013/3, p. 2.
350. *Ibidem*; de Montjoye Yves-Alexandre, *openPDS : Protecting the Privacy of Metadata through SafeAnswers*, in : PLoS one 2014 9/7, pp. 1-9.

fisent pour identifier 95 % des personnes enregistrées dans une base de données composée de 1,5 millions de personnes. Il a également démontré que dans les deux cas, des données brutes ou floues, ne garantissent pas l'anonymat [351].

416 Le niveau de détail des données, leur caractère unique, leur accumulation et leur interconnexion peuvent permettre une réidentification de la personne concernée [352]. Cette évolution porte atteinte aux droits de la personnalité, notamment lorsque des données sensibles sont traitées [353].

417 Prof. Wachter propose de créer un nouveau droit intitulé « reasonable inference » et qui peut se traduire comme un « droit à une déduction raisonnable ». Cette proposition apparaît fondée, compte tenu des évolutions technologiques actuelles.

418 Si l'anonymisation des données personnelles ne constitue plus réellement une garantie suffisante pour les personnes concernées, le législateur devrait faire évoluer sa législation et demander l'application du RGPD aux données anonymisées ce qui n'est pas le cas aujourd'hui. La pratique sera également amenée à évoluer : un refus d'entrer en matière sur une demande de suppression des données ou d'exercice du droit à l'oubli au motif que les données sont anonymisées pourrait des lors être considéré comme infondé. En cas de doute quant à l'identité de la personne, le responsable du traitement pourrait demander des informations complémentaires (art. 12. al. 6 RGPD) [354].Un responsable de traitement dont les données sont volées pourrait en outre voir sa responsabilité engagée malgré l'anonymisation des données, en fonction du cas d'espèce, sur le fondement qu'il ne pouvait pas ignorer le risque de ré-identification ultérieure.

419 Aux États-Unis, l'administration du Président Obama a produit un rapport qui établit que les technologies de Big Data peuvent causer des dommages sociaux qui vont au-delà des dommages relatifs à la vie privée [355]. Ce rapport souligne que les décisions prises sur

351. de Montjoye, *Unique in the Crowd*, p. 2.
352. PFPDT, *24ème Rapport d'activités*, p. 23.
353. Baeriswyl Bruno, *Anonymisierung von genetischen Daten ? : (datenschutz)rechtliche Aspekte der Anonymisierung bei Biobanken*, in : Digma - Zeitschrift für Datenrecht und Informationssicherheit 2008/8, pp. 14-17.
354. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 225.
355. United States / Executive Office of the President / Podesta, *Big data*,

la base des Big Data pourraient avoir des effets discriminatoires, même sans intention discriminatoire initiale lors de la programmation. Le Conseil de l'Europe a ainsi créé un groupe de travail dédié á l'IA et aux droits de l'homme [356].

Du fait des enjeux, la confiance dans les produits et les services digitaux devient centrale. Les mécanismes de soft law (labels de qualité, certifications) combinés aux contrôles des autorités administratives deviennent essentiels. L'effectivité de ces contrôles est cependant difficile du fait des volumes de données concernés et de la nature transnationale des activités (ex : plateformes en ligne). 420

La gouvernance des technologies digitales et l'effectivité du droit de la protection des données constituent un défi central à l'ère des Big Data. Ce défi est d'autant plus grand que les données sont collectées et analysées par des processus qui reposent sur des puissances de calcul croissantes et des algorithmes d'intelligence artificielle,de plus en plus autonomes, opaques, et difficilement intelligibles. 421

VII. L'intelligence artificielle (ci-après «IA»)

Le terme d'intelligence artificielle (« ci-après IA ») a été créé en 1956 par Marvin Minsky [357] du Massachussett Institut of Technology (MIT) aux États-Unis. 422

L'IA repose sur des algorithmes, qui sont une suite d'opérations ordonnées, bien définies, exécutables sur un ordinateur qui permettent d'arriver à la solution en un temps raisonnable. Les principales composantes d'un système d'IA sont les données, le raisonnement, la compréhension du langage naturel et l'apprentissage selon le mathématicien et cryptologue britannique Alan Turing. 423

Gordon Moore, en 1964 avait constaté que que la puissance des microprocesseurs doublaient tous les 18 mois, accordant ainsi deux fois plus de mémoire et de rapidité de calcul aux ordinateurs. Cette observation est qualifiée de « loi de Moore ». Se basant sur cette loi, certains prédisent que les ordinateurs seront de plus en plus puis- 424

pp. 1-85.

356. Conseil de l'Europe, *Conseil de l'Europe et intelligence artificielle*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 2020, p. « https://www.coe.int/fr/web/artificial-intelligence/home » (03/01/2020).

357. Minsky Marvin, *Steps toward Artificial Intelligence*, in : Proceedings of the IRE 1961 49/1, pp. 8-30.

sants, rapides et efficaces, ce qui est contesté par les chercheurs qui observent un ralentissement de cette évolution.

425 Avec l'essor des supercalcultateurs, la capacité et la vitesse de calcul des ordinateurs a permis d'augmenter le nombre de données traitées de manière exponentielle. L'analyse des mégadonnées ou Big Data, données qui se mesurent en pétaoctets (millions de milliards d'octets) est ainsi devenue réalité. Grâce à leur capacité d'analyse, les prédictions gagnent tous les secteurs d'activité, publics ou privés. Transport, défense, urbanisme police prédictive, éducation(data-driven education), la justice prédictive, scoring des individus par les établissements de crédits, les universiteés, reéseaux sociaux, médecine personnalisée, la composition musicale, l'écriture de scénarios, robotique intelligente, logistique..).

426 La combinaison de la disponibilité des données personnelles, des capacités d'analyse des algorithmes et de la puissance de calcul des ordinateurs améliore les prédictions, augmente les économies d'échelle et les gains de productivité, facilite la résolution de problèmes complexes et transforme les organisations sociales traditionnelles [358].

427 Selon une étude du cabinet Accenture, l'apprentissage-machine (ou « Machine Learning ») et l'intelligence artificielle en particulier, permettront d'atteindre une croissance économique de 4,6 % aux États-Unis en 2035 [359] et de 2.7 % au Japon, durant la même période en ayant recours à ces technologies (soit trois fois son taux de croissance actuel). Selon la même étude, l'Allemagne, l'Autriche, la Suède et la Hollande verraient leur taux de croissance annuel doubler durant cette même période.

428 Pour Jean-Gabriel Ganascia, Professeur à l'université Pierre et Marie Curie, « les agents artificiels programmés avec des techniques d'IA sont des systèmes complexes capables de réaliser des tâches précises. Mais ils sont incapables d'utiliser leurs compétences pour

358. Domingos Pedro, *The Master Algorithm : How the Quest for the Ultimate Learning Machine will Remake Our World*, 1e éd., New York 2018, Prologue, p. xiv ; Crawford Kate / Calo Ryan, *There is a blind spot in AI research*, in : Nature News 2016 538/7625, p. 311.

359. Purdy Mike / Daugherty Paul, *Why artificial intelligence is the future of growth ?*, in : Remarks at AI Now : The Social and Economic Implications of Artificial Intelligence Technologies in the Near Term 2016, pp. 1-72.

d'autres tâches ».

Une des innovation majeures est l'apprentissage machine ou ma- 429
chine learning. Avec cette technique, l'ordinateur apprend seul comment résoudre un problème posé. L'homme lui montre les bonnes associations entre les paramètres et les résultats, jusqu'à ce qu'il arrive seul à effectuer des déductions [360]. Des applications surprenantes en sont issues. En 2016, l'IA AlphaGo a battu le champion européen Fan Hui. Son architecture technologique est inspirée du cerveau humain et repose sur « un réseau de neurones [361]». En 2017, une IA dénommée Libratus a battu au poker les champions du monde Jason Les, Dong Kim, Jimmy Chuo et Daniel McAulay durant trois semaines de de compétition. L'IA a appris en observant le comportement des joueurs durant les trois semaines de tournois et en testant les différentes stratégies. La même entreprise DeepMind a ensuite développer un projet de recherche dans le domaine médical au Royaume-Uni et a obtenu l'accès aux données personnelles de santé de millions de patients pour un projet de recherche médical [362]. Les personnes concernées étaient identifiable ce qui a provoqué une perte de confiance dans l'entreprise et les autorités compétentes britanniques [363]. La technique de Machine Learning peut également avoir un impact dans le domaine politique. En 2018, 87 millions de comptes d'utilisateurs Facebook ont été transférés à la société Cambridge Analytica pour analyse et création de profils de personnalité dans l'objectif d'influencer les élections présidentielles américaines [364]. La question de l'éthique dans l'utilisation des technologies d'IA et de Machine Learning et celle de la responsa-

360. Pinaud, *#MaVieSous algorithmes*, p. 31.
361. Gibney Elizabeth, *What google's winning go algorithm will do next*, in : Nature News 2016 531/7594, p. 284 ; Wang Fei-Yue, *Where does AlphaGo go : From church-turing thesis to AlphaGo thesis and beyond*, in : IEEE/CAA Journal of Automatica Sinica 2016 3/2, pp. 113-120.
362. Powles Julia / Hodson Hal, *Google DeepMind and healthcare in an age of algorithms*, in : Health and technology 2017 7/4, pp. 351-367.
363. *Ibidem.*
364. Granville Kevin, *Facebook and Cambridge Analytica : What You Need to Know as Fallout Widens*, in : The New York Times (https ://www.nytimes.com/), New York 2018, p. « https : / / www . nytimes . com / 2018 / 03 / 19 / technology / facebook - cambridge - analytica - explained . html » (28/07/2019).

bilité des acteurs sont désormais au centre des discussions [365].

430 La Commission Européenne a publié en avril 2019, un rapport invitant les entreprises à mettre en œuvre et à respecter plusieurs principes éthiques lors de la conception ou de l'usage de solutions d'IA. La maîtrise des risques éthiques qui naissent de l'IA va devenir un enjeu essentiel de la confiance dans les systèmes déployés sur le marché. Code de conduite, formation à l'éthique pour les ingénieurs, certification de qualité des systèmes d'intelligence artificielle devraient se développer pour le déploiement de systèmes éthiques. Ceci est confirmé par la prise de position officielle de l'IEEE en juin 2019 qui préconise l'intégration d'éléments éthiques dans les systèmes intelligents et autonomes [366].

431 La CNIL, avait lancé dés le mois de décembre 2016, un débat public et décentralisé en France sur l'éthique des algorithmes. Il avait pour objectif de faire progresser la connaissance et la réflexion sur ces questions et d'établir un panorama des défis et enjeux.

432 Ce vaste processus de discussion collectif invitait tous les acteurs – institutions publiques, société civile, entreprises, citoyen – qui souhaitaient y prendre part à organiser des discussions (colloques, séminaires, ateliers), pour sensibiliser le public et approfondir les questions éthiques soulevées par les algorithmes dans divers secteurs d'activité (santé, justice prédictive, éducation, etc.). À l'automne 2017, la CNIL a rendu publique la synthèse des échanges et des contributions. La question des critères sous-jacents à la conception (design) des intelligences artificielles fut au centre des discussions [367].

433 Bien que la législation européenne sur la protection des données consacre le principe de neutralité technologique, il s'agit avant tout d'une fiction juridique qui s'exprime à travers des notions géné-

365. Zunger Yonatan, *Computer Science Faces an Ethics Crisis*, in : The Boston Globe (https://www.bostonglobe.com/), Boston 2018, p. « https://www.bostonglobe.com/ideas/2018/03/22/computer-science-faces-ethics-crisis-the-cambridge-analytica-scandal-proves/IzaXxl2BsYBtwM4nxezgcP/story.html » (28/07/2019).

366. IEEE, *IEEE Position Statement : Ethical Aspects of Autonomous and Intelligent Systems*, in : IEEE (https ://www.ieee.org), New Jersey 2019, p. « https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE19002.pdf » (05/07/2019).

367. Etzioni Amitai / Etzioni Oren, *Designing AI Systems That Obey Our Laws and Values*, in : Communications of the ACM 2016 59/9, pp. 29-31.

riques de données, de traitements ou d'opérations [368] éloignée de la réalité technologique. Si les principes et les concepts juridiques sont neutres sur le plan technologique [369], ils ne sont pas toujours applicables (ex : droit d'explication et algorithmes non supervisés d'IA, droit à l'oubli et technologie Blockchain). Dans les faits les processus de décisions en lien avec la création des algorithmes d'intelligence artificielle, la gestion des données d'entraînement des algorithmes et le design des architectures conditionnent le fonctionnement futur des produits et des services digitaux.

Pour accroître la confiance des utilisateurs et des investisseurs, la question de la création de systèmes d'auditabilité, de contrôle des algorithmes et de la qualité des données se pose de manière centrale [370]. 434

Le conseiller informatique de Barack Obama, Dr. Ed. Felten estime cependant que « tenter de comprendre le fonctionnement d'une intelligence artificielle revient à essayer de décrypter le fonctionnement du cerveau humain [371] ». 435

La complexité des processus en jeu rend certaines décisions inintelligibles et non interprétables. Cet état de fait justifie à lui seul la mise en œuvre de mécanismes de régulation [372]. Ceux-ci doivent être suffisamment souples pour encourager les investissements dans la zone euro et l'innovation tout en garantissant le respect effectif des droits de l'homme et des libertés fondamentales tels que définis dans la Charte des droits fondamentaux de l'UE, rendue contrai- 436

368. Bensoussan Alain (direct.), *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques*, 2e éd., Bruxelles 2018, p. 18.
369. *Ibidem.*
370. Gunning David, *Explainable Artificial Intelligence (XAI)*, in : Defense Advanced Research Projects Agency (DARPA) and Web (https ://www.darpa.mil/), s.l. 2017, p. 36 ; Langley Pat, *Explainable Agency for Intelligent Autonomous Systems*, in : 29th Conference on Innovative Applications of Artificial Intelligence, San Francisco 2017, p. 1 ; Wachter Sandra / Mittelstadt Brent Daniel / Floridi Luciano, *Transparent, explainable, and accountable AI for robotics*, in : Science Robotics 2017 2/6, pp. 1-5.
371. Felten Ed, *What does it mean to ask for an "explainable" algorithm ?*, in : Freedom To Tinker (https ://freedom-to-tinker.com/), s.l. 2017, p. « https : //freedom-to-tinker.com/2017/05/31/what-does-it-mean-to-ask-for-an-explainable-algorithm/ » (28/10/2018).
372. Thelisson Eva / Padh Kirtan / Celis L. Elisa, *Regulatory Mechanisms and Algorithms towards Trust in AI/ML*, in : Proceedings of the IJCAI 2017 Workshop on Explainable Artificial Intelligence (XAI), Melbourne 2017, pp. 1-5.

gnante avec l'entrée en vigueur du Traité de Lisbonne en 2009 [373]. Le contrôleur européen à la protection des données a publié en 2019 des lignes directrices sur ce thème pour conseiller les autorités administratives en charge de la protection des données dans les États membres [374].

437 Philippe Cahen indique avec justesse que « l'algorithme est prédictif de la continuité du passé ». Si les données collectées correspondent à un événement ponctuel, il ne fait aucun sens d'en déduire des associations logiques entre cet événement et une prédiction future. En revanche, certaines association effectuées sur des données exactes et révélatrices de comportements constants dans la durée ont mis en lumières des relations de cause à effets d'une grande importance. Ce fut le cas du lien entre le cancer et l'amiante. En analysant les cas de centaines de jeunes femmes souffrant de cancer, l'algorithme d'IA a repéré que nombreuses vivaient dans des ports. Or de vieux cargos se trouvent dans les ports et ceux-ci ont de l'amiante. Ces jeunes femmes travaillaient dans des ports et étaient exposées à l'amiante [375].

438 L'algorithme prédit un comportement humain et peut donc se tromper. Si les habitudes des personnes examinées changent, les prédictions seront erronées. A titre d'exemple, nous pouvons citer, dans le domaine des élections présidentielles, François Fillon était annoncé au second tour. Or Emmanuel Macron s'est retrouvé au second tour de la présidentielle avec Marine Le Pen. Emmanuel Macron de représentait ni la gauche, ni la droite. Par conséquent, l'algorithme prédictif ne pouvait pas se fier aux données du passé pour voir comment ses chances évolueraient. Cette situation ne s'étant pas présentée dans le passé, il était impossible de prédire le résultat de cette élection [376].

439 Si l'intelligence artificielle est un outil au service du traitement des données, certains courants de pensée ont envisagé des appli-

373. Thelisson / Padh / Celis, *Regulatory Mechanisms and Algorithms towards Trust*, pp. 1-5.
374. EDPS, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, in : EDPS (https ://edps.europa.eu/), Brussels 2019, p. « https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf » (23/03/2020).
375. Pinaud, *#MaVieSous algorithmes*, p. 49.
376. *Idem*, p. 51.

cations, favorisant l'augmentation des capacités humaines. Faisant un parallèle entre le cerveau et la logique computationnelle (« calculatoire ») des ordinateurs, certains chercheurs comme Marvin Minsky ont envisagé l'émergence d'une « superintelligence [377] » excédant l'intelligence humaine en 2030 (singularité). Ces théoriciens font partie du courant transhumaniste, notion apparue en 1966 sous la plume du professeur américano-perse F.M. Esfandiary, alors qu'il enseignait à la New School of Social Research de New York, ainsi que dans les ouvrages d'Abraham Maslow, Toward a Psychology of Being (1968). Au niveau académique, les philosophes universitaires tels que le Suédois Nick Bostrom, qui enseigne à l'Université d'Oxford, et les Anglo-saxons David Pearce, Richard Dawkins et James Hughes, ont fait connaître ce courant transhumaniste.

Pour Luc Ferry, il existe deux grands courants au sein du transhumanisme. Le premier reste dans un cadre « biologique » et se réclame d'une tradition humaniste classique, celle des théoriciens de la « perfectibilité » infinie de l'homme et du progrès sans fin comme le philosophe Condorcet (1743-1794). Le second, est favorable à une hybridation homme/machine par le biais de la robotique, de l'intelligence artificielle (IA) et de la biologie [378]. Le transhumaniste cybernétique repose sur l'idée que des machines dotées d'une intelligence artificielle seront séparables du corps biologique (comme l'information et son support). L'être humain pourrait ainsi stocker sa mémoire sur des machines [379]. 440

Au niveau médical, « il s'agit pour les tenants du courant transhumaniste de passer d'une médecine thérapeutique classique – dont la finalité depuis des millénaires était de soigner, de « réparer » les corps accidentés ou malades – au modèle de « l'augmentation » de l'être humain [380]. De là, l'ambition de combattre le vieillissement [381] et d'augmenter la longévité humaine, non seulement en éradiquant les morts précoces, mais en recourant à la techno-médecine, à l'in- 441

377. Bostrom, *Superintelligence*, p. 22 ; Harrison Harry / Minsky Marvin, *The Turing option : A Novel*, New York 1992, p. 12.
378. Ferry Luc, *La révolution transhumaniste*, Paris 2016, p. 54.
379. *Idem*, p. 57.
380. *Idem*, p. 52.
381. Brinon Jacques, *Avec Calico, Google veut s'attaquer à la vieillesse et à la maladie*, in : Le Monde (https ://www.lemonde.fr/), Paris 2013, p. « https://www.lemonde.fr/technologies/article/2013/09/18/avec-calico-google-veut-s-attaquer-a-la-vieillesse-et-a-la-maladie_3480153_651865.html » (28/10/2018).

génierie génétique et à l'hybridation homme/machine, pour faire vivre les humains vraiment plus longtemps. Google a investi des centaines de millions de dollars dans ce projet [382]».

442 Le slogan du courant transhumaniste est le suivant « *From chance to choice* [383]». Il propose de passer du hasard aveugle des caractéristiques génétiques au choix éclairé afin de lutter contre les inégalités naturelles [384].

443 Il s'agit d'une vision eugénique de l'homme, fort inquiétante. Modifier l'une de nos principales caractéristiques implique inévitablement de modifier un complexe, un ensemble interconnecté de traits, et nous ne pourrons jamais prévoir le résultat final.

444 A la différence de l'eugénisme de l'idéologie nazie, « cet eugénisme n'est cependant pas étatique, il relève de la liberté individuelle. Ensuite, il se veut non-discriminatoire, puisqu'il souhaite supprimer les injustices de naissance. Il s'inscrit donc dans une perspective démocratique : à l'égalité économique et sociale, il entend bien ajouter l'égalité génétique [385]». Enfin, il est tout le contraire de l'eugénisme nazi, attendu qu'il veut, non pas éliminer les faibles ou les supposés « fous », mais au contraire réparer, voire augmenter les qualités humaines que la nature distribue de manière à la fois parcimonieuse et inégalitaire [386].

445 Cette différentiation par rapport à l'eugénisme issu de l'idéologie nazie pourrait faciliter son acceptation sociale et c'est précisément ce qui rend dangereux ce courant idéologique.

446 Président de la cité des sciences, à Paris, Joël de Rosnay envisage « la symbiose de l'intelligence artificielle avec l'homme » ainsi que l'émergence d'une « intelligence collective augmentée » ou le l'émergence d'un « l'hyperhumanisme » à la différence du transhuma-

382. Ferry, *La révolution transhumaniste*, p. 76.
383. Tassel Camille, *Luc Ferry : « Le transhumanisme parie sur le fait que l'homme est perfectible »*, in : Le Monde des Religions (http ://www. lemondedesreligions.fr/), Paris 2016, p. « http://www.lemondedesreligions.fr/savoir/luc-ferry-le-transhumanisme-parie-sur-le-fait-que-l-homme-est-perfectible-17-06-2016-5548_110.php » (21/05/2019).
384. *Ibidem* ; Brinon, *Avec Calico, Google veut s'attaquer à la vieillesse et à la maladie.*
385. Ferry, *La révolution transhumaniste*, p. 45.
386. *Idem*, p. 67.

nisme [387]. « Les interfaces symbiotiques du futur, seront directement implantées sur la peau, dans la tête ou les vêtements [388]». Ils auront la forme d'outils émetteurs-récepteurs communiquant directement du corps vers la machine (internet des objets).

Les penseurs Francis Fukuyama ou Jürgen Habermas, ont souligné 447
l'importance de s'interroger sur les questions de gouvernance [389] et sur les questions éthiques que cette nouvelle conception va poser [390]. Jürgen Habermas souligne le lien entre ces questions éthiques et la notion d'identité, c'est-à-dire « à ce que nous sommes et à ce que nous voulons être en tant qu'être humain [391]». Le progrès des biosciences et des biotechnologies place l'organisme humain dans le domaine de l'intervention, en l'assimilant à un objet potentiellement relié à Internet et pouvant générer et transmettre des données personnelles par le biais corporel [392]. Ainsi la distinction proposée par Helmuth Plessner entre « être un corps » et « avoir un corps » acquiert une actualité surprenante [393]. Selon lui les frontières entre la nature que nous sommes et l'équipement organique que nous nous donnons d'estompe [394]. Habermas plaide pour un « consensus rationnellement motivé » et estime que seule une « éthique de la discussion », en nous permettant de nous accorder librement sur le choix des normes auxquelles nous acceptons de nous soumettre, peut aujourd'hui fonder nos valeurs morales [395]. La compréhension moderne de la liberté est au coeur du questionnement éthique et juridique sous-jacent. Comment interpréter ce nouveau pouvoir d'agir sur le corps humain ? Accroissement de liberté qui requiert d'être réglementé ou autorisation que l'on s'octroie de pro-

387. De Rosnay, *Je cherche à comprendre*, p. 135.
388. Logean Sylvie, *Joël de Rosnay : « L'avenir de l'Humanité réside dans l'intelligence collective augmentée »*, in : Le Temps (https ://www. letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/sciences/joel-rosnay-lavenir-lhumanite-reside-lintelligence-collective-augmentee » (18/04/2017).
389. Fukuyama, *La fin de l'homme*, p. 31 ss et p. 43.
390. Habermas Jürgen, *L'avenir de la nature humaine : vers un eugénisme libéral ?*, 3e éd., Paris 2015, p. 12.
391. *Ibidem.*
392. Millon Louise, *Brainternet : des chercheurs ont lié un cerveau humain à un ordinateur*, in : SiecleDigital (https ://siecledigital.fr/), Lyon 2017, p. « https: / / siecledigital . fr / 2017 / 09 / 28 / brainternet - des - chercheurs - ont - lie - un - cerveau - humain - un - ordinateur/ » (24/03/2020) ; DAPRA, *Six Paths to the Nonsurgical Future of Brain-Machine Interfaces* ; Bostrom, *Superintelligence*, p. 46 (transfert de données entre cerveaux).
393. Habermas, *L'avenir de la nature humaine*, p. 24.
394. *Ibidem.*
395. *Idem*, p. 25.

céder à des transformations préférentielles qui n'exigent aucune auto-limitation [396] ? Pour Habermas, ce n'est qu'en tranchant en faveur de la première question, que la discussion sur les limites de l'eugénisme négatif peut s'engager [397] ?

448 Dans son livre, *L'avenir de la nature humaine*, Jürgen Habermas fait porter sa réflexion sur le défi auquel les récents progrès des biotechnologies confrontent nos conceptions de la liberté et de la responsabilité [398]. Notre nature peut devenir désormais l'objet de manipulations et de programmations, par lesquelles une personne interviendrait intentionnellement en fonction de ses propres préférences sur l'équipement génétique et les dispositions naturelles d'une autre [399]. Ainsi le corps est réduit à un objet dont les organes sont assimilés á des objets imprimables et remplaçables [400].

449 « Avec cette menace d'un effacement de la frontière entre les personnes et les choses risquent également de se trouver remise en cause, estime Jürgen Habermas, la compréhension que nous avons de nous-mêmes comme êtres autonomes et responsables, et par là même les fondements d'une société de sujets libres et égaux [401]». Quelles limites fixer, dans ces conditions, aux interventions génétiques ? Comment garantir la possibilité d'un eugénisme thérapeutique destiné à empêcher l'apparition de maladies graves en évitant la dérive vers un eugénisme libéral, visant l'augmentation ou le design de l'être humain [402] ?

450 Dans son ouvrage intitulé « la fin de l'homme », le philosophe américain Francis Fukuyama, a publié une réflexion sur les conséquences de la révolution bioéthique. Il est parti du postulat que la science, ne peut plus s'autoréguler et prône une législation au ni-

396. Habermas, *L'avenir de la nature humaine*, p. 25.
397. *Ibidem.*
398. *Ibidem.*
399. *Idem*, p. 24 ss.
400. Ginko Bioworks, *ADN et organes de synthèse*, in : Ginko Bioworks (https://www.ginkgobioworks.com/), Boston s.a., p. « https://www.ginkgobioworks.com/ » (05/07/2019) ; Fraga Alberto Iglesias, *This Swedish startup is 3D printing human organs*, in : WEF (https ://www.weforum.org/), Cologny 2018, p. « https://www.weforum.org/agenda/2018/10/this-3d-printer-could-one-day-make-new-body-parts-for-transplant-patients/ » (05/07/2019).
401. Habermas, *L'avenir de la nature humaine*, p. 25.
402. *Idem*, p. 26.

veau international au niveau scientifique [403].

La convergence des biotechnologies, des nanotechnologies, du génie- 451
génétique des sciences cognitives et de la technologie quantique rendent possible l'ingénierie génétique et la modification des caractéristiques intrinsèques de l'être humain [404]. Pour l'avocat, Me Bensoussan, l'enjeu du XXIème siècle sera celui de gérer la convergence entre la biologie, la robotique et l'IA [405]. Les considérations éthiques vont être au premier plan. Cette gestion servira d'autant plus l'intérêt public que les décisions seront prises de manière interdisciplinaire dans le respect de la « communauté politique démocratiquement constituée [406] ».

Le schéma ci-dessous présente le périmètre et les applications les 452
plus connues de l'IA :

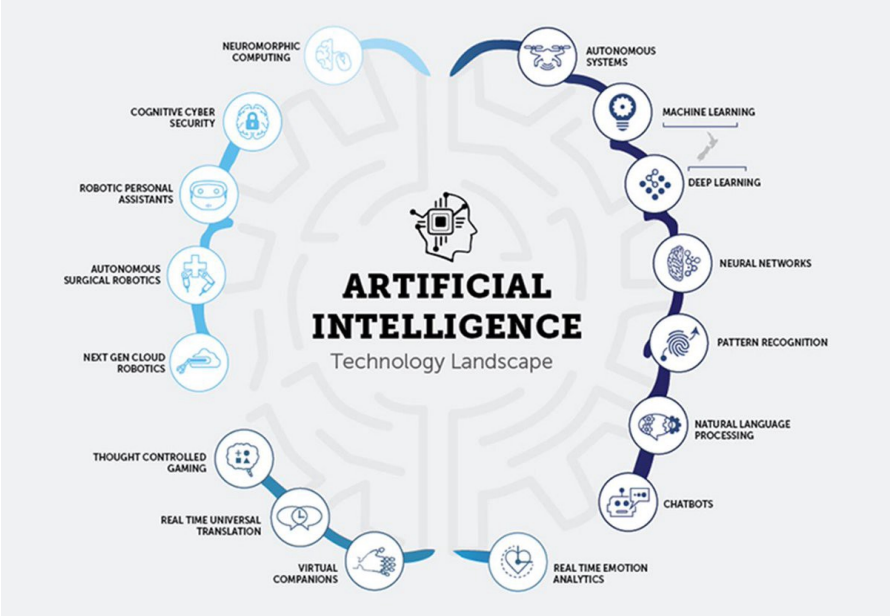

Figure 2.9 – Périmètre et applications les plus connues de l'IA. Source : Medium.com.

Bill Gates, Elon Musk, Georges Church et Stephen Hawking ont 453
publiquement fait connaître leurs préoccupations concernant à la

403. Fukuyama, *La fin de l'homme*, p. 31.
404. *Idem*, p. 136.
405. Présentation de Me Bensoussan, AI Geneva Summit du 22 septembre 2017.
406. Fukuyama, *La fin de l'homme*, p. 323.

fois la rapidité des innovations dans ce domaine et l'impact de ces technologies dans la société.

454 Le rapport du Forum économique mondial, relatif à la gestion des risques, publié en 2017, présente les résultats d'une enquête conduite auprès de 745 leaders issus du secteur économique, politique et académique. Ce rapport a relevé que « l'intelligence artificielle en tant que technologie émergente détenait le plus fort potentiel de conséquences négatives pour la prochaine décennie ».

455 Quels mécanismes de régulation adopter ? Nous proposons avec Elisa Celis et Kirtan Padh, d'effectuer une analogie entre la régulation de l'industrie alimentaire et celle des données sous-jacentes aux algorithmes [407]. Comme l'industrie alimentaire est soumise à des obligations de traçabilité et de transparence à chaque étape du cycle de production et de livraison des denrées alimentaires, à des mécanismes de certification et d'audit, nous proposons de transposer cette réflexion aux données collectées pour le fonctionnement des algorithmes.

456 Cette comparaison pourrait se résumer sous la forme d'une matrice (voir figure 2.10). Celle-ci représente une analogie entre le cycle de la chaîne alimentaire et le développement d'algorithmes transparents. Différentes régulations et codes de conduite applicables à chaque étape du cycle du développement des algorithmes permettraient d'assurer la transparence du mode de fonctionnement des algorithmes.

457 Une présentation détaillée de ce projet a été soumise à la conférence internationale sur l'intelligence artificielle de Melbourne en Australie, au mois d'Août 2017 [408].

458 Il importe que le droit d'accès des individus aux données collectées et traitées par les algorithmes, ainsi que le droit d'en vérifier l'exactitude, de modifier ou de supprimer ces données, soit effectif, ce qu'impose le Règlement européen.

407. Thelisson / Padh / Celis, *Regulatory Mechanisms and Algorithms towards Trust*, p. 3.
408. *Idem*, p. 1.

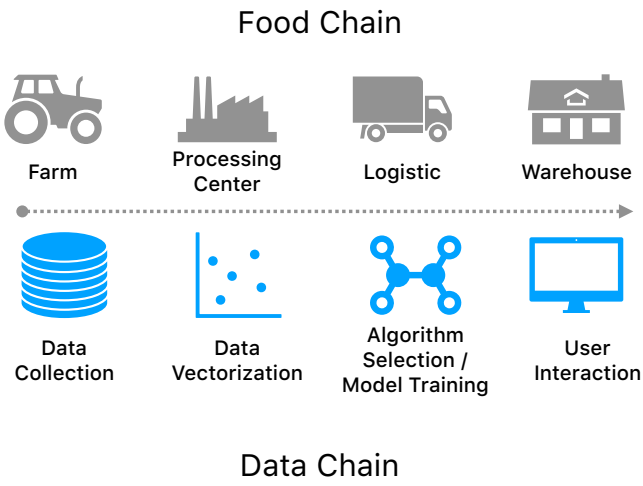

FIGURE 2.10 – Analogie entre le cycle de la chaîne alimentaire et la transparence des algorithmes.

VIII. Les technologies Fintech

L'industrie financière mondiale est actuellement confrontée au défi de repenser son modèle d'affaire. Ceci est dû à l'émergence des technologies digitales et mobiles dans le domaine des paiements et des transferts. 459

Les acteurs traditionnels visent à acquérir de nouvelles parts de marché, à réduire les coûts de transaction, à supprimer les intermédiaires et à accélérer les processus de vente, de paiement, de distribution… Ubiquité, rapidité du service, distribution internationale, sont des éléments clés de ce nouveau modèle d'affaire. 460

A cette fin, l'industrie financière traditionnelle (groupes bancaires, opérateurs de téléphonie, entreprises informatiques) [409] investit dans des innovations de rupture (« disruptive innovation »), par le rachat de start-ups à haute valeur ajoutée (croissance externe). Citons par exemple les applications digitales innovantes dans le domaine du paiement en ligne, et des transferts principalement via un support de téléphonie mobile. Google a investi dans le marché des Fintechs avec le service Google Wallett, qui propose le transfert d'argent à l'aide d'un simple courrier électronique ou le paiement par Smart- 461

409. MCLAUGHLIN Steve, *Weekly Fintech Deal Activity*, in : Financial Trading Partners (http://www.ftpartners.com/), San Francisco 2017, p. « http://www.ftpartners.com/docs/FTPartnersWeeklyDealStats.pdf » (16/04/2017).

phone. Autres innovation, les devises virtuelles (ex. Bitcoins, cryptomonnaies et tokens) et les conseils en ligne pour gérer les investissements financiers. Ces applications présentent la spécificité de supprimer les intermédiaires.

462 L'intelligence artificielle transforment en effet les services financiers. Des « robot-advisors » émergent pour conseiller et gérer le patrimoine des clients à l'aide d'algorithmes, tendant à remplacer progressivement les gestionnaires de fortune traditionnels. En pratique, le client communique ses données personnelles en remplissant tout d'abord un questionnaire en ligne, qui définit son profil de risques. L'algorithme propose en quelques secondes une allocation des actifs. Dans la plupart des cas, l'allocation se fonde sur moins d'une dizaine de portefeuilles standards chacun étant corrélé à un niveau de risque spécifique (conservateur, équilibré, agressif). Ces portefeuilles sont modélisés avec des fonds ETF. A l'avenir, aucun véhicule d'investissement tel que les fonds ou les ETF ne seront plus nécessaires, car toutes les actions pourront être échangées directement par le client, sans intermédiaire. Grâce à ces applications, accessibles depuis les téléphones portables, les tablettes et les ordinateurs, les individus peuvent investir leurs actifs comme des professionnels, dès lors qu'ils satisfont le plancher financier minimum requis.

463 Ces entreprises traditionnelles acquièrent donc des produits et des services qui reposent principalement sur la collecte de données personnelles, leur analyse et des prédictions. Qui a accès à ces données personnelles ? Comment les sécuriser ? Comment la législation sur la protection des données est-elle effectivement respectée ?

464 Le système financier évolue vers une architecture entièrement digitale. Les éléments matériels tendent à disparaître (bureaux,les pièces et les cartes bancaires, les billets sont vouées à disparaître). Elles sont remplacées par des écritures comptables digitalisées, où l'être humain joue un rôle de plus en plus limité, laissant uniquement des traces digitales de ses transactions. Celles-ci sont analysées et vendues à un nombre croissant d'acteurs pour en déduire un profil de comportement et de personnalité, auquel des produits ou des services sont proposés.

465 Les banques traditionnelles modifient leurs processus internes : ainsi aux États-Unis, les banques acceptent d'encaisser des chèques sur la

base d'une simple photo du chèque envoyée par téléphone portable. Apple propose également ce type de service, autorisant le client à s'identifier avec le service TouchID (empreinte digitale), facilitant le paiement par le biais du téléphone portable.

466 Compte tenu de la concentration des données à caractère personnel dans un nombre limité de supports, en premier lieu le smartphone, la question de la sécurité des clouds qui stockent ces données personnelles se pose avec une importance certaine. Ceci d'autant plus que les start-up innovantes n'ont vraisemblablement pas la capacité financière d'investir dans des solutions de sécurité onéreuses offrant toutes les garanties de fiabilité attendues des utilisateurs, comme les banques traditionnelles. Mot de passe, double authentification associée à un SMS, reconnaissance d'empreintes digitales, ou de l'iris, reconnaissance faciale, reconnaissance veineuse (Global ID), les innovations dans le domaine de l'authentification de l'utilisateur sont le corollaire de la collecte massive de données personnelles à sécuriser. Le développement de nouveaux standards techniques offrant des garanties de sécurité et confidentialité des données bénéficie à l'ensemble des acteurs en renforçant la confiance des utilisateurs.

467 Afin de limiter les risques de fraude, la société BOKU a décidé de répercuter les achats effectués par le biais du téléphone portable sur la facture du téléphone portable. En 2017, la plateforme comptait plus de 4 milliards de téléphones portables. Elle est aujourd'hui utilisée sur tous les plus grands marchés numériques tels que Google Play Store, Sony PlayStation Store, Microsoft Windows Store, Facebook App Center et Spotify. Avec son ambition de s'étendre au-delà des biens numériques, Boku veut démocratiser le paiement sur facture par le biais de l'opérateur de téléphonie mobile. Les paiements s'effectuent sans carte et sans banque. En utilisant les fonds que les opérateurs ont déjà intégrés dans chaque téléphone portable (une facture mensuelle pour les abonnements ou du crédit prépayé rechargeable), les commerçants sont dispensés de recueillir les références d'une carte de crédit ou les informations bancaires de leur client pour réaliser leurs ventes. Les clients utilisent uniquement leur numéro de téléphone pour autoriser le paiement. Les commerçants qui choisissent Boku téléchargent l'application et peuvent immédiatement commencer à accepter des paiements depuis tous les téléphones mobiles du monde entier. Cela signifie qu'une fois le numéro de téléphone enregistré, les commerçants peuvent traiter

les paiements en utilisant leur propre processus de paiement, que ce soit pour des paiements ponctuels ou récurrents [410].

468 Dans ce modèle, les opérateurs de téléphonie mobile ont accès à toutes les transactions effectuées par leurs clients, comme les banques autrefois, ce qui pose des problèmes éthiques et juridiques en matière de protection des données. La réglementation bancaire et les règles prudentielles applicables aux établissements bancaires devraient s'appliquer aux opérateurs de téléphonie mobile.

469 Les données transmises lors des paiements par le biais de la téléphonie mobile, donnent des informations sur la personne, sur son comportement, ses habitudes de consommations, sur sa géolocalisation. Ces données à caractère personnel sont collectées, puis analysées avec le soutien d'outils statistiques pour en déduire des liens entre les personnes de son entourage ou encore son mode de vie. Elles sont ensuite traitées dans un but de marketing direct (profilage) ou encore vendues à des tiers.

470 La question de la confiance dans la sécurité des applications et dans la protection des données est centrale pour les infrastructures critiques comme les banques par exemple. Le vol constitue un risque stratégique et systémique [411]. Il peut engendrer un impact négatif en terme d'image et induire une perte de confiance et donc une chute du chiffre d'affaires [412]. La confiance dans les moyens de paiement à distance, et donc la protection des données sous-jacentes est au coeur du développement de l'économie numérique [413]. Comment l'infrastructure informatique est-elle sécurisée ? Les données sont-elles anonymisées de manière irréversibles ? L'authentification forte est elle effectivement mise en oeuvre ? Quelle base légale rend licite le traitement de données ? Autant de questions clefs pour protéger les données et les systèmes d'information d'une organisation et garantir la confiance dans l'économie numérique tout

410. Boku, *Activate and convert more paying users quickly and securely*, in : Boku (https://www.boku.com/), San Francisco s.a., p. « https://www.boku.com/payment-solutions/ » (22/07/2019).
411. Perrin Olivier, *L'anonymisation des informations et l'authentification biométrique pourraient permettre de lutter efficacement contre les vols de données bancaires*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 330.
412. *Idem*, p. 331.
413. *Idem*, p. 331.

en minimisant les risques de réputation [414].

Les start-up offrant des services de paiement par le biais du télé- 471
phone portable ou Peer-to-Peer ont communément recours au standard NFC (« Near Field Communication »). Cette technologie permet à ses utilisateurs d'avoir accès à des objets et des services (par exemple fermer sa maison, ouvrir sa voiture, désactiver l'alarme de son logement, payer dans les commerces avec son téléphone portable). Dans cette configuration, le téléphone portable devient incontournable et la carte SIM joue un rôle central, car elle enregistre toutes les transactions et échange les informations requises pour effectuer le paiement.

En Suisse, l'industrie FinTech est sous la surveillance de la Finma 472
depuis le 30 novembre 2018 [415]. Une autorisation « FinTech », à l'image des licences bancaires, peut désormais être demandée à la FINMA [416]. Les enjeux pour l'innovation sont majeurs [417].

Au niveau européen, la directive (EU) 2015-2366 concernant les 473
services de paiement (dite PSD2) [418] impose de nouvelles obligations aux acteurs traditionnels du secteur des paiements. Ceci est dû au fait que de nouveaux acteurs entrent sur le marché des paiements en proposant des solutions de paiement digital. Cette directive constitue un prolongement de la directive sur les services de paiement adoptée par la Commission européenne en 2007 [419]. Elle vise à renforcer la concurrence afin de proposer un choix élargi aux clients et une transparence accrue.

La directive précise que toute entreprise qui fournit et conserve 474

414. *Idem*, p. 335.
415. Ruche Sébastien, *La surveillance des fintechs entre en vigueur*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https://www.letemps.ch/economie/surveillance-fintechs-entre-vigueur » (28/10/2018).
416. FINMA, *Autorisation Fintech : la FINMA publie un guide pratique*, in : FINMA (https ://www.finma.ch/), Bern 2018, p. « https://www.finma.ch/fr/news/2018/12/20181203-aktuell-fintech-bewilligung/ » (26/07/2019).
417. Van Loo Rory, *Making innovation more competitive : The case of fintech*, in : UCLA Law Review 2018/65, p. 232.
418. Parlement européen et Conseil de l'UE, *Directive (EU) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le Règlement (UE) no. 1093/2010, et abrogeant la directive 2007/64/CE*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2015, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32015L2366 » (09/12/2019).
419. *Idem*, p. 2.

des informations sur des comptes clients doit rendre ces données accessibles à des tiers, notamment à des prestataires de paiement mobile, sous réserve que le client leur en ait donné l'autorisation [420].

475 « Les systèmes fermés de paiement devraient continuer d'être soumis aux règles nationales de l'Union en matière de concurrence, ce qui peut obliger à accorder l'accès à ces systèmes pour maintenir une concurrence effective sur les marchés de paiement [421]». Cette disposition présente des risques majeurs en termes de sécurité. Il semble que ce risque soit identifié, car la directive prévoit un droit de remboursement inconditionnel pour toutes les opérations de prélèvement libellées en Euro dans l'Union [422].

476 Les banques sont ainsi contraintes d'ouvrir à des tiers l'accès aux données des comptes clients via des « interfaces de programmation applicatives » (API). Il est prévisible que la question de la responsabilité en cas de fraudes ou de défaillances, la connaissance du client (KYC) et les contrôles de lutte contre le blanchiment d'argent (AML) gagneront en importance [423].

477 Les activités des fournisseurs tiers (Third Party Providers ou TPP) qui proposent des services de paiement et qui sont souvent des start-ups doivent satisfaire aux exigences de PSD2 comme n'importe quel autre établissement de paiement (agréé enregistré, et contrôlé). Ils sont désormais soumis à des exigences en matière d'information, de transparence et de sécurité des paiements.

§3 Le contexte juridique

478 L'examen des sources internationales et communautaires en matière de protection des données atteste de l'existence de plusieurs normes spécialisées dans ce domaine. Dans la hiérarchie des normes européennes, la protection des données à caractère personnel figure en tant que droit primaire de l'Union (dans le Traité de l'UE, Traité sur le fonctionnement de l'Union européenne (TFUE) et Charte

420. Consid. 52 de la directive PSD2.
421. Consid. 52 de la directive PSD2.
422. Consid. 76 de la directive PSD2.
423. Virdi Tony, *La directive PSD2 provoquera l'un des plus importants bouleversements du secteur bancaire depuis des décennies*, in : Finyear (https://www.finyear.com/), Besançon 2016, p. « https://www.finyear.com/La-directive-PSD2-provoquera-l-un-des-plus-importants-bouleversements-du-secteur-bancaire-depuis-des-decennies_a36367.html » (05/12/2018).

des droits fondamentaux) et en tant que droit dérivé de l'Union (Règlement 2016/679) et textes associés [424]. Le Règlement général sur la protection des données ne constitue pas le premier texte en la matière.

I. Les sources internationales

A. *L'article 17 du Pacte ONU II et la résolution 45/95 des Nations-Unies*

Le Pacte international relatif aux droits civils et politiques conclu à New-York le 16 décembre 1966, est entré en vigueur pour la Suisse le 18 septembre 1992 [425]. Il spécifie que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes [426] ». 479

B. *L'organisation de Coopération et de Développement Économiques (OCDE)*

Les pays de l'OCDE ont pour la plupart adopté des législations sur la protection de la sphère privée (Allemagne, Autriche, Canada, États-Unis, France, Luxembourg, Norvège, Suède, Belgique, Espagne, Suisse). Les pays membres de l'OCDE ont constaté que des disparités dans les législations nationales risquaient de restreindre la libre circulation des données à caractère personnel à travers les frontières. Des restrictions imposées à ces flux pourraient notamment nuire au plan économique. 480

Les pays membres de l'OCDE ont jugé nécessaire d'élaborer des lignes directrices qui permettraient d'harmoniser les législations nationales relatives à la protection de la vie privée et qui, tout en contribuant au maintien des droits de l'homme, empêcheraient que les flux internationaux de données ne subissent des interruptions [427]. Celles-ci sont l'expression d'un consensus sur des principes fondamentaux qui peuvent être intégrés à la législation nationale en vigueur ou servir de base à une législation dans les pays qui ne sont 481

424. Bensoussan, *Règlement européen sur la protection des données (2e éd.)* p. 6.
425. Nivert Nirmal, *Intérêt général et droits fondamentaux*, thèse, Saint-Denis 2012, pp. 1-748.
426. *Idem*, p. 205.
427. *Idem*, p. 205.

pas encore dotés [428].

482 Les lignes directrices, qui revêtent la forme d'une recommandation du conseil de l'OCDE, ont été élaborées par un groupe d'experts gouvernementaux sous la présidence de M. M.D. Kirby, Président de la Commission australienne de la réforme législative. Cette recommandation a été adoptée et a pris effet le 23 septembre 1980.

483 En mai 2019, l'OCDE a également publié les principes directeurs concernant l'intelligence artificielle. Ces principes accordent une place prépondérante aux valeurs et principes démocratiques et à la protection de la sphère privée [429].

C. Les normes « ISO »

484 L'organisation internationale de normalisation (ISO) est une organisation internationale non gouvernementale, dont les 162 membres sont les organismes nationaux de normalisation [430]. L'ISO réunit des experts qui mettent en commun leurs connaissances pour élaborer des normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux [431].

485 Les normes internationales établissent des spécifications de premier ordre pour les produits, les services et les systèmes dans une optique de qualité, de sécurité et d'efficacité. Elles jouent un rôle prépondérant pour faciliter le commerce international. L'ISO a publié plus de 21 580 normes internationales et publications associées qui couvrent la quasi-totalité des secteurs de l'industrie [432].

486 L'ISO élabore des normes internationales, mais ne fournit pas de services de certification selon ces normes, et ne délivre pas de certificats. Ces services sont assurés par des organismes de certification externes. Une certification est une assurance écrite (sous la

428. OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, in : OCDE (https ://www.oecd.org/), Paris s.a., p. « https : / / bit . ly / 2MJ8nPH » (17/04/2017).
429. OECD, *OECD Principles on AI*, in : OECD (https ://www.oecd.org/), Paris s.a., p. « https://www.oecd.org/going-digital/ai/principles/ » (08/06/2019).
430. ISO, *À Propos de L'ISO*, in : ISO (https ://www.iso.org/), Genève s.a., p. « https: //www.iso.org/fr/about-us.html » (18/04/2017).
431. *Ibidem.*
432. *Ibidem.*

forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques. Par conséquent, une entreprise ou une organisation ne peut pas être certifiée par l'ISO [433].

La famille de normes ISO 27000 aide les organisations à assurer la sécurité de leurs informations. 487

Ces normes faciliteront le management de la sécurité des informations, notamment les données qui sont confiées à des organisations par des tiers. ISO/IEC 27001, qui expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI), est la norme la plus célèbre de cette famille. Il existe plus d'une douzaine de normes dans la famille ISO/IEC 27000. 488

En 2014, l'ISO a adopté une nouvelle norme « ISO/IEC 27018 :2014 », spécifique à la protection des données personnelles dans le Cloud. Il s'agit d'une nouvelle norme qui pose un cadre concernant le respect par le prestataire de service de Cloud d'un certain nombre de mesures concernant les données personnelles qui transitent par leurs Clouds. La norme ISO 27018 s'inscrit dans le prolongement des normes existantes en matière de sécurité de l'information, telles que les normes ISO 27001 et ISO 27002 qui permettent d'identifier les risques de sécurité inhérents aux systèmes d'information et de mettre en œuvre les contrôles nécessaires pour les éviter. La norme ISO 27018 est quant à elle spécifiquement adaptée aux services de Cloud et constitue la première norme internationale spécifique à la protection des données personnelles pour le Cloud. Elle augmente ainsi le nombre de contrôles prévus déjà par la Norme ISO 27002, constituant ainsi l'« état de l'art » en la matière. Les prestataires qui la respectent apportent des garanties à leurs clients et renforce la confiance de ces derniers. La conformité à cette norme constitue donc un avantage concurrentiel. 489

Les autorités de contrôle de l'Union Européenne réclamaient l'introduction d'un cadre normatif permettant de contrôler les engagements pris par les sous-traitants. Cette norme ISO/IEC 27018 :2014 répond directement à cette demande. L'objectif est de renforcer la confiance des utilisateurs dans le cadre de l'utilisation de solutions 490

433. Le comité pour l'évaluation de la conformité (CASCO) a produit un certain nombre de normes qui se rapportent au processus de certification, à l'usage des organismes de certification.

Cloud [434].

491 La norme ISO 27018 pose les principes suivants :

— *Consentement* : la norme 27018 pose le principe de l'interdiction du traitement des données personnelles des clients par les prestataires de services Cloud à des fins publicitaires et marketing [435]. Le traitement est uniquement autorisé si le consentement exprès et préalable du client a été recueilli par le prestataire de services Cloud. Ce consentement ne saurait conditionner la prestation de services.

— *Transparence* : les prestataires de services Cloud doivent informer les clients du lieu de stockage des données qui transitent par le Cloud ainsi que sur l'identité des éventuels sous-traitants appelés à traiter les données lors de la conclusion du contrat de Cloud ; ils s'engagent également à prendre des engagements clairs sur la manière dont les données sont traitées.

— *Communication* : les prestataires de services Cloud s'engagent, en cas de failles de sécurité affectant les données, à en informer le client et les autorités et à aider les utilisateurs à se conformer à leurs propres obligations d'information ; ils s'engagent également à ne pas divulguer d'informations aux autorités nationales sauf lorsqu'ils y sont tenus par la réglementation applicable et, dans ce cas, à en informer le client, sauf interdiction légale.

— *Portabilité/destruction des données* : les prestataires de services Cloud s'engagent à mettre en œuvre une politique en matière de transfert ou de destruction des données personnelles à l'issue du contrat.

— *Conformité* : Un auditeur peut contrôler et certifier la conformité à la norme ISO 27018 du prestataire de services, ce qui permet au client de vérifier la conformité du traitement des données personnelles à la réglementation en vigueur.

434. Commission Européenne, *Libérer tout le potentiel de l'informatique en nuage en Europe – qu'en est-il en pratique ?*, in : Commission Européenne (https ://ec.europa.eu/), Bruxelles 2012, p. « http://europa.eu/rapid/press-release_MEMO-12-713_fr.htm?locale=FR » (18/04/2017).

435. Ce principe d'interdiction fait écho à celui du Règlement, à l'art. 6, al.1, consid. 1 ; Härting, *Datenschutz-Grundverordnung*, p. 81.

— *Confidentialité des données* : du fait du principe de confidentialité des données, les prestataires de Cloud s'engagent à conclure des accords de confidentialité avec les membres du personnel qui ont accès aux données personnelles et à leur fournir toute formation requise.

La nouvelle norme ISO 27018 constitue un avantage concurrentiel en termes de sécurité et de confidentialité des données personnelles dans le domaine du Cloud. 492

D. Le projet d'une norme mondiale contraignante

Lors de la 31ème conférence internationale des commissaires à la protection des données, le 3 novembre 2009, une déclaration commune a été adoptée à Madrid. Elle réaffirme l'adhésion à un cadre mondial pour des pratiques loyales de traitement des données (ch. 1) et la création d'un nouveau cadre international pour la protection de la vie privée (ch. 10) [436]. 493

La déclaration du 3 novembre 2009 se fonde sur différents principes communs : la transparence, la responsabilité, les droits à l'accès à l'information, droits à l'information, à la rectification. 494

Les commissaires à la protection des données, la société civile et les représentants de l'industrie ont adhéré à cette déclaration. 495

Pour Jean-Philippe Walter [437], Préposé fédéral suisse suppléant à la protection des données, il s'agit d'une « décision de taille car nous sommes parvenus à trouver des dénominateurs communs entre différents continents. Mais nous n'en sommes pas encore à l'idée d'une autorité internationale de protection des données, ce que je souhaiterais ». 496

Le Président de la Commission nationale de l'informatique et des libertés de l'époque, en France, et Président du groupe de travail des autorités européennes de protection des données à l'époque, Alex Türk, a indiqué que : « tout le monde a enfin compris la nécessité de trouver une norme commune, certains pour des raisons éthiques 497

436. The Public Voice, *Standards mondiaux de respect de la vie privée dans un monde globalisé : Déclaration de la société civile Madrid, Espagne 3 novembre 2009*, in : The Public Voice (https ://thepublicvoice.org/), s.l. 2009, p. « http://thepublicvoice.org/madrid-declaration/fr/ » (29/05/2017).

437. Lombarte Artemi Rallo, *Vers une régulation globale du droit à la vie privée : propositions et stratégies*, in : 31ème conférence internationale des commissaires à la protection des données et à la vie privée, Madrid 2009.

et d'autres parce qu'ils pensent qu'il n'y a pas de développement économique sans confiance [438]».

498 Cette résolution a été soutenue par une dizaine de multinationales (Microsoft, Google, IBM, Walt Disney...). Ces entreprises ont en effet du mal « à s'adapter aux normes différentes de chaque pays ou marché [439]». Cette incertitude est source de risques qu'elles souhaitent minimiser.

499 Pour Alex Türk, « la prochaine étape sera celle de la valeur juridique contraignante [440]». Pour parvenir à une norme juridique contraignante sur le plan mondial, les différences de visions en matière de protection des données entre les États-Unis et l'Union européenne devront être surmontées. Les États-Unis ne disposent pas d'autorité de protection des données, ils privilégient l'autorégulation des acteurs économiques et privilégient une approche plus sectorielle qu'en Europe.

500 Le Règlement, octroie une valeur juridique contraignante à la protection des données au sein de l'UE. Il s'agit en cela d'une avancée majeure vers l'élaboration d'une norme mondiale contraignante.

II. Les sources communautaires

501 Pour des raisons économiques, la Règlementation juridique en matière de protection des données n'a pas été une priorité en Europe.

A. La charte des droits fondamentaux de l'Union européenne

502 Elle dispose dans son article 8, al. 1, que toute personne a droit à la protection des données à caractère personnel la concernant. Selon l'article 16, al. 2, du traité sur le fonctionnement de l'UE, le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives, à la protection des personnes physiques, à l'égard du traitement des données à caractère personnel, par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union et à la libre

438. Demon Valérie, *Vers une norme internationale de protection de la vie privée*, in : La Croix (https ://www.la-croix.com/), Madrid 2009, p. « https://www.la-croix.com/Monde/Vers-une-norme-internationale-de-protection-de-la-vie-privee-2009-11-16-568829 » (24/03/2020).
439. Lombarte, *Vers une régulation globale du droit à la vie privée.*
440. *Ibidem.*

circulation de ces données. L'objectif du Règlement est donc de traduire, dans la pratique, les règles et les exigences qui découlent de ce droit de la protection des données.

Le Règlement précise dans ses premiers considérants que le droit à la protection des données « n'est pas un droit absolu » et qu'il doit être envisagé en relation avec sa fonction sociale et mis en balance avec les autres droits fondamentaux [441]. Le traitement des données à caractère personnel constitue en effet le fondement de la plupart des activités économiques dans une économie de l'information. Règlementer les traitements de données ne peut donc se faire par voie d'interdiction générale et abstraite, mais bien dans le respect du principe de proportionnalité [442]. 503

B. L'article 8 de la Convention européenne des droits de l'homme

La Convention européenne des droits de l'homme (ci-après « CEDH ») est venue la première combler la lacune existant au niveau européen en matière de protection des données à caractère personnel. 504

L'article 8 de la CEDH prévoit la protection de la vie privée et familiale. Il protège également le droit à la protection des données à caractère personnel. Ainsi au niveau du droit international, c'est via le respect de la vie privée et familiale garanti par l'article 8 CEDH, que la Cour européenne des droits de l'homme a assuré la protection des données à caractère personnel, dans la mesure où celle-ci constitue un élément important de la vie privée. 505

Pour chacun des droits qu'elle garantit, la Cour prévoit des conditions spécifiques pour la limitation de ces droits. 506

Ainsi par exemple, l'article 8 de la CEDH garantit, en son paragraphe 1er, le droit de chacun au respect de sa vie privée et familiale, de son domicile, et de sa correspondance, et prévoit les conditions de son éventuelle limitation au paragraphe 2 : « il ne peut y avoir ingérence d'une autorité publique, dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi, et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des 507

441. Consid. 4 RGPD.
442. Consid. 4 et art. 5 et 6 RGPD.

infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits de l'homme et des libertés d'autrui [443]».

508 Dans son arrêt « Amann c. Suisse » [444], la CEDH précise que la vie professionnelle d'une personne physique peut être dans certains cas protégée par les dispositions de l'article 8 CEDH sur le droit à la vie privée. Elle fait référence à la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, indiquant qu'elle entend protéger « toute information concernant une personne physique identifiée ou identifiable ». Cette notion d'« information concernant une personne physique identifiée ou identifiable » « comprend aussi les données de nature publique lorsqu'elles sont recueillies de façon systématique, et mémorisées dans des fichiers par les pouvoirs publics, et ce, d'autant plus lorsqu'il s'agit de données sur le passé lointain d'une personne [445]».

C. La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après « Conv.108 »)

509 Dans le cadre du système juridique du Conseil de l'Europe, il existe des textes spécifiques dans le domaine de la protection des données.

510 Face à la nécessité de protéger les individus d'un traitement abusif et déloyal de leurs données, le Conseil de l'Europe a élaboré un cadre de principes et de normes spécifiques.

D. La Cour de Justice de l'Union Européenne (ci-après « CJUE »)

511 Elle propose une interprétation large de la notion de donnée personnelle. Il s'agit de « toute information concernant une personne

443. Bamdé Aurélien, *Les sources du droit de la protection des données à caractère personnel*, in : A. Bamdé & J. Bourdoiseau (https ://aurelienbamde.com/), s.l. 2018, p. « https://aurelienbamde.com/2018/11/15/les-sources-du-droit-de-la-protection-des-donnees-a-caractere-personnel/ » (21/05/2019).

444. Arrêt CourEDH du 16 février 2000, *Amann contre Suisse*, requête n°27 798/95, consid. 65, ECLI :CE :ECHR :2000 :0216JUD002779895.

445. Arrêt CourEDH du 4 mai 2000, *Rotaru contre Roumanie*, requête n° 28 341/95.

physique identifiée ou identifiable [446]».

Dans un arrêt, la CJUE a précisé que « peu importe que la donnée contienne une information relevant de la vie privée des personnes ou non, dès lors qu'une personne physique est directement ou indirectement identifiée ou identifiable dans une donnée, celle-ci est automatiquement qualifiée de donnée personnelle [447]». 512

La notion de donnée personnelle « n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci « concernent » la personne en cause [448]». 513

La CJUE inclut dans les données personnelles : les registres du temps de travail [449], les adresses IP [450], les images de personnes enregistrées dans le cadre d'un dispositif de vidéosurveillance [451] et les métadonnées de communications [452]. 514

(a) Les éléments historiques

Dans les années 1970, le Comité des ministres a adopté deux importantes résolutions. Si elles n'ont pas de valeur contraignante, elles sont cependant adressées aux États membres. Ceux-ci devant se conformer aux principes établis par le Conseil de l'Europe, elles ne sont pas sans effets. En 1973, le Comité des ministres a adopté la résolution (73) 22, relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques 515

446. CJCE 6 novembre 2003, *Lindqvist*, C—101/01, consid. 24.
447. Arrêt CJUE du 16 juillet 2015, *ClientEarth contre EFSA*, C—615/13P, JOUE 21 septembre 2015, C-311/5, consid. 24, 29 et 30.
448. Arrêt CJUE du 20 décembre 2017, *Peter Nowak contre Data Protection Commissioner*, C—434/16, JOUE 26 février 2018, p. C-72/20, ECLI :EU :C :2017 :994, consid. 34.
449. Arrêt CJUE du 30 mai 2013, *Worten contre ACT*, C—342/12, ECLI :EU :C :2013 :355, consid. 46.
450. Arrêt CJUE du 24 novembre 2011, *Scarlet c. SABAM*, C-70/10, Rec. 2011, p. I-11959, ECLI :EU :C :2011 :771 et ECLI :EU :C :2011 :255, respectivement consid. 51 et 78.
451. Arrêt CJUE 11 décembre 2013, *Frantisek Rynes*, C—212/13, JOUE 9 février 2013, p. C 46/6, consid. 21.
452. Arrêt CJUE du 21 décembre 2016, *Tele2 Sverige*, C—203/15 et C-698/15, JOUE 20 fevrier 2017, p. C 53/11, consid. 97-100.

dans le secteur privé [453].

516 Cette résolution énonce une série de principes pour la protection de la confidentialité des informations à caractère personnel enregistrées et traitées dans les banques de données électroniques du secteur privé. Parmi ces principes, figure la qualité des informations enregistrées, la finalité des informations, la durée de la période de conservation et l'information de la personne concernée.

517 Des principes furent ensuite développés pour les banques de données électroniques dans le secteur public. Ainsi en 1974, le Conseil de l'Europe a adopté la Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données dans le secteur public [454].

518 Cette résolution était nécessaire au vu de l'entraide administrative impliquant l'échange d'informations entre les États européens, tant en vertu d'accords bilatéraux (ex : conventions bilatérales en matière fiscale), que sur la base des conventions européennes. Le but de cette résolution était à la fois d'instaurer des règles communes à l'ensemble des États européens et de contribuer à la compréhension et à la confiance du public dans l'échange de renseignements entre administrations. La résolution adoptée en 1974 énonce donc les principes de protection des données et leur application à l'égard des banques de données électroniques dans le secteur public.

519 Avec ces deux résolutions, le Conseil de l'Europe a défini les principes de la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs privés et public [455].

453. Conseil de l'Europe, *Resolution (73)22 du 26 septembre 1973 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 1973, p. « https://rm.coe.int/native/090000168050329b » (28/10/2018).

454. Conseil de l'Europe, *Resolution (74)29 du 20 septembre 1974 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 1974, p. « https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804cd7a9 » (31/05/2017).

455. Conseil de l'Europe, *Convention 108 + : Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 2018, p. «https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726 » (21/05/2019).

(b) L'adoption de la Convention 108

Par la suite, la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel [456], que l'on nomme Convention 108, a été conclue. Elle a été adoptée le 28 janvier 1981 par le Conseil de l'Europe, qui voulait ainsi protéger la vie privée des citoyens en cas de traitement de leurs données à caractère personnel au moyen des nouveaux systèmes d'information et de communication. 520

L'adoption de cette convention constitue une étape essentielle dans le domaine de la protection des données en Europe. La convention dispose en effet d'une valeur juridique contraignante. Elle conserve aujourd'hui encore toute sa pertinence. Elle doit en effet être appliquée à des domaines extérieurs au système juridique européen (sûreté de l'État, droit pénal…) [457]. 521

Le but de la Conv. 108 est de garantir, sur le territoire de chaque Partie, à toute personne physique, indépendamment de sa nationalité ou de sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »). 522

(c) Les obligations des États signataires

Selon cette Convention, chaque État partie à la Convention s'engage à prendre les mesures nécessaires en droit interne pour donner effet aux principes de base pour la protection des données énoncés dans la Convention. Les États doivent s'assurer en particulier que les données à caractère personnel sont : 523

- obtenues et traitées loyalement et licitement ;
- enregistrées pour des finalités déterminées et légitimes ;
- ne sont pas utilisées de manière incompatible avec ces finalités ;

456. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel STE n°108, ratifiée actuellement par les pays membres du Conseil de l'Europe, sauf la Russie, Saint-Marin, la Turquie et l'Arménie : *Ibidem.*

457. Autorité de protection des données, *Conseil de l'Europe*, in : APD (https://www.autoriteprotectiondonnees.be/), Bruxelles s.a., p.« https://www.autoriteprotectiondonnees.be/conseil-de-l-europe » (24/03/2020).

— adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;

— exactes et si nécessaire mises à jour ; et

— conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (art. 5).

(d) Les données sensibles

524 La Conv. 108 prévoit une catégorie particulière de données. Il s'agit des données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle. Le Règlement reprend cette catégorie, car il s'inspire du Règlement.

525 Ces données ne peuvent pas être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées [458]. Il en est de même des données à caractère personnel concernant des condamnations pénales.

526 Un test de proportionnalité [459] doit systématiquement être effectué entre « le droit à la protection de la sphère privée d'une part, et l'intérêt général poursuivi par l'ingérence ainsi que les modalités de cette ingérence d'autre part [460] ».

527 Selon ce test de proportionnalité, la CEDH vérifie si un État offre des « garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de

458. Cette obligation est imposée par la CEDH « La législation interne doit ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans l'article 8 CEDH » ; Arrêt CourEDH du 4 décembre 2008, *S. et Marper contre Royaume-Uni*, requête n° 30 562/04 et 30 566/04, consid. 103, ECLI :CE :ECHR :2008 :1204JUD003056204.

459. CourEDH du 26 mars 1987, *Leander contre Suède* Requête n° 9248/81, ECLI :CE :ECHR :1987 :0326JUD000924881 ; CEDH 4 décembre 2008, *S. et Marper contre Royaume-Uni*, Requête n° 30 562/04 et 30 566/04., ECLI :CE :ECHR :2008 :1204JUD003056204.

460. CourEDH 16 février 2000, *Amann contre Suisse* Req. 27 798/95, consid. 69 ; Rossi Julien, *Guide de la jurisprudence européenne en matière de protection des données à caractère personnel*, in : Cahiers Costech 2017 58/1, pp. 1-80.

la défendre [461]».

Le test de proportionnalité de la CJUE est inspiré de l'article 52 paragraphe 1 de la Charte des droits fondamentaux de l'UE et de la jurisprudence de la CJUE du 8 avril 2014 « Digital Rights Ireland [462]». Selon cette jurisprudence, les mesures prises ne doivent pas « dépasser les limites de ce qui est nécessaire et approprié à la réalisation de la finalité des limitations au droit à la vie privée et à la protection des données». 528

(e) La sécurité

Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés. 529

(f) Les garanties

La Cour européenne des droits de l'homme comme la Cour de justice de l'union européenne considèrent que toute collecte de données personnelles constitue une forme d'ingérence dans la sphère privée des individus et doit par conséquent non seulement être légitime (d'où les principes de licéité et de loyauté des traitements), mais aussi être proportionnelle à la finalité légitime recherchée. 530

Cette approche justifie aussi le principe de limitation des traitements (minimisation de la collecte et limitation de la durée de conservation). La directive 95/46/CE prévoyait déjà des garanties similaires (art. 6, al 1. let. e)). 531

Le Règlement formalise cette approche et offre des garanties [463] à la personne concernée. Celle-ci doit pouvoir : 532

— connaître l'existence et avoir accès à un fichier automatisé de données à caractère personnel (art. 15 RGPD), connaître ses

461. Arrêt CourEDH du 26 mars 1987, *Leander contre Suède*, requête n° 9248/81, consid. 60 ; Arrêt CourEDH du 2 août 1984, *Malone contre Royaume-Uni*, requête n° 8691/79, consid. 79 ; Arrêt CourEDH du 12 janvier 2016, *Szabó and Vissy contre Hongrie*, requête n° 37 138/14, consid. 73 ; et Arrêt CourEDH du 4 décembre 2015, *Roman Zakharov contre Russie*, requête n° 47 143/06, consid. 284.
462. C-293/12 et C-594/12 consid. 38-46.
463. Voir point 525.

finalités principales (Artr. 5 RGPD), ainsi que l'identité ou le principal établissement du responsable du traitement ;

— obtenir la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible (sans délai ou frais excessifs) (art. 15 RGPD) ;

— obtenir au besoin la rectification (art. 16 RGPD) de ces données ou leur effacement (art. 17 RGPD) ; et

— disposer d'un recours (art. 77 RGPD) [464].

(g) Les dérogations

533 La Conv. 108 prévoit des dérogations lorsque celles-ci constituent une mesure nécessaire dans une société démocratique :

— à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ; et

— à la protection de la personne concernée et des droits et libertés d'autrui.

534 Des restrictions à l'exercice des droits peuvent être prévues par la loi pour les fichiers automatisés de données à caractère personnel utilisés à des fins de statistiques ou de recherches scientifiques, lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées.

(h) Les sanctions

535 Chaque État partie à la Conv. 108 s'engage à établir des sanctions et des recours appropriés en droit interne.

536 En matière de flux transfrontaliers des données personnelles, le principe consiste à interdire à chaque État partie de soumettre à une autorisation spéciale les flux transfrontaliers de données à caractère personnel à destination du territoire d'une autre Partie. Des dérogations sont possibles dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données

464. En cohérence avec les art. 6 et 13 CEDH.

à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente ; des dérogations sont également prévues lorsque le transfert est effectué à partir de son territoire vers le territoire d'un État non contractant par l'intermédiaire du territoire d'un autre État Partie à la Convention, afin d'éviter que de tels transferts n'aboutissent à contourner la législation du premier État Partie.

Cet instrument juridique international constitue le texte de référence du RGPD. Il s'agit du premier et du seul texte international régissant la protection des données ayant un caractère contraignant. La Conv. 108 énonce les principes de base de la protection des données qui sont universellement reconnus et cohérents avec d'autres textes comme par exemple les lignes directrices de l'OCDE ou les principes directeurs des Nations Unies. La Convention est technologiquement neutre. Elle s'applique à l'ensemble des traitements de données automatisées du secteur privé et du secteur public, y compris dans le domaine de la police et de la justice. Elle garantit un haut niveau de protection dans le respect des systèmes juridiques existants et assurer en principe la libre circulation des données entre les États parties. Elle concilie le droit au respect de la vie privée et la liberté d'information (notamment le droit à la libre circulation des données sans considération de frontières). La Convention règle la coopération entre les Parties et l'assistance aux personnes concernées indépendamment de leur nationalité ou leur lieu de résidence. Elle met en place une plateforme de coopération multilatérale par le biais du Comité consultatif. La Conv. 108 a été élaborée avec la participation d'États non membres du Conseil de l'Europe (USA, Canada, Australie, Japon), et n'est donc pas un texte purement européen. Elle est ouverte à l'adhésion d'États tiers, ce qui lui donne un potentiel universel [465]. 537

Contrairement au Règlement, la Conv. 108 nécessite d'être ratifiée par les États pour être applicable. Après sa ratification, elle a une valeur juridique contraignante. 538

Le projet de révision total de la loi sur la protection des données 539

465. Walter Jean-Philippe, *Modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*, in : International Conference on Modernisation of Data Protection Legislation in Europe, Skopje 2012, pp. 1-15.

adopté par le Conseil fédéral le 15 septembre 2017 vise à permettre à la Suisse de signer aussi tôt que possible la nouvelle version de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [466].

540 En Suisse, les normes du droit international sont d'application directe [467]. Dans l'arrêt 105 II 49, 57s., le Tribunal fédéral a considéré qu'un traité international approuvé par l'Assemblée fédérale était contraignant pour la Suisse et faisait partie intégrante du droit suisse dès l'échange des instruments de ratification. Dès ce moment, a-t-il souligné, les normes du traité, lorsqu'elles sont directement applicables, c'est-à-dire suffisamment précises et claires pour pouvoir fonder une décision dans le cas d'espèce, s'imposent non seulement aux autorités, mais aussi aux particuliers [468].

541 En application de cette jurisprudence et contrairement à d'autres États, comme la France, d'inspiration dualiste, la Suisse n'a pas besoin de transposer les traités internationaux en droit interne.

542 Pour les États dualistes, il ressort de la responsabilité de chaque État partie de prendre les mesures nécessaires pour donner effet aux dispositions de la Convention, au plus tard, au moment de l'entrée en vigueur de la Convention. En l'absence d'un système de contrôle et d'évaluation de l'effectivité des mesures prises, la protection des données repose sur la bonne foi et la confiance entre États Parties.

E. Le protocole additionnel à la Convention 108

543 Le Conseil de l'Europe et le Comité Consultatif de la Conv. 108 ont élaboré en 2014 un protocole additionnel à la Conv. 108. Ce protocole a pour but de renforcer le droit à la protection des données en tant que droit fondamental indispensable à l'exercice d'autres droits de l'homme et libertés fondamentales lors du traitement de données à caractère personnel, en tenant compte de la globalisation et de l'essor des technologies de l'information et des télécommunications. Le protocole vise une meilleure maîtrise des données à ca-

466. Conseil fédéral, *Une meilleure protection des données et un renforcement de l'économie suisse*, in : Le Conseil fédéral (https ://www.admin.ch/), Berne 2017, p. « https : / / www . admin . ch / gov / fr / accueil / documentation / communiques.msg-id-68130.html » (24/03/2020).
467. ATF 105 II 49 du 25 janvier 1979, consid. 57s.
468. ATF 105 II 49 du 25 janvier 1979, consid. 57s.

ractère personnel pour les personnes concernées et entend garantir le respect de la dignité humaine lors du traitement de données personnelles.

Le protocole additionnel concilie également le droit à la protection des données avec l'exercice d'autres droits de l'homme et libertés fondamentales, en particulier avec la liberté d'expression. Le droit à la protection des données n'est pas considéré comme une prérogative absolue. Il doit être analysé par rapport à sa fonction dans la société. Conformément au principe de proportionnalité, ce droit ne doit pas être exercé de manière à empêcher l'exercice d'autres droits de l'homme et libertés fondamentales. Il s'agit de concilier les différents droits et libertés en présence. 544

Afin de renforcer l'effectivité des droits des personnes concernées, le protocole additionnel renforce les mécanismes de mise en œuvre et de suivi de la convention et maintient le principe de neutralité technologique des dispositions de la convention. Le protocole exige un niveau de protection adéquat pour le transfert auprès des pays non parties à la convention. Il s'inscrit en cohérence avec le cadre juridique de l'Union européenne et renforce la vocation universelle et le caractère ouvert de la Conv. 108 [469]. 545

Le champ d'application de la Conv. 108 est étendu à l'ensemble des traitements automatisés ou non automatisés de données personnelles qui relèvent de la juridiction d'une partie. 546

Il continue de couvrir les traitements dans les secteurs privés et publics, y compris la police et la justice. Il intègre ainsi les traitements manuels, dans la mesure où les données font partie d'un ensemble dont la structure permet selon des critères déterminés de rechercher les données par personne concernée. 547

L'expression « relevant de sa juridiction » permet de couvrir également les traitements découlant d'activités et de services destinés à des personnes relevant de la juridiction d'une Partie, et aux traitements découlant de l'observation du comportement des personnes concernées, lorsque ces traitements sont opérés par des respon- 548

469. Conseil de l'Europe, *Modernisation de la « Convention n° 108 » sur la protection des données*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 2013, p. « https://www.coe.int/fr/web/portal/28-january-data-protection-day-factsheet » (20/10/2017).

sables du traitement ne relevant pas de la juridiction d'une Partie.

549 Quant aux définitions, elles ont été modifiées. Ainsi une personne n'est pas identifiable si cette identification nécessite des délais ou des activités déraisonnables pour le responsable du traitement ou pour toute personne auprès de qui le responsable du traitement pourrait raisonnablement obtenir l'identification. Par « identifiable », on ne se réfère pas seulement aux éléments de l'identité civile d'un individu, mais aussi à ce qui permet d'individualiser une personne parmi d'autres.

550 En outre, la notion de fichier est abandonnée. Celle de maître du fichier est remplacée par la notion de responsable de traitement, laquelle est complétée par les notions de sous-traitant et de destinataire des données. Ces définitions ont été intégralement reprises par le Règlement général sur la protection des données.

551 La proposition finale du protocole additionnel portant révision de la Convention a été rédigée en 2016 en cohérence avec le nouveau Règlement et la directive de l'UE concernant la protection des données.

552 Le protocole réaffirme au niveau des principes les dispositions conventionnelles appelées à être complétées, par des textes sectoriels plus détaillés sous forme de recommandations ou de directives [470].

553 Il vise à assurer la cohérence et la compatibilité avec le cadre juridique de l'UE, conserve le principe de neutralité technologique et réaffirme la vocation de la Convention à constituer une norme universelle [471].

554 Les principales innovations portent sur les points suivants :

- principe de proportionnalité (implicite jusqu'ici et concernant uniquement les données), notamment principe de minimisation des données ;
- obligation de rendre des comptes, en particulier pour les contrôleurs des données et les responsables de leur traitement ;
- respect de la vie privée ;
- obligation de déclarer les violations de données ;

470. Conseil de l'Europe, *Modernisation de la « Convention n° 108 »*.
471. *Ibidem*.

— transparence du traitement des données ; et

— garanties complémentaires pour la personne intéressée comme le droit de ne pas faire l'objet d'une décision fondée seulement sur un traitement automatisé sans que son avis soit pris en considération, le droit de connaître la logique sous-tendant le traitement et le droit de le contester [472].

Le protocole révisé impose toujours « un niveau de protection adéquat » si les données sont communiquées ou divulguées à des destinataires qui ne relèvent pas de la juridiction d'une Partie à la Convention. 555

La signature du protocole d'amendement de la convention STE 108 constituera un critère central pour l'Union européenne lorsqu'elle aura à décider du maintien de la décision d'adéquation en faveur de la Suisse, qui elle seule peut lui garantir le libre accès au marché européen [473]. Que ce soit pour des raisons tenant à la protection des droits de l'homme ou pour des raisons économiques (faciliter les flux transfrontaliers), la Suisse a intérêt à ratifier rapidement le protocole d'amendement à la convention STE 108 [474]. 556

F. La directive européenne sur la protection des données 95/46/CE

Conçue à une époque antérieure à celle des réseaux sociaux, du Big Data et de l'internet des objets, la directive européenne 95/46/CE, ne répond plus aux exigences du présent et de l'avenir immédiat. 557

Le législateur a constaté l'ampleur sans cesse croissante des collectes et des échanges massifs de données, et reconnu que l'évolution technique et la mondialisation créent « de nouveaux enjeux pour la protection des données à caractère personnel [475] ». Le Règlement évoque à cet égard, les capacités d'utilisation sans précédent des données par les entreprises comme par les autorités publiques, les profondes transformations économiques et sociales provoquées par les technologies et le fait que les individus eux-mêmes partagent publiquement et au niveau mondial des informations les 558

472. *Ibidem.*
473. Message du 15 septembre 2017, concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (17.059), FF 2017 p. 6565 ss.
474. *Ibidem.*
475. Consid. 6 RGPD.

concernant [476].

559 La directive cadre 95/46/CE du 24 octobre 1995 [477] sur la protection des données personnelles et de la vie privée compose un espace global, complété par un espace sectoriel prévu dans une directive propre au secteur des télécommunications électroniques, dont la réforme la plus récente date de 2009 [478]. Le niveau de fragmentation des législations nationales, en dépit des efforts d'harmonisation depuis l'adoption de la directive 95/46/CE, constitue également un obstacle au bon fonctionnement du marché intérieur et au besoin de sécurité juridique des acteurs [479]. Le Règlement tend assurer un niveau cohérent et élevé de protection des personnes physiques et à lever les obstacles aux flux de données au sein de l'Union, conformément au mandat du Parlement européen, qui résulte de l'article 16, al. 2 du traité sur le fonctionnement de l'Union [480]. En application de l'article 288 TFUE, le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable

476. Commission européenne, *« Une approche globale de la protection des données à caractère personnel dans l'UE » (COM(2010) 609/3)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2010, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2010/FR/COM-2010-609-6-FR-MAIN-PART-1.PDF » (09/12/2019), p. 2.

477. Parlement européen et Conseil de l'UE, *Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 1995, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046 » (04/07/2017), pp. 31-50.

478. Commission européenne, *Directive 2002/77/CE du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2002, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32002L0077 » (04/07/2017), pp. 21–26.

479. Epiney Astrid / Kern Markus, *Zu den Neuerungen im Datenschutzrecht der Europäischen Union*, in : Epiney Astrid / Nüesch Daniela (édit.), *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, 1e éd., Zürich 2016, p. 44.

480. Pour une analyse approfondie de l'art. 16 TFUE, Cf. *Idem*, p. 42 ; Voir aussi la jurisprudence de la CJUE, en particulier les arrêts *Rijkeboer*, C-553/07, EU :C :2009 :293, consid. 47, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU :C :2014 :238, consid. 53, *Google Spain et Google*, C-131/12, EU :C :2014 :317, pts. 53, 66 et 74. Également les arrêts *Commission/Allemagne*, C-518/07, EU :C :2010 :125, consid. 24, et *Commission/Hongrie*, C-288/12, EU :C :2014 :237, consid. 51 pour la recherche d'équilibre entre le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel.

dans tout État membre. Il est technologiquement neutre [481].

Le choix d'un Règlement et non d'une directive répond à un objectif d'harmonisation des règles de droit dans l'UE dans le domaine de la protection des données. Il contribue à renforcer la sécurité juridique et la transparence pour offrir à toutes les personnes au sein de l'UE un niveau uniforme de droits, d'obligations et de responsabilités. Ce choix tient compte de la volonté du législateur d'harmoniser la législation sur la protection des données dans les États membres de l'UE [482]. 560

Ce choix du Règlement vise à assurer une surveillance cohérente et des sanctions équivalentes au sein de l'Union : les autorités de contrôle nationales doivent aussi pouvoir coopérer efficacement dans l'exercice de leurs pouvoirs de surveillance et de contrôle [483]. Si la directive 95/46/CE posait comme critère du droit applicable celui de la localisation du responsable du traitement et de ses moyens de collecte, le Règlement retient quant à lui comme critère du droit applicable le « ciblage du citoyen [484]». 561

Après l'adoption en mai 2016 du Règlement Européen sur la protection des données personnelles (GDPR), la Commission Européenne a décidé d'adapter les règles issues de la directive vie privée et communications électroniques (directive 2002/58/CE du 12 juillet 2002, révisée en 2009), notamment l'utilisation des cookies [485]. 562

481. Epiney / Kern, *Zu den Neuerungen im Datenschutzrecht der Europäischen Union*, p. 44 ; Sydow Gernot / Kring Markus, *Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug - Konkurrierende Leitbilder für den europäischen Rechtsrahmen*, in : Zeitschrift für Datenschutz 2014, pp. 271-276.

482. Arrêt CJUE du 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) contre Administración del Estado*, C-468/10 et C-469/10, ECLI :EU :C :2011 :777.

483. Consid. 9 à 13 RGPD.

484. Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*, p. 21.

485. Parlement européen et Conseil de l'UE, *Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2002, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002L0058 » (04/07/2017).

G. La directive 2002/58/CE

563 La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), exige que les États membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, et notamment le droit au respect de leur vie privée, afin d'assurer la libre circulation des données à caractère personnel dans la Communauté.

564 La directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

565 Elle constate que l'internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Si les services de communications électroniques accessibles au public sur l'internet ouvrent de nouvelles possibilités aux utilisateurs, ils présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

566 Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits de l'homme et libertés fondamentales qui n'entrent pas expressément dans le cadre de la directive 2002/58/CE, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel. La directive 95/46/CE s'applique aux services de communications électroniques non publics.

567 La Commission européenne a présenté des mesures qui visent à réformer la directive 2002/58/CE. Elle souhaite étendre le champ d'application du texte à l'ensemble des fournisseurs de services de communications électroniques.

568 La réforme de la directive 2002/58/CE vise à moderniser les règles applicables aux communications électroniques avec les nouvelles dispositions du Règlement, adopté le 27 avril 2016, en remplace-

ment de la directive 95/46/CE.

La Commission propose également de nouvelles règles, afin de garantir que le respect de la vie privée soit assuré de la même manière que dans les États membres en vertu du Règlement, lorsque des données à caractère personnel sont traitées par les institutions et organes de l'UE. 569

L'actuelle directive sur la vie privée et communications électroniques ne s'applique qu'aux opérateurs de télécommunication traditionnels. Avec la révision de la directive, les règles en matière de respect de la vie privée s'appliqueront également aux nouveaux acteurs dans le secteur des services de communications électroniques, tels que WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, ou Viber. 570

La directive sera remplacée par un Règlement. Cette modernisation du droit applicable a pour objectif d'assurer aux particuliers comme aux entreprises de l'UE un niveau de protection uniforme de leurs communications électroniques. L'harmonisation du cadre juridique pour l'ensemble de l'Union profitera aux entreprises, du fait de la sécurité juridique qui en résultera. 571

Ce nouvel instrument juridique vise à renforcer le respect de la vie privée tant dans le contenu des communications électroniques, mais aussi des métadonnées (par exemple, la localisation, la date ou l'heure d'un appel). Ces éléments devront être anonymisés ou effacés, en l'absence de l'autorisation expresse de l'utilisateur, sauf si les données sont « nécessaires ». Il conviendra de clarifier cette notion. Les opérateurs de télécommunications traditionnels auront davantage de possibilités d'utiliser les données personnelles et de fournir des services supplémentaires. Cette prérogative sera conditionnée à l'octroi d'une autorisation d'exploitation des données de communication. Les conditions d'octroi de cette autorisation seront particulièrement importantes à clarifier. La politique des cookies sera réformée. 572

Le projet de Règlement européen E-privacy a été proposé par la Commission Européenne le 10 janvier 2017 [486]. Il introduit des chan- 573

486. Commission européenne, *La Commission propose de resserrer les règles en matière de respect de la vie privée pour toutes les communications électroniques et actualise les règles relatives à la protection des données pour les instituti - Communiqué de presse du 10 janvier 2017*, in : Commission eu-

gements importants dans la régulation des communications électroniques [487]. Le groupe de travail de l'Article 29 de la Commission européenne a pris position le 4 avril 2017 sur ce projet et a accueilli favorablement la proposition de ce Règlement. Il apprécie le choix du Règlement comme instrument législatif, le fait que ce Règlement intègre les OTT (« Over-The-Top » tels que Skype et Whats App) et les mettent sur un pied d'égalité avec les opérateurs télécoms sur le plan des obligations de confidentialité. Le groupe de travail de l'Article 29 de la Commission européenne a également relevé favorablement les efforts de modernisation des règles applicables au tracking en ligne. Néanmoins, les autorités de protection des données ont exprimé leur inquiétude sur quatre sujets : le Wifi tracking, l'analyse du contenu et des métadata, les murs de tracking (tracking wall) et la mise en œuvre effective de protection de la vie privée « par défaut » (privacy by default) dans les terminaux et logiciels.

574 Le 9 juin 2017, le comité LIBE du Parlement européen a rendu son rapport relatif au projet de Règlement E-privacy 2002/58/CE [488].

575 Le rapport rappelle l'objectif du Règlement : renforcer la confidentialité des communications électroniques et la protection des communications électroniques indépendamment des technologies utilisées. Le projet prévoit notamment que le traitement des métadonnées soit conditionné au consentement de la personne concernée. Il vise à garantir un niveau élevé de protection, en parfaite cohérence avec le Règlement. L'existence de règles strictes en matière de protection des données vise à susciter la confiance nécessaire pour que l'économie numérique se développe dans l'ensemble du

ropéenne (https ://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_17_16 » (25/03/2020).

487. Burton Cédric / Cadiot Sarah / De Boel Laura, *EU Commission Publishes Proposal for e-Privacy Regulation : The Top Nine Key Points You Need to Know*, in : The WSGR Data Alert (https ://www. wsgrdataadvisor.com/), s.l. 2017, p. « https://www.wsgrdataadvisor.com/2017/01/eu-commission-publishes-proposal-for-e-privacy-regulation-the-top-nine-key-points-you-need-to-know/ » (04/03/2020).

488. European Commission, *Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive » (04/07/2017).

marché intérieur [489].

Comme l'a souligné le président Juncker dans son discours sur l'État de l'Union prononcé le 14 septembre 2016, « être européen, c'est avoir le droit de voir ses données à caractère personnel protégées par une législation forte, une législation européenne. Car les européens n'aiment pas que des drones planent au-dessus de leur tête pour enregistrer leur moindre geste ni que des entreprises consignent chacun de leurs clics de souris. C'est pourquoi le Parlement, le Conseil et la Commission se sont entendus en mai dernier sur un Règlement européen commun sur la protection des données. Cette législation européenne stricte s'applique aux entreprises, où qu'elles se trouvent, à chaque fois qu'elles traitent nos données. Car en Europe, la vie privée n'est pas un vain mot. C'est une question de dignité humaine [490]». 576

H. Les recommandations du « Groupe 29 »

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales [491]. 577

Ce groupe de travail contribue à l'élaboration des normes européennes en adoptant des recommandations. Il rend des avis sur le niveau de protection dans les pays hors UE. Il conseille la Commission européenne sur tout projet ayant une incidence sur la protection des données et des libertés des personnes [492]. 578

Les recommandations de ce groupe facilitent l'interprétation des textes de l'Union et contribuent à l'uniformisation de la pratique 579

489. European Commission, *Communication on Building a European Data Economy*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy » (23/10/2017).
490. Commission européenne, *Discours sur l'état de l'Union du Président Juncker du 14 septembre 2016*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/france/news/20160914_discours_soteu_fr » (05/12/2018).
491. European Commission, *Article 29 Working Party*, in : European Commission (https ://ec.europa.eu/), Brussels s.a., p. « https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358 » (06/12/2019).
492. *Ibidem.*

en matière de protection des données au sein de l'UE.

580 Concernant le Règlement, un Fablab a été organisé le 26 juillet 2017 à Bruxelles relatif à la mise en œuvre du Règlement. Des représentants de la société civile, de l'industrie et des autorités de protection des données se sont réunis autour de quatre ateliers pour réfléchir aux outils de mise en œuvre du Règlement. Les thèmes abordés furent les suivants : la certification et les labels, les délégués à la protection des données et les analyses d'impact relatives aux données personnelles, ainsi que le droit à la portabilité des données.

581 Toutes les recommandations du Groupe 29 sont publiées sur le site de la Commission européenne [493]. Il a été remplacé par le comité européen de la protection des données lors de l'entrée en vigueur du Règlement le 25 mai 2018.

I. La jurisprudence de la Cour de Justice de l'Union européenne relative à la protection des droits fondamentaux

582 Le droit fondamental à la protection des données constitue une priorité de l'Union européenne. Preuve en est le processus législatif initié par la Commission européenne, visant à réformer le cadre réglementaire de l'Union relatif à la protection des données. Preuve en sont également les négociations entre les États-Unis et l'Union européenne en vue de la conclusion d'un nouvel accord visant à remplacer l'accord Safe Harbor, dans le domaine des transferts de données personnelles entre l'UE et les USA.

583 Il est intéressant d'observer que la jurisprudence de la Cour de Justice de l'Union européenne relative à la protection des droits fondamentaux se reflète dans les dispositions du Règlement européen sur la protection des données. Cette cohérence répond au besoin de sécurité juridique au sein de l'Union européenne.

584 Quels sont les critères retenus par le juge de l'Union lorsqu'est soumise à son contrôle une mesure limitative de l'exercice d'un droit fondamental prise par une institution de l'Union ?

493. Recommandations du groupe de travail de l'art. 29 sur European Commission, *Article 29 Working Party*.

(a) Le droit à la protection des données, un droit fondamental consacré à l'article 8 de la Charte des droits fondamentaux de l'Union

Au niveau du droit de l'Union, un droit à la protection des données a été érigé en droit fondamental avec la Charte des droits fondamentaux de l'Union, du 7 décembre 2000 et a été doté d'une valeur juridique contraignante depuis l'entrée en vigueur du Traité de Lisbonne depuis le 1er décembre 2009 [494]. 585

L'article 8 de la Charte garantit ce droit et le distingue du droit au respect de la vie privée et familiale, visé à l'article 7 de la Charte. 586

(b) La limitation des droits fondamentaux (article 52 de la Charte)

Les limitations apportées à des droits fondamentaux sont définies à l'article 52 de la Charte. 587

Selon Mr Guy Braibant, qui a participé à l'élaboration de la Charte, il existerait 3 régimes de limitations à l'exercice des droits fondamentaux [495]. 588

La clause générale de limitation est exprimée dans ses termes : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ». Il s'agit du paragraphe 1er de l'article 52 de la Charte. 589

Le paragraphe 2 de l'article 52 de la Charte dispose que « les droits reconnus par la Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci ». 590

Le paragraphe 3 de l'article 52 de la Charte, prévoit que « le sens et la portée des droits garantis par la Charte qui correspondent à des droits garantis par la CEDH sont les mêmes que ceux que leur confère la CEDH ». Ainsi une limitation à un droit garanti par la 591

494. art. 6, par.1, al. 1 Traité sur l'Union européenne.
495. Braibant Guy, *La Charte des droits fondamentaux de l'Union européenne*, 1e éd., Paris 2001, p. 257.

Charte, qui correspond à un droit garanti par la CEDH, ne peut être admise que si la CEDH, admet la même limitation à ce dernier droit.

(c) L'analyse de l'article 52

592 L'article 52, paragraphe 1er indique que la limitation doit être prévue par la loi. Il ressort de la jurisprudence que la condition d'être prévue par la loi exige que la limitation ait une base légale expresse [496].

593 L'article 52, paragraphe 1 de la Charte pose également comme condition que la limitation de l'exercice des droits et libertés doit « respecter le contenu essentiel desdits droits et libertés ». S'il s'agit d'une condition autonome, nous pouvons nous interroger sur l'articulation entre cette condition et le principe de proportionnalité [497].

594 Il ressort de la jurisprudence que lorsque cette condition est examinée par le juge de l'Union, elle l'est tantôt en amont du contrôle de proportionnalité, en tant que condition autonome, tantôt dans le cadre dudit contrôle [498].

595 En amont du contrôle de proportionnalité : Dans l'arrêt Digital Rights e.a, la Cour de Justice a conclu à l'absence d'atteinte au contenu essentiel du droit garanti par l'article 7 de la Charte et de celui garanti par l'article 8 de celle-ci avant même d'examiner si la mesure litigieuse poursuivait un objectif d'intérêt général et de s'engager dans le contrôle de proportionnalité de ladite mesure. La Cour de Justice a conclu à l'absence d'atteinte en raison du fait que la directive 2006/24/CE [499], ne permettait pas la prise de connaissance du contenu des communications électroniques et prévoyait

496. Arrêt CJUE du 1er juillet 2010, *Knauf Gips c. commission*, C-407/08 P, Rec. 2010, p. I-06375, consid. 91 ; Arrêt CJUE du 29 novembre 2012, *Schrecke et Eifert, Schwarz, Thesing et Bloomberg Finance c. BCE*, T-590/10, JOUE, 5 mars 2011, ECLI :EU :T :2012 :635, consid. 76 ; Arrêt CJUE du 28 mai 2013, *Trabelsi e.a. c. Conseil*, ECLI :EU :T :2013 :273, consid. 35 et Arrêt CJUE du 21 février 2018, *Ezz e.a.c Conseil*, T-256/11, JOUE, 7 avril 2014, ECLI :EU :T :2018 :90, consid. 198.

497. Placco Agostino Valerio, *La protection des données à caractère personnel dans le cadre de la jurisprudence de la cour de justice de l'union européenne relative aux droits fondamentaux*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 33.

498. *Idem*, p. 34.

499. Parlement européen et Conseil de l'UE, *Directive 2006/24/CE du 13 avril 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public*

une règle relative à la protection et à la sécurité des données visant à prévenir la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données [500].

Dans le cadre du contrôle de proportionnalité : Dans l'arrêt Ezz e.a.c Conseil, la Cour de Justice a examiné la condition autonome dans le cadre d'un test de proportionnalité. Elle a effectué le constat que les inconvénients générés par les mesures litigeuses de gel d'avoir n'étaient pas démesurées par rapport aux objectifs poursuivis. Elle a illustré son propos en indiquant que lesdites mesures présentaient un caractère temporaire et réversible. Elles ne portaient pas atteinte au « contenu essentiel » du droit de propriété [501]. Dans un autre arrêt du 8 avril 2014, la Cour de justice de l'UE a invalidé la directive 2006/24 en particulier parce qu'elle viole le principe de proportionnalité. Si son objectif est légitime, la conservation systématique et sans exception des données accessoires de communications de tous les utilisateurs européens pour une durée déterminée (sans lien avec leur situation particulière, le type de donnée et le but poursuivi) n'est pas proportionnée. L'absence de garanties concernant la sécurité des données, les modalités d'accès et leurs conditions utilisation constituent également une atteinte particulièrement grave [502]. 596

Quel que soit le stade où le contrôle de proportionnalité est effectué, le juge de l'Union vérifie que certaines facultés ou prérogatives inhérentes au droit fondamental sont préservées. 597

(d) Le contrôle de proportionnalité

L'article 52, paragraphe 1 de la Charte prévoit, dans sa seconde phrase que : « Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général recon- 598

ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2006, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32006L0024&from=LV » (09/12/2019).

500. Arrêt *Digital Rights e.a.*, précité, consid. 39 et 40.

501. Arrêt CJUE du 27 février 2014, *Ahmed Abdelaziz Ezz e.a. contre Conseil de l'Union européenne*, T-256/11, EU :T :2014 :93, consid. 198.

502. Métille Sylvain, *Directive sur la conservation des données invalidée par la CJUE*, in : Village de la Justice (https ://www.village-justice.com/), Paris 2014, p. « https : / / www . village - justice . com / articles / Directive - sur - conservation-des,16679.html » (09/12/2019).

nus par l'union ou au besoin de protection des droits et libertés d'autrui ».

599 Tout d'abord, une limitation à l'exercice d'un droit fondamental doit répondre à un objectif d'intérêt général reconnu par l'Union ou satisfaire à un besoin de protection des droits et libertés d'autrui. Les objectifs d'intérêt général ne sont cependant pas limitativement énumérés comme c'est le cas de certaines dispositions de la CEDH, telles que l'article 8, paragraphe 2.

600 Dans le cadre de la jurisprudence du contrôle de la légalité d'actes des institutions de l'Union au regard des droits fondamentaux, deux définitions différentes du principe de proportionnalité se rencontrent [503].

601 La première définition retenue est celle qui exige que « les moyens mis en œuvre par un acte de l'Union soient aptes à réaliser l'objectif visé et n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre [504] ».

602 La seconde définition du principe de proportionnalité exige que « les actes des institutions de l'Union ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation des objectifs légitimes poursuivis par la réglementation en cause, étant entendu que lorsqu'un choix s'offre entre plusieurs mesures appropriées, il convient de recourir à la moins contraignante et que les inconvénients causés ne doivent pas être démesurés par rapport aux buts visés [505] ».

603 Agostino Valerio Placco, ancien Conseiller juridique pour les affaires administratives et délégué à la protection des données à la Cour de Justice de l'Union européenne, a comparé les deux définitions.

604 L'exigence selon laquelle la mesure doit être apte/appropriée à atteindre l'objectif poursuivi est commune, selon lui, aux deux défi-

503. Arrêt *Digital Rights e.a.*, précité, consid. 39 et 40.
504. Arrêt CJCE du 22 janvier 2013, *Sky Österreich*, C-283/11, JOUE, 9 mars 2013, p. C 71/3, consid. 50 ; Arrêt CJUE du 17 octobre 2013, *Schaible*, C-101/12, JOUE C 367/7, 14 décembre 2013, consid. 29 ; Arrêt CJUE du 13 November 1990, *The Queen / Ministry of Agriculture, Fisheries and Food, ex parte FEDESA e.a.*, C-331/88, Rec. 1990, p. I-04023, ECLI :EU :C :1990 :391, consid. 13 et Arrêt CJUE du 8 juillet 2010, *Afton Chemical*, C-343/09, Rec. 2010, P.I-07027, consid. 45.
505. *Idem*, consid. 45.

nitions.

L'exigence retenue dans la première définition, selon laquelle la mesure ne doit pas aller au-delà de ce qui est nécessaire pour atteindre ledit objectif semble correspondre à l'exigence, retenue dans la seconde définition, selon laquelle il convient de recourir à la mesure la moins contraignante. 605

En revanche, seule la seconde définition présente l'exigence selon laquelle « les inconvénients générés par la limitation au droit fondamental en cause ne doivent pas être démesurés par rapport au but poursuivi [506] ». 606

Il ressort cependant de la jurisprudence, que le juge de l'Union vérifie tout de même, après avoir vérifié le caractère approprié de la mesure litigieuse par rapport au but poursuivi et l'absence de mesures appropriées moins contraignantes, si les inconvénients générés par ladite mesure demeurent proportionnés par rapport audit but [507]. 607

Par conséquent, quelle que soit la définition retenue par le juge de l'Union, il vérifie le respect du principe de proportionnalité en trois temps [508]. 608

Tout d'abord il vérifie si la limitation à l'exercice d'un droit fondamental constitue un moyen pertinent pouvant conduire à la réalisation effective de ce but. 609

Ensuite, le juge se demande si d'autres mesures, moins attentatoires au droit fondamental concerné, mais permettant d'atteindre le but poursuivi existent. 610

En l'absence de mesures moins attentatoires au droit fondamental en cause, la limitation sera jugée nécessaire. 611

À défaut, la limitation au droit fondamental sera censurée. Ce sera le cas si les mesures alternatives moins attentatoires au droit fondamental concerné sont jugées aussi efficaces que la mesure litigieuse, 612

506. Placco, *La protection des données à caractère personnel*, p. 34.
507. Arrêt CJUE du 8 juin 2010, *Vodaphone, e.a*, C-58/08, Rec. 2010, p. I-04999, consid. 59 ; Arrêt CJUE du 12 juillet 2012, *Association Kokopelli*, C-59/11, JOUE 22 Septembre 2012, C 287/9, consid. 61 à 68.
508. Placco, *La protection des données à caractère personnel*, p. 34.

ou à tout le moins suffisante pour atteindre l'objectif recherché [509] ou contribuant de manière efficace [510] ou suffisamment [511] efficace à la réalisation de cet objectif.

613 Enfin, le test proportionnalité au sens strict [512] a pour objectif de vérifier si la limitation à l'exercice d'un droit fondamental n'impose pas une charge excessive sur le titulaire de ce droit. Il s'agit d'analyser les avantages de la mesure (au regard du but poursuivi) et les inconvénients de celle-ci (au regard du droit fondamental dont l'exercice se trouve limité).

614 Le juge vérifie ainsi que la limitation à l'exercice d'un droit fondamental ne constitue pas compte « une intervention démesurée et intolérable » dans les prérogatives des titulaires dudit droit, qui porterait atteinte à la substance même de ce droit [513].

615 Seul un déséquilibre excessif entre le coût imposé au titulaire du droit fondamental concerné et le bénéfice engendré par la mesure litigieuse est censuré lorsqu'il en résulte une atteinte à la substance même du droit fondamental concerné.

616 Bien que la Charte ait une valeur contraignante, le juge de l'Union continue parfois à faire référence à l'exigence « d'absence d'intervention démesurée et intolérable » qui porterait atteinte à la substance même du droit fondamental en cause [514]. Il fait référence à

509. Arrêt CJUE du 12 juillet 2005, *Alliance for Natural Health e.a*, C-154 / 04 et C-155/04, ECLI :EU :C :2005 :449, consid. 70.
510. Arrêt CJUE du 9 novembre 2010, *Schecke et Eifert*, C-92/09, Rec. 2010, p. I-11063, consid. 86.
511. Arrêt CJUE du 24 novembre 2005, *Schwarz*, C-366/04, Rec. 2005 p. I-10139, consid. 53.
512. Ce concept apparaît dans l'Arrêt CJUE du 13 septembre 2016, *Arctic Paper Mochenwangen c. Commission*, T-634/130, C-454/6, ECLI :EU :C :2016 :684, consid. 70, et Arrêt CJUE du 13 septembre 2016, *Raffinerie Heide c. Commission*, T-631/13, C-313/18, ECLI :EU :T :2013 :423, consid. 74.
513. Arrêt CJUE du 13 décembre 1979, *Liselotte Hauer contre Land Rheinland-Pfalz*, 44/79, ECLI :EU :C :1979 :290 ; Arrêt CJUE du 13 juillet 1989, *Hubert Wachauf contre Bundesamt für Ernährung und Forstwirtschaft*, 5/88, ECLI :EU :C :1989 :321, consid. 18 ; Arrêt CJUE du 5 octobre 1994, *X contre Commission des Communautés européennes*, C-404/92 P., ECLI :EU :C :1994 :361, consid. 18 et Arrêt CJUE du 13 avril 2000, *Kjell Karlsson e.a.*, C-292/97, ECLI :EU :C :2000 :202, consid. 45.
514. Arrêt CJUE du 16 novembre 2011, *Bank Melli Iran c. Conseil*, C-548-09 P, ECLI :EU :C :2011 :735, consid. 114 ; Arrêt CJUE du 9 septembre 2010, *Al-Aqsa c. Conseil*, T-348/07, Rec.2010, p. II-04575, consid. 121 ; Arrêt CJUE du 14 juin 2018, *Markhlouf c. Conseil*, C-458/17 P, ECLI :EU :C :2018 :441, consid.

cette exigence en même temps que celle d'un « juste équilibre » ou d'une « pondération équilibrée » dans le cadre d'une même analyse [515].

La jurisprudence de l'Union se rapproche ainsi de celle de la Cour européenne des droits de l'homme. Cette dernière a affirmé que la CEDH impliquait le maintien d'un juste équilibre entre les exigences de l'intérêt général et les impératifs de la sauvegarde des droits fondamentaux de l'individu [516]. 617

(e) L'analyse d'impact préalable

Il ressort de la jurisprudence de l'Union que le juge recherche « le juste équilibre [517] » ou une « pondération équilibrée [518] ». 618

A titre d'exemple, l'arrêt Schecke et Eifert traitent de la validité de dispositions contenues dans deux Règlements communautaires, adoptés l'un par le Conseil de l'Union européenne, l'autre par la Commission européenne qui prévoyaient, pour les autorités nationales compétentes, une obligation de publication annuelle a posteriori sur un site internet unique par État membre, des noms, municipalités de résidence, et le cas échéant code postal des bénéficiaires de certaines aides agricoles, ainsi que des montants reçus au titre de ces aides par chacun d'eux. Cette mesure avait pour objectif d'intérêt général la transparence de l'utilisation des fonds communautaires de la Politique agricole commune et la bonne gestion finan- 619

97.

515. Arrêt CJUE du 13 septembre 2016, *Arctic Paper Mochenwangen c. Commission*, C-551/14 P, C-454/6, ECLI :EU :C :2016 :684, consid. 55 et 73 ; Arrêt CJUE du 13 septembre 2016, *Raffinerie Heide c. Commission*, C-454/7, ECLI :EU :C :2016 :685, consid. 55-77 ; Arrêt du 22 juin 2016, *Recycling und Roheisen c. Commission*, ECLI :EU :C :2016 :469, consid. 56 et 74 et Arrêt du 26 septembre 2014, *Molda c. Commission*, T-629/13, ECLI :EU :T :2014 :834, consid. 57 et 75.

516. Arrêt CourEDH du 23 juillet 1968, *Relative à certains aspects du régime linguistique de l'enseignement en Belgique c. Belgique*, requête n° 1474/62, 1677/62, 1691/62, 1769/63,1994/63, 2126/64, in : Revue générale du droit, consid. 5.

517. Arrêt CJUE du 6 septembre 2012, *Deutsches Weintor*, C-544/10, ECLI :EU :C :2012 :526, consid. 47, Arrêt CJUE du 22 janvier 2013, *Sky Österreich*, C-283/11, ECLI :EU :C :2013 :28, consid. 60 et 67, Arrêt CJUE du 3 septembre 2008, *Commissione.a.c Kadi*, C-584/10 P, C-593/10 P, C-595/10 P, ECLI :EU :C :2013 :518, consid. 131).

518. Arrêt CJUE du 9 novembre 2010, *Schecke et Eifert*, ECLI :EU :C :2010 :662, Rec. 2010 p., I-11063, consid. 77, et Arrêt du 16 décembre 2008, *Satakunnan Markkinaporssi et Satamedia*, C-73/07, EU :C :2008 :727, consid. 56.

cière de ces fonds au travers d'un contrôle public de ladite utilisation. La Cour de Justice a constaté qu'à l'égard des personnes physiques bénéficiaires de ces aides, la mesure constituait une atteinte aux droits reconnus par les articles 7 et 8 de la Charte et qu'une telle atteinte était contraire au principe de proportionnalité.

620 La Cour de Justice a notamment relevé que ni le Conseil de l'Union européenne, ni la Commission européenne n'avaient cherché à effectuer une pondération équilibrée entre les objectifs d'intérêt général poursuivis et les droits fondamentaux en cause, dès lors que rien n'indiquait selon la Cour de Justice, que ces institutions avaient pris en considération lors de l'adoption des dispositions litigieuses, des modalités de publication d'informations relatives aux bénéficiaires concernés qui seraient conformes auxdits objectifs, mais moins attentatoires à ces droits.

621 Lesdites institutions auraient dû examiner, dans le cadre d'une « pondération équilibrée » des différents intérêts en cause, si une publication nominative plus limitée n'aurait pas été suffisante pour atteindre les objectifs poursuivis [519]. La référence à une « pondération équilibrée » des intérêts entre le respect d'un droit fondamental et un objectif d'intérêt général est capitale. Elle suggère une pesée minutieuse des intérêts en présence qui ne peut intervenir que dans le cadre d'une analyse explicite et détaillée. Pour la première fois, le juge de l'Union développe l'exigence formelle d'une analyse d'impact préalable, qui est devenue une exigence fondamentale du Règlement européen sur la protection des données (article 35 Règlement [520, 521].

622 Le Règlement européen sur la protection des données ne fait pas explicitement référence aux notions de : « pondération équilibrée », « juste équilibre », « limitations strictement nécessaires » ou « né-

519. Arrêt *Schecke et Eifert*, consid. 83.

520. « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

521. art. 35 RGPD.

cessaires ».

Le RGPD précise que « le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données lorsque le traitement risque d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Cette analyse d'impact a pour but d'évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque [522]». 623

Ce même considérant impose au responsable du traitement, la consultation de l'autorité de contrôle avant que le traitement n'ait lieu « lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé, que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre [523]». 624

Il ressort de ce considérant que le Parlement européen semble avoir recherché à effectuer une pondération équilibrée des intérêts en présence, entre les objectifs d'intérêt général et les droits fondamentaux en cause. Cela correspond à l'ambition du Parlement européen formulée un mois après que la Cour de Justice a rendu son arrêt Schecke et Eifert, de renforcer son évaluation d'impact autonome sur les droits fondamentaux afin de la rendre plus systématique [524]. En cohérence avec le Parlement européen, le Conseil a également formellement confirmé que ses amendements aux propositions législatives devaient être conformes à la Charte [525]. En 2015, le Conseil a élaboré des lignes directrices relatives à la méthodologie à suivre afin de vérifier la compatibilité avec les droits fondamentaux au sein des instances préparatoires du Conseil [526]. 625

522. Consid. 84 RGPD.
523. Consid. 84 RGPD.
524. Parlement européen, *Résolution du 15 décembre 2010 sur la situation des droits fondamentaux dans l'Union européenne - Aspects institutionnels à la suite de l'entrée en vigueur du Traité de Lisbonne (2009/2161(INI))*, in : Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2010, p. « https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0483+0+DOC+XML+V0//FR (10/12/2019).
525. Conseil de l'UE, *Conclusions du Conseil sur le rapport 2013 de la Commission sur l'application de la Charte des droits fondamentaux de l'UE et sur la cohérence entre les aspects internes et externes de la protection et de la promotion des droits de l'homme dans l'Union européenne*, in : Conseil de l'UE (https ://www.consilium.europa.eu/), Bruxelles 2014, p. « https://www.consilium.europa.eu/media/28080/143100.pdf » (23/12/2019).
526. Conseil de l'UE, *Compatibilité avec les droits fondamentaux : Lignes di-*

Ces lignes directrices ont été mises à jour en 2014 sous l'effet de la jurisprudence récente du juge de l'Union (arrêts Shecke et Eifert et Digital Rights e.a). Il a intégré une liste des droits fondamentaux comme l'avait fait en 2010 la Commission européenne.

626 La jurisprudence du juge de l'Union en matière de protection des données à caractère personnel rappelle de façon récurrente que les dérogations à cette protection des données et les limitations de celle-ci doivent s'opérer dans les limites du « strict nécessaire [527] ».

627 L'article 52, paragraphe 1 de la Charte impose que la limitation à l'exercice du droit fondamental concerné soit nécessaire, et non strictement nécessaire. Il apparaît dans la jurisprudence de la CourEDH que ces deux notions n'ont pas la même portée [528]. Force est de constater cependant que la distinction à faire entre ce qui est « strictement nécessaire » et ce qui est « nécessaire » n'apparaît pas avec évidence.

628 Il apparaît dans les arrêts Schecke et Eifert du 9 novembre 2010, l'arrêt Schwarz du 17 octobre 2013 et l'arrêt Digital Rights e.a du 8 avril 2014, tous rendus sur renvoi préjudiciel, que l'exigence de « stricte nécessité » a pu se matérialiser par certaines obligations mises à la charge du législateur de l'Union. Le législateur est ainsi tenu d'effectuer, avant d'adopter un acte portant ingérence aux droits fondamentaux, une analyse de l'impact de l'acte sur les droits fondamentaux susmentionnés. Le législateur doit prévoir des règles claires et précises dotées de garanties suffisantes pour les personnes concernées, contre les risques d'abus lors du traitement de leurs données à caractère personnel.

---

rectrices à l'intention des instances préparatoires du Conseil, in : Conseil de l'UE (https ://www.consilium.europa.eu/), Bruxelles 2015, p. « https://www.consilium.europa.eu/media/30208/qc0214079frn.pdf » (23/12/2019).

527. Arrêt CourEDH du 27 juin 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, requête n° 931/13, ECLI :CE :ECHR :2017 :0627JUD000093113, consid. 56 ; Arrêt CJUE du 9 novembre 2010, *Schecke et Eifert*, Rec. 2010 p., I-11063, consid. 77 et 86 ; Arrêt CJUE du 7 novembre 2013, *Institut professionnel des agents immobiliers (IPI) contre Geoffrey Englebert e.a.*, C-473/12, ECLI :EU :C :2013 :715, consid. 39 ; Arrêt CJUE du 8 avril 2014, *Digital Rights*, précité, consid. 52 et Arrêt CJUE du 11 décembre 2014, *Rynes*, C-212/13, ECLI :EU :C :2014 :2428, consid. 28.

528. Arrêt *Handyside c. Royaume-Uni* du 7 décembre 1976 (req. 5493/72).

J. L'exigence de garanties suffisantes contre les risques d'abus

L'exigence de garanties contre les risques d'abus a été inaugurée dans la jurisprudence de l'Union par l'arrêt Schwarz et a été ensuite confirmé dans l'arrêt Digital Rights e.a. 629

K. L'arrêt Schwarz

L'arrêt Schwarz aborde la question de l'obligation de prélever et de conserver sur le support de stockage intégré dans le passeport les empreintes digitales [529] des demandeurs de passeport. Cette obligation avait pour but d'empêcher l'utilisation frauduleuse des passeports pour endiguer les entrées illégales de personnes sur le territoire de l'Union. 630

La Cour de Justice a considéré que ces prélèvements et conservations des empreintes digitales constituaient un traitement de données à caractère personnel et ainsi une atteinte aux droits reconnus par les articles 7 et 8 de la Charte. Elle a cependant considéré que la clause litigieuse était conforme au principe de proportionnalité. 631

La Cour de Justice s'est interrogée sur le caractère nécessaire du prélèvement d'empreintes digitales et donc sur la question d'éventuelles mesures alternatives. Elle a constaté que la mesure alternative évoquée au cours de la procédure, la saisie d'une image de l'iris de l'œil, est moins attentatoire aux droits reconnus par les articles 7 et 8 de la Charte que le prélèvement d'empreintes digitales. Elle a également constaté que la méthode alternative, fondée sur la reconnaissance de l'iris était non seulement plus onéreuse et aussi moins efficace que celle fondée sur des empreintes digitales du fait de la moindre fiabilité technologique. Elle a conclu en notant que la méthode alternative n'était pas susceptible de contribuer de manière suffisamment efficace, au but tenant à la prévention de l'utilisation frauduleuse des passeports. 632

Concernant le traitement ultérieur de telles empreintes prélevées, la Cour de Justice a relevé, en se référant à l'arrêt de la Cour euro- 633

529. « Les empreintes digitales relèvent de cette notion dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise » (voir en ce sens, notamment, « Arrêt CourEDH du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, Recueil des arrêts et décisions 2008-V, p. 213, consid. 68 et 84 »).

péenne des droits de l'homme dans l'arrêt *S. et Marper c. Royaume-Uni* [530], que le législateur devait s'assurer « qu'il existe des garanties spécifiques visant à protéger les données efficacement contre les traitements impropres et abusifs ».

634 En l'espèce, la Cour de Justice a constaté qu'il existait de telles garanties étant donnée la délimitation de la finalité admise de l'utilisation des empreintes (celle de vérifier l'authenticité du passeport et l'identité de son titulaire) et les modalités de conservation prévues dans le Règlement en cause (stockage sur un support intégré au sein même du passeport et hautement sécurisé). La Cour de Justice en a conclu que le traitement des empreintes digitales n'allait pas au-delà de ce qui était nécessaire pour la réalisation du l'objectif consistant à la prévention de l'utilisation frauduleuse des passeports [531].

635 L'exigence de garanties contre les abus s'est imposée dans l'arrêt Digital Rights e.a. Sur la base de cette jurisprudence, la Cour de Justice a invalidé la directive 2006/24 [532] estimant qu'en adoptant cette dernière « le législateur de l'union avait excédé les limites qu'impose le respect du principe de proportionnalité au regard des article 7, 8 et 52 paragraphe 1 de la Charte [533]».

636 La directive 2006/24 prévoyait l'obligation pour les fournisseurs de services de communications électroniques accessibles au public ou des réseaux publics de communications de conserver pendant une certaine durée des données relatives au trafic et à la localisation des communications électroniques afin de permettre aux autorités nationales chargées de la recherche, détection ou poursuite d'infractions graves, d'y avoir accès. La Cour de Justice a estimé que cette obligation ainsi que l'accès desdites autorités aux données susmentionnées constituaient des ingérences dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Elle a également constaté

530. Arrêt CourEDH du 4 décembre 2008, *S.Marper c. Royaume-Uni*, requêtes n°30562/04 et 30566/04, ECLI :CE :ECHR :2008 :1204JUD003056204. Pour une analyse approfondie, voir « https://conflits.revues.org/17805 » (01/10/2017).

531. Placco, *La protection des données à caractère personnel*, p. 44 ss.

532. Parlement européen et Conseil de l'UE, *Directive 2006/24/CE du 13 avril 2006*, J.O., L105, p. 54.

533. Arrêt *Digital Right e.a.*, précité consid. 69 ; voir aussi les conclusions de l'avocat général du 23 septembre 2015, relatives au renvoi préjudiciel dans l'affaire *Maximillian S. / Data Protection Commissioner*, p. « https://www.legalis.net/jurisprudences/cour-de-justice-de-lunion-europeenne-conclusions-du-23-septembre-2015 » (21/05/2019).

que ces ingérences répondaient effectivement à un objectif d'intérêt général, celui de contribuer à la lutte contre la criminalité grave, et à la sécurité publique.

637 La Cour de Justice a rappelé dans le cadre de l'analyse du caractère nécessaire de ces ingérences que : « les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire [534] ». Faisant référence à la jurisprudence de la Cour européenne des droits de l'homme, l'arrêt *S. et Marper c. Royaume-Uni précité*, la Cour de Justice a rappelé que « la réglementation de l'union en cause devait prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre accès et toute utilisation illicites de ces données [535] ».

638 La Cour de Justice a indiqué : « que la nécessité de disposer de telles garanties est d'autant plus importante, lorsque, comme le prévoyait la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données [536] ».

639 La Cour de Justice en déduit que la directive 2006/24 n'offre pas de garanties suffisantes eu égard à « l'absence générale de limites » quant aux données, aux moyens de communication électronique et aux abonnées ou utilisateurs concernés ainsi qu'à la relation entre les données à conserver et une menace pour la sécurité publique. Elle retient également l'absence de critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et l'utilisation ultérieure de celles-ci aux fins prévues ainsi qu'à l'absence d'indication des conditions matérielles et procédurales afférentes à cet accès et à cette utilisation ; à l'absence de distinction s'agissant de la durée de conservation des données, en fonction de l'utilité éventuelle de celles-ci ou selon les personnes concernées ; à l'absence de règles spécifiques et adéquates régissant la protection et la sécurité des données en cause et à l'absence d'une règle imposant la conservation desdites données sur le territoire de l'union,

534. *Idem*, consid. 191.
535. Placco, *La protection des données à caractère personnel*, p. 18 ss.
536. Arrêt *Digital Right e.a.*, précité, consid. 52 à 55.

de façon à garantir le contrôle, par une autorité indépendante tel qu'exigé par l'article 8, paragraphe 3 de la Charte [537].

640 Il a été en particulier relevé que la directive 2006/24 comportait une ingérence dans les droits fondamentaux en cause « d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'elle telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire ».

641 Le Règlement européen mentionne à l'article 23, paragraphe 2, lettre d, que « toute mesure législative contient des dispositions spécifiques, relatives, au moins le cas échéant, aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicite ».

642 Cet article autorise des limitations aux libertés et droits fondamentaux dans la mesure où elle constitue une « mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité nationale, la défense nationale, la sécurité publique, etc. [538]».

643 Il importe de relever que le critère de la « nécessité » et non pas de la « stricte nécessité » retenu dans la jurisprudence de la Cour de Justice [539] a été retenu par le législateur dans le cadre de l'élaboration du Règlement européen.

644 Les tests de nécessité et de proportionnalité devront donc être conduits lors d'un contrôle juridictionnel de la Cour de justice pour déterminer si les limitations imposées au droit fondamental de la protection des données dans le Règlement correspondent à une pondération équilibrée et à un juste équilibre des intérêts en présence. La question se posera de savoir si d'autres mesures moins attentatoires au droit fondamental de la protection des données existent, permettant d'atteindre le but poursuivi.

645 Il sera intéressant de noter que pour la première fois dans l'arrêt Digital Rights e.a, précité, s'agissant d'un acte adopté par le légis-

537. Arrêt *Digital Rights e.a*, précité, consid. 56 à 68.
538. art. 23 RGPD.
539. Arrêts CJUE du 16 décembre 2008, *Satakunnan Markkinaporssi et Satamedia*, C-73/07, ECLI :EU :C :2008 :727, consid. 56, Arrêt CJUE du 9 novembre 2010, *Scheke et Eifert*, C-92/09 et C-93/09., ECLI :EU :C :2010 :662, consid. 77 et 86, Arrêt CJUE du IPI du 7 novembre 2013, C-473/12, EU.C.2013.715, consid. 39, Arrêt CJUE du 8 avril 2014, *Digital rights e.a.*, consid. 52 et Arrêt *Rynes*, C-212/13, ECLI :EU :C :2014 :2428, consid. 28.

lateur de l'Union, et portant ingérence dans l'exercice d'un droit fondamental, la Cour de Justice détermine l'étendue du pouvoir d'appréciation dudit législateur, et, par conséquent, l'intensité de son contrôle juridictionnel du respect du principe de proportionnalité, en fonction de plusieurs facteurs traditionnellement utilisés par la Cour européenne des droits des l'homme. Dans l'arrêt Digital Right e.a la Cour de Justice constate que « compte tenu, d'une part du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée, et d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict [540] ».

646 L'étroite association entre la protection des données à caractère personnel et le respect de la vie privée ainsi que l'importance de la première pour assurer le second, soulignées dans sa jurisprudence, amènent le juge de l'Union, d'une part à établir que les limitations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du « strict nécessaire » et d'autre part à effectuer un « contrôle strict » du respect , par un acte du droit dérivé de l'union portant atteinte aux droits consacrés aux articles 7 et 8 de la Charte des conditions inhérentes au principe de proportionnalité [541].

647 Au profit des titulaires desdits droits, un contrôle de proportionnalité particulièrement étendu prend progressivement forme au fil des arrêts rendus par le juge de l'Union en la matière [542]. Dans l'ensemble ces évolutions témoignèrent d'une valorisation du rôle de la Cour de Justice de l'Union européenne en tant que véritable juge constitutionnel de l'Union ainsi que d'une convergence significative avec la jurisprudence de la Cour européenne des droits de l'homme, particulièrement importante tant au regard de l'article 52 paragraphe 3 et 54 de la Charte que dans la perspective de l'adhésion de l'Union à la CEDH.

540. Arrêt *Digital Rights e.a.*, précité, consid. 48.
541. Placco, *La protection des données à caractère personnel*, p. 50.
542. *Idem*, p. 51.

L. La proposition de Règlement dédié à la libre-circulation des données non-personnelles

648 Cette proposition a été déposée par la Commission européenne, le 13 septembre 2017 [543].

649 Elle correspond à la volonté de la Commission européenne de « construire une économie européenne des données [544]». « L'analyse des données permet d'améliorer le processus décisionnel, l'innovation et la prévision des événements. Cette tendance mondiale représente un énorme potentiel dans divers domaines, allant de la santé, de l'environnement, de la sécurité alimentaire, du climat et de l'utilisation efficace des ressources à l'énergie, aux systèmes de transport intelligents et aux villes intelligentes [545]». L'économie des données devrait représenter 643 milliards d'euros d'ici à 2020, soit 3,17 % du PIB global de l'Union. [546].

III. Les sources nationales

A. La Loi fédérale sur la protection des données (LPD) du 19 juin 1992, R.S 235.1

650 La protection des données est actuellement régie, au niveau fédéral, par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)1 qui est entrée en vigueur le 1er juillet 1993.

651 La LPD régit le traitement de données concernant des personnes physiques et des personnes morales effectué par des personnes privées et des organes fédéraux (art. 2, al. 1).

652 Cette loi ne s'applique toutefois pas aux données personnelles qu'une

543. European Commission, *Proposal of 13 September 2017 for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017) 495 final)*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF » (23/10/2017).

544. Commission européenne, *« Créer une économie fondée sur les données » - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions du 10 janvier 2017 (COM(2017) 9 final)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2017, p.« http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-9-F1-FR-MAIN-PART-1.PDF » (21/05/2019), pp. 1-4.

545. *Ibidem.*

546. *Ibidem.*

personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers (al. 2, let. a), aux délibérations des Chambres fédérales et des commissions parlementaires (al. 2, let. b), aux procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif, à l'exception des procédures administratives de première instance (al. 2, let. c), aux registres publics relatifs aux rapports juridiques de droit privé (al. 2, let. d) et enfin aux données personnelles traitées par le Comité international de la Croix-Rouge (CICR) (al. 2, let. e).

La LPD fixe les principes à respecter lors du traitement de données. Elle prescrit en particulier que toute collecte de données personnelles ne peut être entreprise que d'une manière licite (art. 4, al. 1), que le traitement de ces dernières doit être effectué conformément aux principes de la bonne foi et de la proportionnalité (art. 4, al. 2) et uniquement dans le but qui est indiqué lors de la collecte, qui est prévu par une loi ou qui ressort des circonstances (art. 4, al. 3). La collecte de données, en particulier la finalité du traitement, doivent en outre être reconnaissables pour la personne concernée (art. 4, al. 4). L'art. 4, al. 5 détermine quant à lui les conditions applicables au consentement de la personne concernée. D'autre part, la personne ou l'organe fédéral qui traite des données personnelles doit s'assurer qu'elles sont correctes (art. 5). Ce principe prend toute sa valeur à l'ère digitale du fait du rôle joué par les algorithmes dans le traitement des Big Data. Le responsable du traitement doit prendre toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. 653

La LPD règle la communication des données à l'étranger (art. 6). Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, du fait de l'absence d'une législation assurant un niveau de protection adéquat. 654

En dépit de l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger, à l'une des conditions suivantes uniquement : 655

— Des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger.

— La personne concernée a donné son consentement.

656 La LPD régit aussi le droit d'accès (art. 8 à 10) et le traitement de données par un tiers (art. 10, a)). L'art. 11a prévoit une obligation pour le Préposé fédéral à la protection des données et à la transparence (ci-après « Préposé ») de tenir un registre des fichiers en ligne et accessible au public ainsi qu'un devoir pour les maîtres du fichier de déclarer leurs fichiers sous réserve d'exceptions. La section 3 contient des dispositions applicables aux traitements de données effectués dans le secteur privé. Ainsi, la LPD interdit aux personnes privées qui traitent des données personnelles de porter une atteinte illicite à la personnalité des personnes concernées (art. 12, al. 1) et en particulier de traiter des données contre la volonté expresse de la personne concernée en l'absence de motif justificatif (art. 12, al. 2, let. b et art. 13). L'art. 14 prévoit une obligation pour les personnes privées d'informer la personne concernée de toute collecte de données sensibles ou de profils de personnalité les concernant, sous réserve d'exceptions. La LPD règle en outre les prétentions de droit civil que les personnes lésées peuvent faire valoir, ainsi que la procédure applicable (art. 15). Les art. 16 à 25 LPD régissent le traitement de données personnelles par des organes fédéraux. Ceux-ci ne sont en droit de traiter des données personnelles que s'il existe une base légale (art. 17, al. 1). Une base légale dans une loi au sens formel est exigée pour le traitement de données sensibles ou de profils de la personnalité (art. 17, al. 2). L'art. 18a prévoit une obligation pour les organes fédéraux d'informer la personne concernée de toute collecte de données personnelles la concernant, sous réserve de certaines exceptions (art. 18b). La communication de données personnelles à des tiers est subordonnée en principe à l'existence d'une base légale (art. 19, al. 1). Les données personnelles ne peuvent être rendues accessibles au moyen d'une procédure d'appel que si cela est prévu expressément par la loi (art. 19, al. 3). Les exigences sont encore plus strictes pour les données sensibles ou les profils de la personnalité, lesquels ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément (art. 19, al. 3).

657 La fourniture d'un service qui est subordonnée à l'autorisation d'une personne pour que ses données soient utilisées à des fins non essentielles (tels que le marketing) est interdite.

658 Toute personne concernée peut requérir la rectification des don-

nées inexactes.

« Le maître du fichier qui fait traiter des données par un tiers demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers, s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse. Les renseignements sont, en règle générale, fournis gratuitement et par écrit sous forme d'imprimé ou de photocopie. Nul ne peut renoncer par avance au droit d'accès [547] ». 659

Le Conseil Fédéral est venu préciser des aspects de la LPD dans une ordonnance relative à la protection des données [548]. Il est vraisemblable que cette ordonnance fera l'objet d'une révision du fait de la refonte de la loi fédérale sur la protection des données en Suisse. 660

547. art. 8 LPD.
548. Ordonnance relative à la loi fédérale sur la protection des données (OLPD) du 14 juin 1993, RS 235.11.

Chapitre 3: L'analyse juridique du Règlement (but, champ d'application, définitions et principes applicables)

§1 Les buts du Règlement européen

Les dispositions du Règlement sur son propre but, telles que présentées à l'article 1 et au considérant 13 du Règlement, sont peut-être ce qui permet le mieux de montrer le bien-fondé de la thèse de la présente étude. Contrairement à la réglementation antérieure, le droit positif de la protection des données, mis en place au niveau européen, avec le Règlement, est un droit qui, selon le Règlement, poursuit de façon égale deux buts distincts, en soi concurrents entre eux et dans une certaine mesure incompatibles, mais que le Règlement met expressément au même niveau. Le droit de la protection des données personnelles n'est plus construit sur la priorité de la protection de la sphère privée. La libre circulation des données personnelles, c'est-à-dire le principe de la liberté de traitement par le responsable de traitement, est placée au même niveau que la protection des personnes. En refusant expressément d'établir une hiérarchie entre eux, mais au contraire en montrant bien la volonté du législateur de les placer au même niveau, cela donne une place de choix à l'action civile en responsabilité (voir paragraphe 1294). 661

La construction de la phrase principale de la disposition du Règlement sur le but est très particulière. Elle l'est, en vue d'exprimer aussi clairement que possible l'égalité de valeur de deux buts concurrents. Il vaut la peine d'examiner cette phrase de près dans différentes langues. Elle présente en effet à deux reprises les deux buts concurrents, mais cette répétition, loin d'être stérile, permet au Règlement de les mettre au même niveau, en les mentionnant chacun à leur tour en premier dans le déroulement de la phrase. C'est comme si cette répétition, avec variante, n'était faite que pour affirmer l'égale importance des deux buts, l'absence de hiérarchie entre 662

eux.

663 La première fois le texte présente les deux buts ainsi [549] :

- « afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'union, à l'égard du traitement des données à caractère personnel »
- « [afin] d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur ».

664 La seconde fois, lors de la répétition donc, la formulation est la suivante :

- « pour garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micro, petites et moyennes entreprises »
- « pour offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de **responsabilités** pour les responsables du traitement et les sous-traitants ».

665 L'action civile et le contrôle a posteriori des autorités de contrôles vont faciliter la prise de conscience et l'acceptation pour les acteurs économiques, que le but de la protection des données est la protection des personnes et le corollaire du principe de liberté, pilier du monde digital [550]. Cette protection des personnes est rendue possible par l'action civile en responsabilité offerte par le Règlement (voir paragraphe 1294), en plus du contrôle a posteriori effectué par des autorités de contrôle. Plus précisément, le contrôle mis en place exige des États de l'UE :

- que les personnes physiques aient certes le droit d'introduire une réclamation auprès des autorités de contrôle contre le responsable du traitement (art. 77 RGPD), ce qui n'a rien d'exceptionnel, mais aussi, en plus, qu'il y ait mise en place du droit à un recours juridictionnel effectif [551] contre les décisions des autorités de contrôle (art. 78 RGPD), qui doivent pouvoir condamner les responsables de traitements à des amendes

549. Consid. 13 RGPD.

550. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. « https://mafr.fr/fr/article/lapport-du-droit-de-la-compliance-dans-la-gouverna/ » (07/03/2020).

551. En cohérence avec l'art. 6 CEDH, et l'art. 47 Charte des droits fondamentaux de l'UE

administratives calculées sur la base du chiffre d'affaires du groupe concerné (art. 79 RGPD).

— que les personnes physiques aient non seulement un droit à la réparation du préjudice en cas de violation du Règlement par le responsable du traitement (art. 82 et 24, qui prévoient le renversement du fardeau de la preuve, le responsable devant désormais prouver que son comportement est conforme au règlement), mais aussi, en plus, qu'il y ait mise en place de ce qui doit représenter « un recours juridictionnel effectif » (art. 79) pour attaquer les responsables de traitement ou les sous-traitants (cela comprend en particulier, selon l'art. 80 du Règlement, la possibilité de class actions).

Cette analyse du rôle central de la responsabilité des acteurs économiques est confirmée par la comparaison des traductions du Règlement. La version anglaise présente ainsi les buts du Règlement : 666

— « In order to ensure a consistent level of protection for natural persons »

— « and to prevent divergences hampering the free movement of personal data within the internal market ».

La seconde fois, donc lors de la répétition, la formulation est la suivante : 667

— « to provide legal certainty and transparency for economic operators »,

— « to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and **responsibilities** for controllers and processors ».

La version espagnole confirme cette perspective selon laquelle la responsabilité des responsables du traitement et des sous-traitants constitue un but central du Règlement. 668

— « Para garantizar un nivel coherente de protección de las personas físicas »

— « evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior ».

La seconde fois, donc lors de la répétition, la formulation est la suivante : 669

— « seguridad jurídica y transparencia a los operadores económicos »

— « y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de **responsabilidades** para los responsables y encargados del tratamiento ».

670 Plus précisément, les trois versions se réfèrent explicitement à la notion de responsabilité par l'usage des mots : « responsabilités », « responsabilities » dans la version anglaise, et « responsabilidades ».

671 C'est manifestement un point central pour les pays tiers, en particulier pour un pays comme la Suisse. Est-il nécessaire qu'une telle action soit mise en place en Suisse, ou suffit-il que les opérateurs économiques suisses puissent être poursuivis dans l'union ? Une analyse approfondie de l'action en responsabilité seulement sera présentée dans la dernière partie de cette thèse, dans le cadre d'une analyse comparée avec le droit de la concurrence.

672 Quel est le but du principe de responsabilité ? Pour le groupe de travail de l'article 29 de la Commission européenne, la responsabilité est le moteur de l'application efficace des principes de protection des données [552]. Pour M.A. Frison-Roche, il s'agit de rétablir la confiance, « confiance dans l'information, confiance dans les systèmes de transmission d'information, confiance dans les opérateurs cruciaux eux-mêmes dans l'indifférence de leur nationalité. Cette confiance provient du principe de Liberté, et de la reconnaissance du principe de l'existence d'une personne humaine, que certains veulent méconnaître, s'approprier ou détruire, non seulement dans le monde digital, mais par le monde réel [553]».

§2 Le champ d'application matériel

673 Le droit européen de la protection des données se fonde sur un principe d'interdiction du traitement de données à caractère person-

552. Groupe de Travail de l'Article 29, *Avis 03/2010 du Groupe de travail de l'Art. 29 sur le principe de la responsabilité - Adopté le 13 juillet 2010 (WP 173)*, in : CNPD (https ://cnpd.public.lu/), Luxembourg 2010, p. « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp173_fr.pdf » (25/03/2020).

553. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. 9.

nel [554] (contrairement au droit suisse qui se fonde sur un principe d'autorisation, l'interdiction du traitement constituant une exception).

Ce principe d'interdiction est limité aux traitements de données à caractère personnel. Les données non-personnelles sont échangées librement et font l'objet d'une réglementation spécifique [555]. Si le caractère personnel fait défaut, alors le droit européen de la protection des données n'est pas applicable [556]. 674

Le champ d'application matériel du Règlement est défini à l'article 2, al. 1er du Règlement. Il s'inscrit dans la continuité de la directive 95/46/CE. Il recouvre tous les traitements de données personnelles qu'ils soient automatisés (même en partie) ou non (à condition que les données traitées soient contenues ou appelées à figurer dans un fichier). 675

À cet égard, il convient de préciser qu'un traitement de données est défini comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel ». 676

À titre d'exemple, seront considérés comme des traitements « la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion, la mise à disposition, le rapprochement, l'interconnexion, la limitation, l'effacement, la destruction, etc. [557] ». 677

Les notions de données à caractère personnel et de traitement, définies à l'article 4 du Règlement sont quasiment identiques à celles 678

554. art. 4, al. 1 RGPD.

555. Parlement européen et Conseil de l'UE, *Règlement (UE) 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (Texte présentant de l'intérêt pour l'EEE)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2018, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1807&from=FI » (07/12/2019).

556. Härting, *Datenschutz-Grundverordnung*, p. 71.

557. Landes-Gronowski Laure, *Le Règlement Général sur la Protection des Données (RGPD) en 10 leçons : L'essentiel du RGPD dans un guide pratique*, in : Avistem Avocats (http ://www.avistem.com/), Paris 2017, p. « http://www.avistem.com/sites/default/files/2017%2001%2010%20Le%20RGPD%20en%2010%20le%C3%A7ons%20V.1_0.pdf » (05/12/2018) ; et voir aussi art. 4, al. 2 RGPD.

émanant de la directive 95/46/CE [558].

679 Une donnée à caractère personnel est constituée par « toute information qui se rapporte à une personne physique, qu'elle soit identifiée, voire simplement identifiable » (même indirectement, par exemple, par un numéro identifiant ou un recoupement d'informations).

680 Cette notion fait référence a l'objectif premier du Règlement qui est de protéger les données personnelles et les droits fondamentaux et libertés fondamentales des personnes physiques.

681 À titre d'exemple, seront considérées comme des données à caractère personnel « les données relatives à la gestion du personnel, aux rémunérations, les trombinoscopes et annuaires d'entreprise, la gestion des fournisseurs, la gestion de la comptabilité, la gestion des clients et des opérations commerciales, de fidélisation et de prospection, la gestion des outils informatiques, la lutte contre la fraude (interne / externe), la surveillance (vidéo, alarme, contrôle des accès,...) etc. [559]».

682 Comme le notent très justement de Terwangne, Rosier et Losdijk [560], la notion de données à caractère personnel, évolue d'une notion « d'identification vers un concept d'individualisation (en anglais « singling out », soit l'individualisation ou le ciblage) ».

683 La notion de personne directement ou indirectement identifiable constitue une nouveauté [561]. La définition de cette notion se scinde en deux catégories :

1. La première catégorie concerne les éléments qui permettent de connaître la personne. Ces éléments sont le nom, les données de géo-localisation, les éléments d'identification en ligne (adresses IP, Cookies...) [562].

2. La seconde catégorie concerne les spécificités individuelles. Il s'agit par exemple des signes physiques distinctifs, des signes

558. Härting, *Datenschutz-Grundverordnung*, p. 71.
559. Landes-Gronowski, *Le RGPD en 10 leçons*, p. 5 ss.
560. Rosier Karen / Losdyck Bénédicte / De Terwangne Cécile, *Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel*, in : Revue du Droit des Technologies de l'information 2016/62, p. 6.
561. art. 4, al. 2 RGPD.
562. Consid. 30 RGPD.

physiologiques, psychiques, génétiques, économiques, culturels ou d'une identité sociale [563].

Le rapport explicatif de l'article 2 de la nouvelle Convention n° 108 du Conseil de l'Europe précise que : Le terme « identifiable » ne fait pas uniquement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'« individualise » ou de distinguer (et, donc, de traiter différemment) une personne. 684

Le champ d'application matériel du Règlement exclut le traitement des données à caractère personnel relatif aux personnes morales et se limite au traitement de données à caractère personnel de personnes physiques ,« indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel » (consid. 14 RGPD). 685

Le Règlement s'applique enfin aux données à caractère personnel traitées par les institutions, organes et organismes de l'union (art. 2, al.3 du Règlement). 686

Des exceptions sont prévues à l'article 2 al. 2 Règlement. Il s'agit des traitements des données à caractère personnel qui sont effectués [564] : 687

(a) « dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'union ;
(b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ; il s'agit des politiques relatives au contrôle aux frontières, à l'asile et à l'immigration [565]
(c) par une personne physique dans le cadre d'une activité strictement / exclusivement personnelle ou domestique ; et
(d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ».

563. Härting, *Datenschutz-Grundverordnung*, p. 73.
564. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2016, p. « https : / / eur - lex . europa . eu / legal - content / FR / TXT / HTML / ?uri = CELEX : 32016R0679 » (18/06/2019).
565. Traité sur le fonctionnement de l'UE, JO C-326/47 du 26 octobre 2012.

688 Le dernier paragraphe *(d)* fait référence à la directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil [566], adoptée par le Parlement européen le 14 avril 2016.

689 Le Règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale [567]. Toutefois, le présent Règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

690 Des dérogations sont prévues concernant la liberté d'expression et d'information pour les traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire (art. 85 RGPD). Les États membres de l'UE concilient ainsi le droit à la protection des données personnelles et le droit à la liberté d'expression et d'information.

691 La question se pose de savoir si les traitements de données stockées sur une Blockchain entrent dans le champ d'application matériel du Règlement européen [568]. Pour Michèle Finck, les traitements de données personnelles stockées sur la Blockchain, sous format texte, entrent dans le champ d'application du RGPD. Il en va de même des données chiffrées qui sont accessibles via une clef publique. Celles-ci ne sont pas chiffrées de manière irréversible. Par conséquent, le Règlement sera applicable. En effet, le caractère irréversible du chiffrement est une condition essentielle pour la non-application du Règlement [569]. Comme la personne demeure identifiable de ma-

566. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016.*
567. art. 18 RGPD.
568. Finck Michèle, *Blockchains and Data Protection in the EU*, in : European Data Protection Law Review 2018/4, p. 22.
569. Groupe de Travail de l'Article 29, *Avis 05/2014 du Groupe de travail de l'Art. 29 sur les Techniques d'anonymisation - Adopté le 10 avril 2014 (WP 216)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2014,

nière indirecte, le RGDP demeure donc applicable. La technique de chiffrement constitue une technique de pseudonymisation au sens du Règlement européen [570]. Le contrôleur européen à la protection des données a publié un guide sur l'utilisation de la fonction hash de chiffrement pour pseudonymiser les données personneles [571]. La même question se pose pour les données bénéficiant d'une fonction de hachage sécurisée, parfois appelée « fonction de hachage unidirectionnelle ». Une fonction de hachage est un processus mathématique fondé sur un algorithme, qui crée une représentation numérique, ou forme comprimée du message, souvent appelée « abrégé » ou « empreinte digitale », et qui prend la forme d'une « valeur de hachage » ou d'un « résultat de hachage » d'une longueur normalisée généralement bien plus courte que le message lui-même, mais qui lui est néanmoins unique. Toute modification apportée au message produit inévitablement un résultat de hachage différent lorsqu'on utilise la même fonction de hachage. Dans le cas d'une fonction de hachage sécurisée, parfois appelée « fonction de hachage unidirectionnelle », il est pratiquement impossible, connaissant la valeur de hachage, de déduire le message initial [572].

Si cette fonction de hachage unidirectionnelle offre des garanties supérieures au chiffrement classique dans le domaine de la protection de la vie privée, il n'en reste pas moins que cette technique demeure une technique de pseudonymisation et non d'anonymisation pour le Groupe de l'Article 29, sur le fondement qu'il est encore possible de faire le lien entre la base de données et la personne concernée. D'autres technologies de chiffrement sont en cours de développement et permettent d'éviter d'avoir accès aux données personnelles elles-mêmes. C'est le cas des techniques de « zero-knowledge proof » et du système MedCo développé par Prof. J.P 692

p. « https : / / ec . europa . eu / justice / article - 29 / documentation / opinion - recommendation/files/2014/wp216_fr.pdf » (11/03/2019).

570. *Idem*, p. 22 ss.

571. EDPS, *Introduction to the hash function as a personal data pseudonymisation technique*, in : EDPS (https ://edps.europa.eu/), Brussels 2019, p. « https:// edps.europa.eu/node/5553 » (30/12/2019).

572. Nations Unies / Commission pour le droit commercial international, *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*, New York 2002, p. 5.

Hubaux et Brian Ford à l'EPFL [573].

693 Le Règlement ne s'applique pas non plus aux questions en lien avec la protection des libertés et droits fondamentaux ou le libre flux des données à caractère personnel, concernant des activités qui ne relèvent pas du champ d'application du droit de l'union, telles que les activités relatives à la sécurité nationale [574].

694 La jurisprudence de la Cour de Justice de l'UE viendra préciser le champ d'application du nouveau Règlement (notions de données personnelles et de traitement, activités échappant ou non au domaine du droit de l'union, etc.). Les règles d'exonération de responsabilité et leurs interactions avec le Règlement, notamment en lien avec le droit à l'effacement et à la limitation du traitement, mériteraient en particulier d'être clarifiées [575].

695 Le Règlement s'applique sans préjudice de la directive 2000/31/CE [576] et notamment des articles 12 à 15. Ces articles exonèrent les prestataires intermédiaires tels que les fournisseurs d'accès et d'hébergement, à raison des informations fournies ou stockées par des tiers sur leurs serveurs ou au moyen de leurs installations.

696 Le champ d'application matériel de la directive 2000/31/CE est le même que celui de la directive 95/46/CE [577]. En revanche, le Règlement vient préciser la notion de traitement de données à caractère personnel, tel que défini à l'art. 4, al. 2 [578]. Celle-ci comporte deux nouvelles opérations dans le Règlement : la « structuration » et la « limitation » [579].

697 La multitude de données non structurées (commentaires, vidéos, photos, blogs, réseaux sociaux...) dans le cadre du traitement de Big

573. MedCo, *Collective Protection of Medical Data*, in : EPFL (https://www.epfl.ch/), Lausanne s.a., p. « https://medco.epfl.ch » (11/03/2019).
574. Consid. 16 RGPD.
575. art. 2, al. 4 RGPD.
576. Parlement européen et Conseil de l'UE, *Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2000, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32000L0031 » (01/10/2017).
577. art. 3 Directive 95/46/CE et art. 2 RGPD.
578. Bensoussan Alain (direct.), *Règlement européen sur la protection des données : Textes, commentaires et orientations pratiques*, 1e éd., Bruxelles 2016, p. 52.
579. *Idem*, p. 52.

Data rend l'opération de structuration fondamentale. Les données non structurées sont des données dont l'ensemble des valeurs possibles n'est pas déterminé à l'avance [580].

Afin d'exploiter ces données et réaliser des calculs, il faut les intégrer dans une structure de base. Cette opération constitue en elle-même un traitement de données à caractère personnel. Le Règlement encadre donc cette opération de structuration pour tenir compte de l'évolution et de la diversité des processus de calcul pratiqués dans un environnement de type Big Data. 698

Le considérant 15 nuance cependant le principe précédent, en indiquant que « les dossiers ou ensembles de dossiers, qui ne sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent Règlement ». Des critères déterminés doivent donc être définis préalablement à toute structuration, afin de rendre le Règlement applicable au traitement de ces données. 699

Quant au principe de limitation, il constitue un nouveau droit accordé aux personnes concernées dans les cas visés à l'art.18 du Règlement. 700

§3 Le champ d'application territorial

Le Règlement étend le champ d'application territorial pour offrir une protection élargie à toutes les personnes concernées qui se trouvent dans l'Union européenne [581]. Cette extension peut s'analyser comme une volonté du législateur de renforcer la protection des citoyens européens et la compétitivité des entreprises européennes, autrefois désavantagées de subir des règles contraignantes qui ne visaient pas les entreprises situées hors de l'Union ou étaient facilement contournées [582]. Cependant, il est décevant de noter que les problèmes essentiels en lien avec les réseaux sociaux n'ont pas été 701

580. Rouvroy Antoinette, *« Des données et des hommes », droits et libertés fondamentaux dans un monde de données massives (T-PD-BUR (2015) 09REV)*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 2016, p. « https://rm.coe.int/16806b1659 » (26/03/2020), p. 5.

581. art. 3 RGPD.

582. Castets-Renard, *Quelle protection des données personnelles en Europe ?*, p. 36.

traités dans le cadre du Règlement [583]. Pour l'instant, ces problématiques sont abordées dans un document séparé au niveau national uniquement [584].

702 L'article 4 de la directive 95/46/CE s'appliquait aux traitements de données à caractère personnel, lorsque le responsable de traitement était établi sur le territoire de l'État membre ou s'il recourait, à des fins de traitement de données à caractère personnel, à des moyens situés sur le territoire d'un État membre, sauf si ces moyens, n'était utilisés à des fins de transit sur le territoire de la Communauté. Une telle règle avait pour effet que des géants de l'Internet, en grande majorité implantés en Californie, échappaient à l'application du droit de l'union [585].

703 Ce critère d'établissement est désormais applicable au responsable du traitement et au sous-traitant, afin de responsabiliser tous les acteurs économiques lors d'un traitement de données à caractère personnel, transferts transfrontaliers inclus.

704 L'article 3 du Règlement précise que : « le présent Règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'union, que le traitement ait lieu ou non dans l'union ». Ainsi, le Règlement est applicable, lorsque le responsable du traitement est établi dans l'union, et que le traitement est effectué dans le cadre des activités d'un établissement de ce responsable au sein de l'union, même si le traitement a lieu en dehors de l'union (ex. : données collectées en France et stockées sur un Cloud en Suisse).

705 Cependant la notion d'établissement est une question de fait qui est interprétée sur la base de l'ensemble des circonstances du dossier. La jurisprudence de la CJUE est à ce titre riche d'enseignements. L'arrêt Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság rendu le 1er octobre 2015 par la CJUE, précise que la no-

583. Blume Peter, *Will it be a better world ? The proposed EU Data Protection Regulation*, in : International Data Privacy Law 2012 2/3, pp. 130-136.

584. Department for Digital, Culture, Media & Sport, *Online Harms White Paper of 8 April 2019*, in : UK Government Home Office (https ://www.gov.uk/), London 2019, p. « https://www.gov.uk/government/consultations / online - harms - white - paper / online - harms - white - paper » (05/08/2019).

585. Castets-Renard, *Quelle protection des données personnelles en Europe ?*, p. 36.

tion d'établissement dans un pays n'est pas limitée à la présence d'une entité juridique dans ce pays. La Cour relève que la présence d'un seul représentant peut suffire, dans certaines circonstances, pour constituer un établissement, si ce représentant agit avec un degré de stabilité suffisant à la fourniture des services concernés dans l'État membre en question. De plus, la Cour précise que la notion d'« établissement » s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable [586].

La notion d'« établissement » est donc interprétée de façon particulièrement souple par la CJUE. Les autorités de protection des données nationales bénéficieront ainsi d'une grande liberté d'action envers les entreprises enregistrées dans un autre État membre, mais agissant sur leur territoire. Avec le mécanisme du guichet unique mis en place dans le Règlement, la protection des données personnelles des citoyens européens dans le cas des affaires transnationales semble devenir une priorité des autorités. 706

L'innovation majeure du Règlement européen réside dans son application extraterritoriale. En effet, le Règlement s'applique aux traitements de données à caractère personnel relatives à des personnes concernées qui se trouvent **sur le territoire de l'union** par un responsable du traitement ou un sous-traitant **qui n'est pas établi dans l'union**, lorsque les activités de traitement sont liées [587] : 707

(a) « à l'offre de biens ou de services à ces personnes concernées dans l'union, qu'un paiement soit exigé ou non desdites personnes ; ou

(b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'union ».

Le champ d'application extraterritorial du Règlement constitue l'une des plus importantes modifications matérielle de la réforme [588]. 708

« Le présent règlement s'applique au traitement des données a caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : 709

586. Arrêt de la CJUE du 1 octobre 2015, *Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, ECLI :EU :C :2015 :639, consid. 41.
587. art. 3, al. 2 RGPD.
588. Simitis Spiros / Hornung Gerrit / Döhmann Spiecker Indra (édit.), *Datenschutzrecht : DSGVO mit BDSG*, 1e éd., Baden-Baden 2018, p. 266, point I.3.

(a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

(b) au suivi du comportement de ces personnes, dans la mesure où

il s'agit d'un comportement qui a lieu au sein de l'Union ».

710 Ainsi, si une entreprise suisse, établie en-dehors de l'UE, en Suisse, offre des biens ou des services via une boutique en ligne, ou suit le comportement de ses clients dans l'UE par le biais de cookies en ligne, afin de leur proposer des offres personnalisées (ex. : suivi de la navigation sur internet), alors le Règlement européen s'applique. (art. 3, al. 2 RGPD).

711 Exemple : une entreprise basée en Suisse vend des meubles à des personnes domiciliées en France, Italie, Espagne, et Grèce par le biais d'une boutique en ligne. Le RGPD est applicable car la société suisse offre des biens à des personnes dans l'Union.

712 Afin de vérifier l'intention du responsable du traitement, il faut identifier un faisceau d'indices. Ainsi « l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue, la mention de clients ou d'utilisateurs qui se trouvent dans l'Union » sont des éléments laissant penser « que le responsable du traitement envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union » (consid. 23 RGPD).

713 La CJCE retient comme faisceaux d'indices valables « la mention d'un numéro de téléphone avec un indicatif téléphonique international, la description de l'itinéraire d'un État membre au lieu où le service est offert (ex. un hôtel suisse indiquant l'itinéraire à emprunter depuis l'étranger), la mention sur le site internet d'une clientèle internationale domiciliée dans divers États membres de l'Union, l'utilisation d'un domaine internet de premier niveau autre que celui de l'État membre où le service est offert (ex. le site www.exemple.ch sera également accessible sous www.exemple.fr et www.exemple.eu) [589] ». La Cour de Justice, dans un arrêt Rundfunk [590]

589. Arrêt de la CJUE du 7 décembre 2010, *Pammer et Hotel Alpenhof*, Affaires jointes C-585/08 et C-144/09, ECLI :EU :C :2010 :740.

590. Arrêt CJUE du 13 décembre 2007, *Bayerischer Rundfunk et autres contre*

considéra que la publication précise des données relatives au revenu d'un agriculteur sur un site internet constituait une interférence avec les droits consacrés aux art. 7 et 8 de la Charte des droits fondamentaux de l'UE.

Il s'agit donc d'un aspect important à prendre en considération par les responsables du traitement. Un test en ligne est disponible pour aider les entreprises suisses à déterminer, au cas par cas, si le Règlement est ou non applicable [591]. 714

Par exemple, « la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention ». 715

Le critère retenu est celui du « ciblage ». Dès qu'une personne se trouve sur le territoire de l'UE, ses données personnelles sont protégées. Le Préposé fédéral adopte une approche restrictive du cadre juridique en retenant que « dès qu'un résident européen, peu importe sa nationalité ou son lieu de domicile, est directement visé par un traitement de données, le Règlement s'applique ». Or le statut de résident est un statut spécifique octroyé en fonction du nombre de jours passés sur le territoire d'un État et ayant des incidences dans le domaine fiscale. 716

Quant au suivi de comportement, il fait référence à une activité de profilage d'une personne physique, « afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ». Le profilage repose en principe sur des cookies ou de proxys dans le but de personnaliser la publicité envoyée à la personne concernée. Il s'agit de la publicité comportementale : « elle repose sur l'observation du comportement des individus au fil du temps. Elle vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.) pour établir un profil spécifique et proposer 717

GEWA - Gesellschaft für Gebäudereinigung und Wartung GmbH., C-337/06, ECLI :EU :C :2007 :786, consid. 64.

591. Economiesuisse, *Les règles de protection des données "Online Check"*, in : Economiesuisse (https://www.economiesuisse.ch/), Genève s.a., p. « https://www.economiesuisse.ch/fr/datenschutz-online-check » (07/06/2019).

aux personnes concernées des publicités adaptées à leurs centres d'intérêt ainsi déduits » (Groupe de travail de l'Article 29, WP 171, 00909/10/FR).

718 Exemple : Un restaurateur établit des profils de ses clients espagnols, français, et belges afin de leur proposer des offres pour d'autres visites, le RGPD sera applicable pour autant que le profil soit établi sur la base d'un suivi de comportement dans l'UE [592].

719 Le législateur européen exige ainsi de toute entreprise multinationale (suisse, américaine, asiatique…) traitant des données à caractère personnel de personnes « se trouvant sur le territoire de l'UE », qu'elles appliquent les mêmes règles contraignantes que les entreprises européennes concurrentes.

720 Il n'est pas explicitement indiqué que le Règlement s'applique aux résidents uniquement.

721 Le Préposé fédéral rappelle avec justesse que « le RGPD n'est pas directement applicable aux entreprises suisses. Toutefois, certains traitements de données peuvent être concernés, de sorte que les dispositions pertinentes s'appliquent. Les entreprises suisses peuvent donc être directement concernées [593] ».

722 La mise en œuvre du Règlement en-dehors de l'UE, comme en Suisse par exemple, pose des problèmes spécifiques. Les mécanismes de contrôle de l'art. 3 RGPD ne sont pas applicables de manière générale en Suisse. Les droits des personnes concernées ne sont pas identiques entre l'UE et la Suisse. Le droit d'introduire des recours et les prérogatives des autorités de contrôle diffèrent entre la Suisse et les États membres de l'UE.

723 Il est probable que la définition de la notion du « suivi du comportement de ces personnes » fasse l'objet de discussions voire d'un contentieux compte tenu des enjeux pour les pays ne faisant pas

592. PFPDT, *Le RGPD et ses conséquences sur la Suisse*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2018, p. « https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf.download.pdf/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf » (07/12/2019).

593. PFPDT, *Conseils pratiques concernant le RGPD*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2019, p. « https://www.edoeb.admin.ch/edoeb/fr/home/actualites/rgpd-last-minute.html » (26/03/2020).

partie ni de l'Union européenne ni de l' espace économique européen, ce qui est le cas de la Suisse.

« Il existe un suivi du comportement lorsque des personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données qui consistent en un profilage, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit [594]». 724

Le responsable du traitement sera considéré comme ayant l'intention d'offrir des biens ou des services à des personnes dans l'UE, en présence de certains indices spécifiques. Concrètement, l'utilisation d'une langue ou d'une monnaie d'usage courant dans des États de l'UE, l'utilisation d'un nom de domaine autre que celui du pays dans lequel se trouve la société (« **fr** » ou « **eu** »), le recours à des publicités ou des offres spécifiques pour les pays de l'UE constituent des éléments indiquant l'application du Règlement européen [595]. 725

Le Règlement précise que « peu importe que le traitement ait lieu dans l'Union ou non » (art. 3, al. 1 RGPD). Cela signifie que les données personnelles de la succursale peuvent être traitées sur un Cloud suisse. D'où l'intérêt pour la Suisse d'assurer un niveau de protection équivalent au droit européen pour conserver l'attrait de l'hébergement des données en Suisse et la compétitivité économique du pays. La responsabilité étant en outre conjointe entre le responsable du traitement et le sous-traitant en cas de litige, les responsables des traitements établis dans l'UE, choisiront un sous-traitant offrant des garanties de fiabilité. La législation joue donc un rôle clef dans le choix des sous-traitants pour limiter les risques de contentieux et de réputation en cas de litige (ex. : vol de données). Il est donc fortement recommandé d'harmoniser la législation suisse sur le Règlement européen pour favoriser l'activité économique en lien avec l'hébergement de données en Suisse. 726

La localisation du public cible constitue le critère prioritaire. La localisation effective du traitement importe peu [596]. Le Règlement eu- 727

594. Consid. 24 RGPD.
595. Consid. 23 RGPD ; Arrêt CJUE, *Weltimmo c. NAIH*, C-230/14, consid. 41, confirmé par CJUE *Hotel Alpenhof c. Heller*, C-585/08, consid. 93.
596. Fanti Sébastien, *Le nouveau règlement général sur la protection des données et la Suisse : le noeud gordien de la double régulation et le fragile substrat légis-*

ropéen présente donc un caractère extra-territorial (arrêt Google Street View) [597].

728 En Suisse, dès lors que certains traitements entrent dans le champ d'application de l'art. 3 al. 2 RGPD, deux cadres juridiques peuvent être applicables : la LPD et le RGPD.

729 Examinons en particulier, la situation du sous-traitant :

730 Lorsque le sous-traitant est établi dans l'Union européenne, le Règlement s'appliquera d'office, que le traitement ait lieu dans l'Union européenne ou non.

731 Le Règlement s'applique-t-il si le responsable du traitement se trouve en dehors de l'Union européenne et que le sous-traitant se trouve au sein de l'Union européenne ? Dans cette situation, le Règlement s'applique car le traitement a lieu au sein de l'UE. Lorsque le sous-traitant se trouve dans l'UE, le Règlement est appliqué dans son intégralité, aussi bien pour le sous-traitant que pour le responsable du traitement.

732 Si le sous-traitant est établi en dehors de l'Union européenne, le Règlement va s'appliquer au traitement de données de personnes concernées qui sont dans l'Union européenne lorsque les activités de traitement concernent l'offre de biens ou services à cette personne ou lorsque les activités de traitement concernent la surveillance des comportements de ces personnes pour autant que ce comportement a lieu au sein de l'Union européenne.

733 Exemple : une société chinoise de sous-traitance en marketing direct crée des profils de clients belges, français et luxembourgeois sur instruction de son responsable de traitement belge. Est-il soumis au Règlement ? Oui le Règlement s'applique, sauf pour le pro-

latif, in : Expert Focus : schweizerische Zeitschrift für Wirtschaftsprüfung, Steuern, Rechnungswesen und Wirtschaftsberatung = revue suisse pour l'audit, la fiscalité, la comptabilité et le conseil économique 2017, p. 858 ss.

597. PFPDT, *Arrêt du Tribunal fédéral dans l'affaire Google Street View : Règles en matière de traitement de données personnelles*, in : Le Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2019, p. « https://www.edoeb.admin.ch / edoeb / fr / home / protection - des - donnees / Internet _ und _ Computer / services - en - ligne / google - street - view / arret - du - tribunal - federal - dans - laffaire - google - street - view - - regl.html » (24/03/2018).

filage des clients américains aux États-Unis.

La simple accessibilité du site internet d'une organisation depuis le territoire de l'Union européenne ne suffit cependant pas pour considérer que celle-ci offre des biens ou des services à des personnes concernées se trouvant dans l'Union européenne. En revanche, des éléments tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs pays de l'Union européenne, avec la possibilité de commander des biens ou services dans cette langue, ou la référence sur le site internet à des clients ou utilisateurs établis dans l'Union européenne, peuvent constituer des indices que des biens ou services sont proposés à des personnes concernées dans l'Union européenne. 734

En résumé : Le Règlement s'applique aux données à caractère personnel concernant les personnes domiciliées dans l'Union européenne [598] tout citoyen européen ou non européen résident sur le territoire de l'Union européenne sera concerné par le Règlement. 735

Tous les traitements dont la finalité et les moyens ont été définis dans le cadre des activités d'un établissement situé au sein de l'Union européenne sont soumis au Règlement [599]. 736

Les traitements visés sont ceux du responsable du traitement et du sous-traitant. Le critère est celui de la décision effective et peu importe que le traitement ait lieu ou non dans l'union [600]. 737

Les traitements de données personnelles enregistrés sur une Blockchain soulèvent des questions spécifiques dans le cadre du champ d'application territorial du Règlement européen. Comme le souligne Michèle Finck [601], les blockchains fonctionnent par le biais de nœuds situés dans de multiples juridictions. Le Règlement européen s'applique aux responsables du traitement qui disposent d'un établissement situé dans l'UE, même lorsque le traitement est situé en-dehors de l'Union européenne (art. 3. 1 RGPD). Il s'applique également aux responsables du traitement qui sont situés en-dehors de l'UE, mais qui vendent des biens ou des services dans l'UE ou qui effectuent un suivi de comportement de personnes situées dans l'UE (art. 3 al 2 a et b RGPD). Enfin, le Règlement européen s'applique 738

598. Bensoussan, *Règlement européen sur la protection des données (1^e éd.)* p. 8.
599. art. 3, al. 1 RGPD.
600. Consid. 22 RGPD.
601. Finck, *Blockchains and Data Protection in the EU*, p. 27.

au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'union, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public (art. 3, al 3 RGPD). Le Règlement peut s'appliquer à des traitements de données personnelles lorsque les données sont stockées sur la Blockchain, et ont un lien indirect avec l'UE [602].

739 Dans le cadre de l'analyse du champ territorial du Règlement européen appliqué à la Blockchain, se pose la question de savoir comment mettre en œuvre les dispositions relatives aux transferts de données vers des pays tiers.

740 L'élément d'extranéité appartient par essence à la Blockchain. Or, le Règlement européen contient des dispositions spécifiques pour les transferts vers des pays tiers au chapitre V. Les données stockées dans des blocs sont hashées par un mineur qui peut-être situé dans n'importe quelle juridiction. L'article 49, al. 1 a RGPD pourrait trouver application. « La personne concernée donnerait son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées [603]». Même si la Suisse dispose d'une décision d'adéquation avec l'UE, il apparaît raisonnable d'informer la personne concernée des risques potentiels dérivant d'un transfert de données personnelles dans le cadre d'une activité effectuée par le biais de la Blockchain. Le Règlement européen est avant tout conçu pour la collecte, le stockage et le traitement centralisé des données personnelles. Il ne peut pas être aisément transpose à la Blockchain qui offre un système par nature décentralisé [604].

§4 Les définitions

741 Les définitions (art. 4 RGPD) s'inscrivent dans la continuité de la directive 95/46/CE. Certaines ont été complétées et modernisées. D'autres sont nouvelles. C'est le cas des notions de pseudonymisation, de profilage, de données biométriques ou génétiques ou de

602. Finck, *Blockchains and Data Protection in the EU*, p. 27.
603. art. 49 RGPD.
604. Finck, *Blockchains and Data Protection in the EU*, p. 28.

violation de données à caractère personnel [605].

Le législateur a choisi de respecter le principe de la neutralité technologique [606]. Ce concept de neutralité technologique est louable dans sa philosophie, mais pose problème en pratique. Certaines architectures, comme la Blockchain, permettent en effet une traçabilité de chaque transaction, et rendent impossible l'effacement des données, ce qui rend impossible en pratique la protection de la sphère privée et l'exercice de certains droits, comme le droit à l'oubli. Pour cette technologie, le Règlement apparaît sur certains points inapplicable. 742

I. Les données personnelles (article 4, al. 1 du Règlement)

Le Règlement définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Les données personnelles doivent faire référence à une personne physique. Il s'agit d'une nouveauté du Règlement. 743

Est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique (nouveauté de la version finale), psychique, économique, culturelle ou sociale [607]. Sur cette base, toutes les informations qui peuvent être reliées à un identifiant technique, peuvent être qualifiées de données à caractère personnel [608]. 744

Les identifiants numériques et les données de localisation sont considérées comme des données à caractère personnel. 745

Il existe désormais *trois* catégories de données à caractère personnel : 746

- Les données particulières (données sensibles) [609] ;
- Les données relatives aux infractions et mesures de sécurité ; et

605. Docquir, *Vers un droit européen de la protection des données ?*, p. 92.
606. Sydow / Kring, *Die Datenschutzgrundverordnung*, pp. 271-276.
607. Consid. 2-29 et consid. 38.
608. Weber, *Datenschutz*, p. 619.
609. Consid. 10 RGPD.

— Les autres données soumises à un principe de finalité spécifique.

747 Les données sensibles concernent :

— « l'origine raciale ou éthnique ;

— les opinions politiques ;

— les convictions religieuses ou philosophiques ;

— l'appartenance syndicale ;

— les données génétiques ;

— les données biométriques aux fins d'identifier une personne physique ;

— les données concernant la santé ; et

— les données concernant la vie ou l'orientation sexuelle [610] ».

748 Les données sensibles (art. 9 RGPD), les données d'enfants mineurs (art. 8 RGPD) ou encore les données des collaborateurs bénéficient de droits renforcés [611]. Ces droits peuvent être exercés par le biais d'une action collective au sein de l'UE ce qui contribue à la responsabilisation des acteurs et à une pesée des intérêts en présence.

749 Analysons de manière critique le Réglement. Celui-ci analyse la finalité du traitement pour en déduire son caractère ou non sensible. Le RGPD examine la finalité du traitement a priori mais les technologies d'IA rendent pertinentes un contrôle de la finalité du ciblage a posteriori [612]. Pour Yves Poullet, dont nous partageons l'analyse, c'est l'usage des données et non pas la nature intrinsèque de celles-ci qui prime [613]. Du fait des technologies digitales, un ciblage des personnes en fonction de critères spécifiques, comme la race, la religion ... ou l'état de santé peut être source de discriminations [614]. Le Conseil de l'Europe a souligné que le « contexte du traitement

610. art. 9 RGPD.

611. Article 29 Data Protection Working Party, *Opinion 02/2017 of Article 29 Data Protection Working Party on Data Processing at Work - Adopted on 8 June 2018 (WP 249)*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 » (06/12/2018).

612. Poullet Yves, *La vie privée à l'heure de la société du numérique*, 1e éd., Bruxelles 2019, p. 130.

613. *Idem*, p. 112.

614. *Idem*, p. 112.

était déterminant [615]». Il peut en effet augmenter le risque pour la personne concernée et justifier un cadre juridique spécifique et une protection accrue.

II. Le traitement (article 4, al. 2 du Règlement)

Le Règlement définit le traitement comme « toute opération ou tout ensemble d'opérations effectués ou non à l'aide de procédés automatisés et appliqués à des données personnelles, ou des ensembles de données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou a modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction ». 750

Constitue ainsi un traitement « toute opération en lien avec des données à caractère personnelle [616]». Cette notion suppose toutefois un comportement actif de la part du responsable du traitement [617]. 751

De concert avec la notion de données à caractère personnel, la qualification de traitement constitue la condition fondamentale à l'application du droit de la protection des données, selon les articles 2, al. 1 et 3, al. 1 du Règlement. Ces deux notions de données et de traitement sont très larges. Par conséquent, le Règlement sera applicable à toute forme d'opération automatisée ou non, en lien avec des informations à caractère personnel [618]. 752

En principe, le traitement de données sensibles est interdit. Par exception, un traitement de données sensibles est autorisé dans un cadre pré-défini (art. 9 RGPD). A titre d'exemple, des données sensibles pourront être traitées avec le consentement explicite de la personne concernée. Les traitements des données sensibles doivent être effectués sous le contrôle de l'autorité de contrôle compétente 753

615. Rapport explicatif de la Convention 108 du Conseil de l'Europe, consid. 59 et 60, p. 25.
616. Wybitul Tim / Bausewein Christoph, *EU - Datenschutz - Grundverordnung : Handbuch*, 1e éd., Frankfurt am Main 2017, p. 207.
617. *Ibidem.*
618. *Idem*, p. 208.

dans le domaine de la protection des données.

754 En Suisse, dans son arrêt du 19 mars 2019 [619], le Tribunal administratif fédéral a qualifié d'illicite la collecte de données au moyen de l'application Helsana+, faute de consentement valable des assurés à la communication de données personnelles, provenant de l'assurance-maladie obligatoire, à des tiers. Le consentement à la collecte de données relatives à l'assurance obligatoire obtenues auprès de sociétés sœurs n'est pas valable car les conditions plus restrictives applicables aux organes fédéraux sont applicables. En revanche, Helsana peut se prévaloir du consentement valable des personnes concernées pour le traitement de données personnelles obtenues directement auprès de ces personnes, car elle agit en tant que personne privée. L'entreprise Helsana doit remédier aux lacunes constatées par le tribunal. Pour le Préposé, « le respect du principe de la transparence exige en particulier que des progrès soient faits en ce qui concerne l'utilisation et la protection des données. Les participants au programme de bonus Helsana+ doivent pouvoir comprendre aisément et sans ambiguïté quels traitements de données ils autorisent et leur autorisation doit se limiter à ce qui est effectivement nécessaire, conformément au principe de la proportionnalité [620]. Le Tribunal administratif fédéral relève également qu'un organe fédéral ne peut demander l'autorisation de communiquer des données à des tiers que dans un seul cas d'espèce [621] ».

755 Il faut souligner que la collecte des données doit respecter des principes spécifiques [622].

- « Licéité [623] ;
- Loyauté ;
- Transparence ;
- Finalité explicite avec une limitation desdites finalités ;
- Adéquation, pertinence et non-excessivité ;

619. TAF, 19.03.2019, A-3548/2018, consid. 4.8.4.
620. EDPS, *EDPS Guidelines on assessing the proportionality*, p. 6 ss.
621. Conseil fédéral, *Helsana+ : Le jugement entre en force*, in : Le Conseil fédéral (https ://www.admin.ch/), Berne 2019, p. « https : / / www . admin . ch / gov / fr / accueil / documentation / communiques . msg - id - 75039 . html » (17/05/2019) ; Schürch Simone, *Le programme Helsana+ (2/2)*, in : LawInside (http : //www.lawinside.ch/), Zürich 2019, p. « http://www.lawinside.ch/748/ » (29/12/2019).
622. art. 5 RGPD.
623. art. 6 RGPD.

— Minimisation des données personnelles ;

— Exactitude et pertiennce ; et

— Limitation de la durée de conservation ».

« Une cartographie détaillée des activités de traitements doit être préparée par le responsable du traitement [624] pour avoir une vision d'ensemble des données à caractère personnel et de leur niveau de risques, pour protéger les données personnelles de manière appropriée conformément au Règlement [625]». 756

III. Le profilage (article 4, al. 4 du Règlement)

Le profilage se définit comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique [626]». 757

Le législateur européen a reconnu le profilage comme un traitement présentant un risque pour les droits et libertés fondamentales des individus. Le profilage rend en effet possible le suivi de comportement des individus en temps réel et requiert une protection adaptée [627]. La reconnaissance du profilage constitue une nouveauté du Règlement [628]. 758

624. art. 30 RGPD.
625. Skouma Georgia / Léonard Laura, *Les grands changements liés à la règlementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professonnels*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 425.
626. art.4, al. 4 RGPD.
627. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 209.
628. *Ibidem* ; Poullet Yves / Frenay Benoît, *Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe » (T-PD(2019)07)*, in : Conseil de l'Europe (https ://www.coe.int/), Strasbourg 2019, p. « https://rm.coe.int/rapport-et-propositions-de-recommandations-sur-le-profilage-et-la-conv/1680973672 » (07/12/2019).

IV. La pseudonymisation (article 4, al. 5 du Règlement)

759 La pseudonymisation est « le traitement de données à caractère personnel effectué de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable [629] ».

760 « Cela signifie que l'individualisation de la personne est rendue impossible sans complément d'information [630] ». « Cette individualisation nécessite des mesures techniques et organisationnelles pour empêcher la mise en relation avec ces informations complémentaires permettant d'identifier ou de rendre la personne physique identifiable [631] ». Ces informations complémentaires devront donc être « protégées et contrôlées [632] ».

761 « La notion de pseudonymisation est à différencier de la notion d'anonymisation [633] ». Cette dernière ne figure pas dans le Règlement [634].

762 « La pseudonymisation fait partie des éléments de sécurité du traitement [635] ». Elle consiste à séparer les caractéristiques d'une personne physique de son identification tout en conservant la globalité de ces données [636]. La documentation de la pseudonymisation permet au responsable du traitement de démontrer le respect du principe de minimisation des données, et son comportement diligent en cas de violation des données à caractère personnel (ex. : faille de sécurité). Une fois le traitement effectué, le responsable du traitement peut décider de pseudonymiser les données, afin de

629. art. 26-29 RGPD.
630. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 209.
631. Troncoso Carmela, *Privacy & Online Rights Knowledge Area*, in : The Cyber Security Body of Knowledge (https ://www.cybok.org/), Bristol 2019, p. 9.
632. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 209.
633. Consid. 26, al. 5 et 6 RGPD. La question de la valeur contraignante du consid. 26, al.5 du Règlement se pose.
634. art. 4, al. 5 RGPD et consid. 26-29 RGPD.
635. art. 32, al. 1 RGPD ; Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p 210.
636. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 20.

démontrer la limitation des finalités du traitement. Il s'agit d'une méthode qui peut être valablement utilisée pour le traitement de données à des fins d'archivage, de recherches scientifiques, historiques ou statistiques [637]. Elle constitue une des mesures techniques et organisationnelles imposées par le Règlement.

763 Du fait de la réversibilité potentielle de la pseudonymisation, la charge de la preuve incombe au responsable du traitement qui doit garantir que les données ne peuvent être rapprochées de la personne physique en cause. En cas de suppression de la réversibilité, les données deviennent anonymes et sortent du champ d'application du Règlement [638]. La question se pose de savoir s'il ne faudrait pas étendre la protection à l'usage des données anonymes [639] du fait de la ré-identification possible de ces données et du caractère obsolète de l'anonymisation au temps des Big Data [640].

764 À titre d'exemple, une adresse IP est une donnée pseudonyme pour un commerçant en ligne, dans la mesure où l'identification de la personne reliée à cette adresse ne peut être obtenue que sur une décision de justice. De même l'anonymisation de données au moyen d'un numéro d'identification dont la relation avec une personne physique est détenue par un tiers de confiance qui s'interdit par contrat de révéler l'identité, constitue un procédé opérationnel de pseudonymisation [641].

765 En revanche, un procédé de chiffrement qui organise la confidentialité des données ne correspond pas à une technique de pseudonymisation si les clefs de chiffrement et de déchiffrement sont sous la maîtrise du responsable du traitement lors d'un transfert transfrontalier ou d'une assistance administrative [642].

766 « La peudonymisation des données sera un élément pour déterminer si le traitement est licite ou non [643]». Ainsi dans l'hypothèse d'une modification de la finalité du traitement, « la pseudonymisation sera interprétée en faveur de la licéité du traitement ». La

637. art. 89, al. 1 RGPD.
638. art. 11, al. 1 RGPD.
639. Poullet, *La vie privée à l'heure de la société du numérique*, p. 107.
640. Rouvroy Antoinette, *Homo juridicus est-il soluble dans les données ?*, in : Degrave Elise (édit.), *Law, norms and freedoms in cyberspace : liber amicorum Yves Poullet*, 1e éd., Bruxelles 2018, p. 428.
641. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 21.
642. *Ibidem.*
643. Härting, *Datenschutz-Grundverordnung*, p. 78.

pseudonymisation fait partie des méthodes, que le responsable du traitement peut utiliser pour mettre en œuvre le Privacy-by Design [644]. D'autres méthodes comme les Privacy-Enhancing technologies peuvent être utilisées [645].

767 En revanche, le Règlement n'est pas applicable lorsque les données sont anonymisées. Le responsable du traitement demeure cependant responsable du traitement, en particulier si les données sont ré-identifiables ultérieurement ou font l'objet d'une violation de données ultérieure.

768 La recherche a démontré en 2015, que seuls 3 éléments suffisaient pour ré-identifier un individu du fait de son unicité [646]. Par conséquent, ni les techniques de pseudonymisation ni les techniques d'anonymisation n'offrent de garanties suffisantes pour s'assurer d'une confidentialité effective des traitements.

V. La notion de fichier (article 4, al. 6 du Règlement)

769 Un fichier est défini comme « tout ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

770 Il ressort de cet article que le fichier doit avoir une structure spécifique. La collecte de données à caractère personnel doit en outre être accessible selon des critères définis [647].

VI. Le responsable du traitement (article 4, al. 7 du Règlement)

771 Le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme, qui seul ou conjointement avec d'autres, détermine les finalités et les moyens

644. art. 25, al. 1 RGPD et aussi Ervik Sara, *Privacy by Design applied in Practice and the Consequences for System Developers*, thèse, Stockholm 2019, pp. 1-47.
645. Troncoso, *Privacy & Online Rights*, p. 21.
646. de Montjoye, *Unique in the Crowd*, p. 1376 ; Weber / Staiger, *Transatlantic Data Protection in Practice*, p. 52.
647. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 211.

du traitement [648]».

S'agissant de l'identification du responsable de traitement, une analyse au cas par cas, doit être menée pour tout traitement mis en œuvre, dans la mesure où cette notion est centrale : il s'agit de l'entité sur laquelle repose les principales obligations, en matière de protection des données à caractère personnel [649]. Comment définir quelle entité doit être qualifiée de responsable du traitement ? Les critères suivants pourront être utilisés : « initiative du traitement et définition de la finalité / des objectifs, influence de droit ou de fait sur le traitement et degré d'influence, autonomie et pouvoir décisionnaire, image donnée aux personnes concernées et attentes raisonnables que cette visibilité peut susciter chez ces dernières, détermination des moyens matériels, humains, techniques et organisationnels du traitement [650]». 772

Pour Tim Wytibul, le responsable du traitement est la personne juridique qui décide du traitement de donnnées à caractère personnel [651]. La notion de responsabilité est selon lui inséparable de la notion de traitement [652]. Il s'ensuit selon ce raisonnement qu'il existe un responsable pour chaque traitement [653]. La formulation « seule ou conjointement avec d'autres » donne la possibilité d'une responsabilité collective [654]. 773

Deux acteurs économiques peuvent également être qualifiés de responsables conjoints du traitement, lorsqu'elles déterminent les finalités et les moyens d'un traitement de données à caractère personnel. La CJUE a retenu que Facebook et l'administrateur d'une page hébergée sur le réseau social pouvaient être qualifiés de responsables conjoints du traitement de données personnel des visi- 774

648. art. 4, al. 7 RGPD ; Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016.*
649. Docquir, *Vers un droit européen de la protection des données ?*, p. 16.
650. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016*, pp. 1-88.
651. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 212.
652. *Ibidem.*
653. *Ibidem.*
654. *Ibidem.*

teurs de la page [655].

775 La notion de responsable du traitement a été précisée par la jurisprudence. Ainsi l'arrêt « Google contre Espagne [656] », qualifie de responsable du traitement les moteurs de recherche, « qui ont une activité d'indexation des données (y compris personnelles) disponibles sur le web ». Pour la CJUE, « l'enregistrement ou encore la conservation de données personnelles constituent des traitements ». De même, la « communication de données à caractère personnel constitue un traitement de données [657] ».

776 La Cour a en outre indiqué que si internet est utilisé pour générer des données, alors le traitement peut-être qualifié de traitement automatisé : « [...] il convient de relever que faire apparaître des informations sur une page Internet implique, selon les procédures techniques et informatiques appliquées actuellement, de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à internet. Ces opérations sont effectuées, au moins en partie, de manière automatisée [658] ».

VII. Le sous-traitant (article 4, al. 8 du Règlement)

777 Le sous-traitant se définit comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement [659] ».

778 La définition du sous-traitant est inséparable de la notion de responsable du traitement [660]. Le sous-traitant est impliqué dans le traitement des données à caractère personnel, sans qu'il ne décide ni des finalités ni des moyens du traitement des données à caractère

655. Arrêt CJUE du 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI :EU :C :2018 :388 ; Métille Sylvain / di Tria Livio, *Protection des données : responsabilité croissante ?*, in : Expert Focus 2019 2019/4, p. 308.
656. Arrêt CJUE du 8 avril 2014, *Google contre Espagne*, C—131/12, ECLI :EU :C :2014 :317, consid. 2.
657. CJUE 4 mai 2017, *Rigas Satiksme*, C—13/16, consid. 26.
658. CJCE 6 novembre 2003, *Lindqvist*, C-101/01, consid. 26.
659. Voir également l'art. 28 RGPD pour un complément.
660. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 214.

personnel [661].

Le Règlement présente le sous-traitant comme un partenaire du responsable du traitement [662]. Cependant, le contrôle du traitement et sa maîtrise demeurent de la compétence du responsable du traitement. 779

Il en découle que le contrat entre le responsable du traitement et le sous-traitant est de toute première importance. 780

VIII. Le représentant (article 4, al. 17 du Règlement)

Le Règlement introduit une nouvelle notion, celle de « représentant [663] » comme « toute personne physique, ou morale, établie dans l'Union européenne, désignée par le responsable du traitement ou le sous-traitant par écrit, qui les représente en ce qui concerne les obligations de chacun en vertu du présent Règlement ». 781

Par conséquent, si le représentant est établi en-dehors de l'Union européenne, celui-ci n'est pas concerné par l'application du Règlement, sauf si sa législation en dispose autrement (ex. : législation reconnue comme adéquate). 782

Le considérant 80 précise que « le représentant devrait agir pour le compte du responsable du traitement ou du sous-traitant et peut être contacté par toute autorité de contrôle. Le représentant devrait être expressément désigné par un mandat écrit du responsable du traitement ou du sous-traitant pour agir en son nom en ce qui concerne les obligations qui lui incombent en vertu du présent Règlement. La désignation de ce représentant ne porte pas atteinte aux responsabilités du responsable du traitement ou du sous-traitant au titre du présent Règlement ». Ce représentant devrait accomplir ses tâches conformément au mandat reçu du responsable du traitement ou du sous-traitant, y compris coopérer avec les autorités de contrôle compétentes en ce qui concerne toute action entreprise pour assurer le respect du présent Règlement. Le représentant désigné devrait faire l'objet de procédures coercitives en cas de non-respect du présent Règlement par le responsable du traitement 783

661. *Idem*, pp. 426-457.
662. *Idem*, pp. 426-457.
663. art. 27 RGPD.

ou le sous-traitant [664].

784 L'obligation de désigner un représentant ne s'applique pas « lorsque le traitement est occasionnel, n'implique pas un traitement, à grande échelle, de catégories particulières de données à caractère personnel ou le traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions, et est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement. Le responsable du traitement ou le sous-traitant ne doit pas non plus désigner de représentant, s'il s'agit d'une autorité publique ou d'un organisme public [665] ».

785 En pratique, si le responsable du traitement ou le sous-traitant établi en Suisse, remplissant les conditions de l'art. 3, al. 2 RGPD, n'a pas désigné de représentant dans l'UE, le Préposé à la protection des données sera compétent pour trancher un litige. Dans le cadre des administrations fédérales comme les écoles polytechniques, il n'existe aucune obligation de désigner un représentant dans l'UE. Les personnes concernées par un traitement de données en violation du RGPD pourront certes saisir une autorité de contrôle dans l'UE en plus du Préposé fédéral en Suisse, mais en pratique, la question de l'effectivité de la sanction sur une administration fédérale d'un État tiers reste entière. Cette carence dans la mise en oeuvre effective des décisions et exécution des sanctions pour certains responsables du traitement ou sous-traitants d'un État tiers soulève des questions essentielles en lien avec la confiance dans la protection juridictionnelle effective des personnes concernées dont les données personnelles, parfois sensibles, sont traitées.

786 Pour le cabinet d'avocat Ledieu, le rôle du représentant dans l'UE d'un prestataire situé en-dehors de l'UE sera de garantir la conformité au Règlement, pour le compte du prestataire hors UE. La question de l'existence d'un for dans l'UE mérite d'être soulevée. Le représentant étant le point de contact des autorités de contrôle (cf. article 58 RGPD) et des personnes concernées, sur les questions en lien aux traitements de données à caractère personnel, il apparaît cohérent de reconnaître un for à l'adresse du représentant. Le représentant pourra en effet faire l'objet de procédures coercitives, en cas de non-respect du présent règlement, par le responsable du

664. Consid. 80 RGPD.
665. art. 27 RGPD.

traitement ou le sous-traitant. Le responsable du traitement ou le sous-traitant demeure responsable à l'égard des autorités et des personnes concernées [666].

Le projet de Règlement e-privacy [667] prévoit également d'imposer la désignation d'un représentant dans l'union à tous les fournisseurs de services électroniques, situés hors UE. 787

IX. Le destinataire (article 4, al. 9 du Règlement)

Le destinataire est défini comme « la personne physique, ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ». 788

Cette définition est très large et toutes les catégories de personnes physiques ou morales recevant des données à caractère personnelles peuvent être qualifiées de « destinataires [668]». 789

Une exception concerne les autorités publiques, auxquelles « des données à caractère personnel sont communiquées conformément à une obligation légale pour l'exercice de leurs fonctions officielles ». Il s'agit des administrations fiscales, douanières, les cellules d'enquêtes financière, les autorités administratives indépendantes, ou les autorités des marchés financiers. Elles ne devraient pas être considérés comme des destinataires, si elles reçoivent des données à caractère personnel, qui sont nécessaires pour mener à bien une enquête particulière, dans l'intérêt général, conformément au droit de l'union ou au droit d'un État membre [669]. 790

Le Règlement précise que « les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées, et revêtir un caractère occasionnel, et elles 791

666. Fanti Sébastien, *Le Réseau Lexing offre d'être votre représentant au sein de l'UE conformément au RGPD !*, in : Lexing Switzerland (https ://lexing.ch/), Sion 2019, p. « https://lexing.ch/le-reseau-lexing-vous-offre-de-vous-representer-au-sein-de-lue-dans-le-cadre-du-rgpd/ » (30/06/2019).

667. European Commission, *Proposal for a Regulation on Privacy and Electronic Communications*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications » (26/03/2020) ; Commission européenne, *La Commission propose de resserrer les règles en matière de respect de la vie privée.*

668. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 215.

669. consid. 31 RGPD, et aussi *Ibidem.*

ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers [670]». Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement [671].

X. Le tiers (article 4, al. 10 du Règlement)

792 Le tiers est défini comme « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes, qui placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ».

793 Il ressort de cette définition que le tiers est défini par la négative. Est un tiers toute personne, qui n'est pas personne concernée, responsable du traitement ou sous-traitant et qui n'est pas placée sous la responsabilité immédiate du responsable du traitement ou du sous-traitant [672].

XI. La notion de consentement (article 4, al. 11 du Règlement)

794 Le consentement est l'un des moyens de rendre licite un traitement de données personnelles.

795 La directive 95/46/CE imposait dans son article 7 que « le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement ». Au sens de la directive, le consentement de la personne concernée se comprenait comme toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement [673]. Le Groupe de travail « Article 29 » sur la protection des données a émis un avis en 2011 sur la notion de

670. Consid. 31 RGPD.
671. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 215.
672. *Idem*, p. 216.
673. art. 2 let. h. de la directive 95/46/CE.

consentement [674] sur la définition à donner au consentement.

La définition du consentement dans la directive 95/46/CE a été transposée de manière très hétérogène dans les différents États membres, certains exigeant un consentement explicite, d'autres considérant qu'un consentement implicite était suffisant. 796

Dans le Règlement, un traitement de données ne sera licite que lorsque l'une des conditions de l'article 6 RGPD est remplie, notamment lorsque la personne concernée a donnée un consentement valide au traitement de données la concernant. A défaut, le principe d'interdiction du traitement de données à caractère personnel prévaut [675]. Le Réglement définit le consentement comme « toute manifestation de la volonté, libre, spécifique, éclairée et univoque, par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement [676]». 797

Le consentement doit être donné de façon indubitable. Le responsable du traitement doit apporter la preuve de celui-ci (art. 7, al.1 RGPD). Le consentement doit être concret, informé et volontaire. Le législateur vise ainsi à faire obstacle au caractère fictif du consentement [677]. 798

Le Règlement impose un consentement exprès. La personne doit avoir été mise devant la nécessité de donner son accord au traitement. Plus précisément, le considérant 32 indique qu'« il ne saurait y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité ». La charge de la preuve pèse sur le responsable du traitement (art. 7, al. 1 RGPD). La personne dont les données sont collectées peut retirer son consentement à tout moment (art. 7, al. 799

674. Groupe de Travail de l'Article 29, *Avis 15/2011 du Groupe de travail de l'Art. 29 sur la définition du consentement - Adopté le 13 juillet 2011 (WP 187)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2011, p. « https : / / ec . europa . eu / justice / article - 29 / documentation / opinion - recommendation/files/2011/wp187_fr.pdf » (26/03/2020).

675. Schneider Jochen, *Datenschutz : nach der EU - Datenschutz - Grundverordnung*, 2e éd., München 2019, p. 160.

676. art. 6, 7 et 8 RGPD.

677. Epiney / Kern, *Zu den Neuerungen im Datenschutzrecht der Europäischen Union*, p. 51 ; Simitis Spiros, *Entwicklung und Dilemmata des Datenschutzes*, in : Epiney Astrid / Hänni Julia / Brülisauer Flavia (édit.), *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, Zürich 2012, p. 6 ss.

3 RGPD).

800 Le consentement consiste en principe en une action. Il ne devrait être donné passivement (ou par une abstention) que pour des cas limités. Pour être valable, aucune pression ne doit avoir été exercée sur la personne concernée pour obtenir son consentement (par ex. un rapport hiérarchique, lien de dépendance, etc.) [678]. Le consentement doit être donné spécifiquement pour un traitement particulier. Il ne peut être donné de manière générale. Aucune exigence formelle n'est requise [679].

801 Le consentement, pour être valable, doit consister en une « déclaration ou un acte positif univoque, ce qui semble exclure un consentement tacite ou purement passif [680] ».

802 Le consentement ne sera pas réputé être donné « librement » si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au traitement de données personnelles, qui ne sont pas nécessaires à l'exécution du contrat ou si la personne concernée ne dispose pas d'une « véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice, en particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement [681] ». Ce sera notamment le cas dans le cadre de relations salariées du fait de l'existence d'un lien hiérarchique entre les salariés et leur employeur.

803 La charge de la preuve incombe au responsable du traitement [682]. Celui-ci doit donc documenter le consentement.

804 Le Groupe de Travail de l'Article 29 considère que « si le consentement est demandé, le responsable du traitement doit renoncer à

678. Gola Peter / Schulz Sebastian, *DS-GVO–Neue Vorgaben für den Datenschutz bei Kindern*, in : Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD 2013, p. 475.
679. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 217.
680. CNIL, *Conformité RGPD : comment recueillir le consentement des personnes ?*, in : Commission Nationale de l'Informatique et des Libertés (https ://www.cnil.fr/), Paris 2018, p. « https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes » (01/01/2020), p. 1.
681. art. 7, al. 4 RGPD et consid. 42 in fine et 43 RGPD.
682. art. 7, al. 1 RGPD.

invoquer une autre justification du traitement [683]».

Le Règlement européen exige que tout traitement repose sur l'un des fondements énumérés à l'article 6 RGPD, en relation avec le considérant 40 RGPD : consentement de la personne concernée (art. 6 al. 1 let. a RGPD), nécessité contractuelle(art. 6 al. 1, let. b RGPD), conformité à l'égard d'une obligation légale d'un État membre ou de l'UE (art. 6 al. 1 let. c RGPD), ou intérêts légitimes du responsable de traitement (art. 6 al. 1 let. f RGPD). Le fondement choisi doit être communiqué pour chaque traitement (art. 13 al. 1 let. c RGPD) à la personne concernée. 805

Le considérant 47 RGPD précise qu'un intérêt légitime pourrait par exemple, exister « lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans les situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service ». La détermination d'un intérêt légitime requiert une évaluation attentive, pour déterminer « si une personne concernée peut raisonnablement s'attendre, à ce que ces données fassent l'objet d'un traitement à une fin donnée [684]». 806

La jurisprudence de la CJUE a précisé que l'intérêt légitime constitue un fondement valable pour « légitimer la collecte de données personnelles qui ne sont pas disponibles publiquement [685]» ou qui sont nécessaire pour la sécurité de leurs systèmes d'information [686]. 807

La pesée des intérêts en présence ressort cependant de la jurisprudence de la CJUE [687], qui se fonde sur l'article 7 let. f de la directive 808

683. Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679 - Adopted on 28 November 2017, Last Revised and Adopted on 10 April 2018 (WP 259 rev.01)*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 » (31/12/2019), consid. 23.

684. Groupe de Travail de l'Article 29, *Avis 06/2014 du Groupe de travail de l'Art. 29 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE - Adopté le 9 avril 2014 (WP 217)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2014, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf » (31/12/2019), p. 70.

685. Arrêt CJUE du 24 novembre 2011, *ASNEF et FECEMD contre Administracion del Estado*, C-468/10 et C–469/10, ECLI :EU :C :2011 :777.

686. Arrêt CJUE du 19 octobre 2016, *Breyer contre Allemagne*, C—582/14, ECLI :EU :C :2016 :779, pts. 63 et 64.

687. Arrêt CJUE du 4 mai 2017, *Rigas Satiksme*, C—13 / 16, ECLI :EU :C :2017 :336,

95/46/CE [688]. Pour la doctrine, cette pesée des intérêts doit être effectuée par le responsable du traitement, tout en communicant de manière transparente avec la personne concernée [689].

809 Le consentement n'est pas systématiquement requis du Règlement. Des exception sont prévues à l'article 6, let. b) à f).

810 En outre, le Règlement prévoit des dispositions spécifiques concernant les mineurs de moins de 16 ans ce qui constitue une nouveauté par rapport à la directive [690].

XII. La violation de données à caractère personnel (article 4, al. 12 du Règlement)

811 Le Règlement définit la violation de données à caractère personnel comme « une violation de la sécurité, entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données a caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données [691] ».

812 Dans cette perspective, il existe un lien entre la violation de données à caractère personnel et la violation de sécurité, qui renvoie à l'obligation d'intégrité (art. 5, al. 1 f) RGPD). L'intégrité est examinée au regard des mesures techniques et organisationnelles prises par le responsable du traitement pour protéger les données à caractère personnel (art. 25 et 32 RGPD) [692].

813 L'article 33 du Règlement précise les obligations de notification de la violation de données à caractère personnel et de la violation de

Arrêt CourEDH du 5 septembre 2017, *Barbulescu contre Roumanie*, Requête n° 61.496/08, consid. 132, ECLI :CE :ECHR :2017 :0905JUD006149608.

688. « [le traitement] est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée [...] ».

689. Lhemery François / Roques-Bonnet Marie-Charlotte, *Peering into the Future of Privacy*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 435.

690. Gola / Schulz, *DS-GVO*, pp. 475-481 et aussi art. 8 RGPD.

691. art. 33 et 34 RGPD et consid. 85 et 87 RGPD.

692. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 218.

sécurité à l'autorité compétente et à la personne concernée.

La notification de la violation de données à caractère personnel à l'autorité compétente doit être faite « dans les meilleurs délais, par le responsable du traitement, si possible 72 heures au plus tard après en avoir pris connaissance [693] ». En cas de doute, il est souhaitable de prévenir l'autorité compétente pour une évaluation du devoir d'information, compte tenu du risque d'amende [694]. 814

La notification doit comprendre « une description de la nature de la violation de données à caractère personnel si possible les catégories et le nombre approximatif de personnes concernées ; communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel les informations peuvent être obtenues ; décrire les conséquences probables de la violation de données à caractère personnel ; décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris les mesures pour en atténuer les éventuelles conséquences négatives » (art. 33 RGPD). 815

Le responsable du traitement doit veiller à « documenter toute violation de données à caractère personnel, en indiquant les faits, les effets et les mesures prises » (art. 33 RGPD). 816

En principe, le responsable du traitement doit également informer la personne concernée de l'existence d'une violation de données à caractère personnel, s'il existe un risque élevé pour les droits et libertés de la personne physique concernée [695]. Cette obligation trouve son fondement dans le principe de transparence reconnu par le Règlement [696]. Cette notification doit pouvoir être comprise par des un non-spécialiste. Elle doit être rédigée en des termes « clairs et simples » qui décrivent la nature de la violation de données à caractère personnel [697]. 817

Par exception, aucune notification n'est nécessaire pour les cas sui- 818

693. art. 33 RGPD. Il importe également de noter que « le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel, dans les meilleurs délais ».
694. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 514.
695. art. 34 RGPD.
696. art. 12 à 15 RGPD.
697. art. 34, al. 2 RGPD.

vants :

- si des mesures techniques de chiffrement ne permettent plus l'identification de la personne concernée (ex. : hachage des données).
- si le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser [698].
- si la notification nécessiterait « des efforts disproportionnés, alors le responsable du traitement privilégie une communication publique permettant à la personne concernée d'être informée de manière tout aussi efficace [699] ».

819 Le responsable du traitement peut être contraint de notifier la personne concernée de la violation de données, par l'autorité de contrôle, « si cette violation est susceptible d'engendrer un risque élevé » pour les personnes concernées [700].

820 Toute violation des dispositions de l'art. 25 RGPD relative à l'obligation d'annonce de la violation de données peut donner lieu à une amende administrative. Cette amende est dissuasive dans son montant qui peut atteindre jusqu'à EUR 10 millions ou 2 % du chiffre d'affaires mondial annuel de l'année précédente (art. 83, al. 4 RGPD) jusqu'à EUR 10 millions ou 2 % du chiffre d'affaires mondial pour une entreprise. Ce risque de sanction s'applique également aux cas de non-respect d'une injonction de l'autorité compétente sur la base de l'article 34, al. 4, 1 du Règlement [701].

821 Les personnes concernées sont habilitées à demander le versement de dommages et intérêts sur le fondement de l'article 82, al. 1 du Règlement, en cas d'omission de notification ou de notification tardive [702].

822 Afin de préserver l'intégrité des systèmes informatiques, la plupart des organisations développent un système de détection automatisé des violations de données à caractère personnel. Cette pratique est recommandée par le Règlement (consid. 87 RGPD). Il sera également indispensable d'élaborer un plan d'action pour la gestion de

698. art. 34, al. 3, b) RGPD.
699. art. 34, al. 3, c) RGPD.
700. art. 34, al. 4 RGPD.
701. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 522.
702. *Ibidem.*

crise en cas d'incident. Ce plan précisera les rôles et responsabilités des membres de la cellule de la crise. Une violation de données à caractère personnel peut en effet créer une perte de confiance des investisseurs et des partenaires de l'entreprise, induisant un préjudice économique [703].

XIII. Les données génétiques (article 4, al. 13 du Règlement)

Les données génétiques se définissent comme « des données personnelles relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent notamment d'une analyse d'un échantillon biologique de la personne physique en question [704] ». 823

Le considérant 34 apporte des éléments concrets en indiquant que « les données génétiques sont issues d'une analyse des chromosomes, des acides désoxyribonucléiques, et ribonucléiques ». 824

L'analyse des données issues du séquençage d'ADN permet l'identification de marqueurs génétiques indiquant le risque d'une maladie future. L'accès à ces données personnelles facilite la prévention des maladies, tout en soulevant la question du « droit de ne pas savoir ». En effet, le droit à l'autodétermination informationnelle est central dans des sociétés dans le lequel le dépistage systématique risque d'être fortement encouragé voir imposé adoptant la médecine personnalisée, comme modèle de santé publique. Dés lors se pose la question de la liberté du patient dans une économie de la santé de plus en plus soucieuse de personnaliser ses soins et de réduire ses coûts. 825

Une mise en parallèle des prestations d'assurance et des données génétiques fait apparaître le risque d'une discrimination des personnes concernées. Ainsi en droit suisse, se pose le problème du respect de l'article 8, al. 2 de la Constitution suisse [705]. L'inégalité de traitement lors de la conclusion d'un contrat d'assurance ou la fixation d'un montant de prime en fonction du résultat de données génétiques deviennent des questions fondamentales [706]. 826

703. *Idem*, p. 523.
704. art. 4 al. 13 RGPD.
705. Fasnacht, *Die Einwilligung im Datenschutzrecht*, p. 227.
706. *Idem*, p. 228.

XIV. Les données biométriques (article 4, al. 14 du Règlement)

827 Les données biométriques sont « des données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques, ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales [707] ». De telles données appartiennent à la catégorie des données particulières [708].

828 Le considérant 51 précise que « les traitements de photos ou de vidéos à des fins de classement automatique ne relèvent pas de la biométrie, sauf si de tels éléments ont pour objet l'identification sans équivoque d'une personne ».

829 Si un traitement biométrique engendre des risques élevés pour les droits droits et libertés des personnes, alors le responsable du traitement devra effectuer une analyse d'impact [709].

830 Les États membres sont habilités à introduire des conditions supplémentaires pour les traitements biométriques [710].

XV. Les données concernant la santé (article 4, al. 15 du Règlement)

831 Les données concernant la santé sont des « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique y compris la prestation de services de soins de santé, qui révèlent des informations sur l'État de santé de cette personne [711] ».

832 Le considérant 35 du Règlement apporte des précisions sur les maladies, les handicaps, les risques médicaux.

833 « Il importe de noter que les données de santé ne se confondent pas avec les données médicales. Ces dernières peuvent être des données de santé. Le champ d'application des données de santé est cependant plus large que celui des données médicales ». Le groupe de

707. art. 4 RGPD.
708. art. 9, al. 1 RGPD.
709. art. 35 RGPD et commentaires, in : Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 538 ; Wright David / de Hert Paul (édit.), *Privacy Impact Assessment*, 6e éd., Dordrecht 2012, p. 10.
710. art. 9, al. 4 RGPD.
711. art. 9, consid. 35 et 91 RGPD.

travail de l'Article 29 de la Commission européenne a pris position en faveur de la classification du quotient intellectuel, du port ou de lunettes, ou de lentilles de contact en tant que données de santé [712].

XVI. La notion d'établissement principal (article 4, al. 16 du Règlement)

« Lorsqu'un responsable du traitement est établi dans plusieurs États membres, le lieu de son administration centrale dans l'union, est le lieu dans lequel l'établissement prend des décisions quant aux finalités et aux moyens du traitement de données à caractère personnel, sauf si ces décisions sont prises dans un autre établissement du responsable du traitement dans l'union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions. Pour un sous-traitant établi dans plusieurs États membres, il s'agit du lieu de son administration centrale dans l'union. Si le sous-traitant ne dispose pas d'une administration centrale dans l'union, l'établissement principal du sous-traitant dans l'union est l'établissement où se déroule l'essentiel des activités de traitement [713]». 834

Cette définition différencie le responsable du traitement et le sous-traitant. 835

La notion d'établissement est importante pour déterminer la compétence de l'autorité compétente en matière de protection des données, en application de l'article 56, al. 1 du Règlement. 836

Le Règlement renvoie au considérant 19 de la directive 95/46/CE selon lequel « l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable ». La forme juridique n'est pas un critère déterminant [714]. 837

712. Article 29 Data Protection Working Party, *Advice paper on special categories of data ("sensitive data")*, in : European Commission (https ://ec.europa.eu/), Brussels 2011, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf » (26/03/2020).
713. art. 4, al. 16 RGPD.
714. CJUE 13 mai 2014, *Google contre Espagne*, C—131/12, consid. 97 ss. et CJUE 1er octobre, *Weltimmo*, C—230/14, consid. 41.

XVII. La notion d'entreprise (article 4, al. 18 du Règlement)

838 Une entreprise est définie par le Règlement comme « toute personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique ».

XVIII. Les règles d'entreprises contraignantes (article 4, al. 19 du Règlement)

839 « Les règles d'entreprises contraignantes sont les règles internes relatives à la protection des données à caractère personnel utilisées pour des transferts ou pour un ensemble de transferts de données à caractère personnel. Ces règles sont mises en œuvres par un responsable du traitement ou par un sous-traitant établi sur le territoire d'un État membre. Elles sont utilisées pour le transfert de données personnelles « au sein au sein d'un groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique ».

840 Le considérant 37 précise que l'influence déterminante d'une entreprise sur une autre constitue le critère déterminant. Cette influence peut trouver sa source dans les participations financières ou les liens de propriété entre les deux entreprises [715].

XIX. L'autorité de contrôle (article 4, al. 21 du Règlement)

841 Il s'agit « d'une autorité publique indépendante qui est instituée par un État membre en vertu de l'art. 51 du Règlement ».

XX. L'autorité de contrôle concernée (article 4, al. 22 du Règlement)

842 Il s'agit « d'une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que :

(a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;

715. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 222.

(b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ; ou

(c) une réclamation a été introduite auprès de cette autorité de contrôle ».

XXI. Le traitement transfrontalier (article 4, al. 23 du Règlement)

Un traitement transfrontalier de données est un transfert de données à caractère personnel dans l'UE ou en-dehors de l'UE. 843

Un traitement transfrontalier est défini dans le Règlement comme : 844

(a) « un traitement de données à caractère personnel qui a lieu dans l'union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou

(b) un traitement de données à caractère personnel qui a lieu dans l'union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ».

Cette notion est nouvelle [716], et est particulièrement importante pour déterminer la compétence territoriale de l'autorité de contrôle, en application de l'article 56 du Règlement [717]. 845

La CJUE a reconnu que « l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que tel, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 [...] effectué sur le territoire d'un État membre [718]» (voir paragraphe 140). 846

716. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 224.
717. *Ibidem.*
718. Arrêt CJUE du 6 octobre 2015, *Schrems contre DPC*, C—362/14, ECLI :EU :C :2015 :650, consid. 45.

XXII. L'objection pertinente et motivée (article 4, al. 24 du Règlement)

847 « L'objection pertinente et motivée », est une « objection à un projet de décision quant à savoir s'il y a ou non violation du présent Règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent Règlement. Cette objection démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des personnes concernées et, le cas échéant, le libre flux des données à caractère personnel au sein de l'union ».

848 La généralisation des définitions du Règlement européen permet cependant aux entreprises de traiter des données personnelles en appliquant les termes les plus favorables du Règlement européen, jusqu'à ce la jurisprudence vienne limiter cette interprétation, plusieurs années plus tard [719].

§5 Les principes de protection des données

849 Le Règlement pose plusieurs principes applicables au traitement de données personnelles (art. 5 RGPD). Les entreprises veilleront à documenter le respect de ces principes dans le cadre de leur gestion des risques car ils ont une valeur juridique contraignante. En cela, ils sont révélateurs du changement de paradigme du Règlement.

850 Outre leur intérêt pratique, ils présentent un intérêt théorique. Ils sont en effet essentiels à la compréhension et à l'interprétation du Règlement [720].

851 La directive 95/46/CE posait déjà les principes essentiels au traitement des données à caractère personnel. Ceux-ci furent consacrés par les législations nationales lors de la transposition de la directive 95/46/CE. Le Règlement confirme et renforce ces principes. Si les principes relatifs au traitement des données à caractère personnel sont mentionnés à l'art. 5, al. 1 du Règlement, un principe structurel, de responsabilité des responsables du traitement et des sous-traitants est posé à l'art. 5, al. 2 du Règlement. Ce principe n'est pas directement lié aux traitements de données, mais renvoie à

719. Weber / Staiger, *Transatlantic Data Protection in Practice*, p. 136.
720. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 227.

une nouvelle obligation prudentielle du responsable du traitement. Celui-ci doit démontrer son comportement diligent en apportant la preuve, que des mesures techniques et organisationnelles ont été prises (art. 24, al. 1 RGPD) [721] (voir paragraphe 941). La charge de la preuve lui incombe.

L'approche adoptée par le législateur européen dans le domaine de la protection des données est similaire à celle du législateur lors de l'élaboration des normes comptables IFRS (International Financial Reporting Standard). Ces normes sont également basées sur des principes généraux, ce qui permet leur utilisation dans des pays aux cultures juridiques variées. L'objectif est de donner une image fidèle – « true and fair view » – des comptes de la société [722]. Un effort de jugement est cependant demandé aux entreprises et à leurs auditeurs, comme c'est le cas les responsables du traitement et les sous-traitants qui collectent et traitent des données personnelles plus ou moins sensibles. 852

Si ces principes reprennent en partie ceux de la directive européenne (UE)95/46/CE et des normes ISO (29100 :2011), il importe de relever que la violation des principes du Règlement peut être sanctionnée (art. 83 al. 5, a) RGPD) par le paiement d'une amende équivalente à 4 pour cent du chiffre d'affaires annuel global. 853

I. La licéité, la loyauté et la transparence (articles 5 et 6 du Règlement)

En application de l'article 5 du Règlement, les données à caractère personnel doivent être « traitées de manière licite, loyale et transparente au regard de la personne concernée ». 854

Pour qu'un traitement soit licite, il doit remplir l'une des conditions posées par le Règlement à l'art. 6, al. 1. 855

A. Le consentement

La directive 95/46/CE définissait le consentement de la personne concernée comme « toute manifestation de volonté, libre, spécifique, et informée par laquelle la personne concernée accepte que 856

721. *Ibidem.*

722. Callao Susana / Jarne José Ignacio, *Have IFRS affected earnings management in the European Union ?*, in : Accounting in Europe 2010 7/2, pp. 159-189.

des données à caractère personnel la concernant fasse l'objet d'un traitement [723]».

857 Le Règlement, quant à lui, propose une vision plus restrictive du consentement. Celui-ci est défini comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque, par laquelle la personne concernée accepte par une déclaration ou par un acte positif clair que des données à caractère personnel la concernant fasse l'objet d'un traitement [724]».

858 L'article 4, al. 11 du Règlement, impose un acte positif. Ainsi le silence, l'existence d'une case cochée préalablement, ou l'inaction de la personne concernée, ne valent pas comme consentement. Celui-ci doit être exprès.

859 Le considérant 32, al. 6 du Règlement précise que la personne concernée peut donner son consentement « en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».

860 Ce considérant reprend l'avis 15/2011 du groupe de travail de l'Article 29 de la Commission européenne sur la définition du consentement, adopté le 13 juillet 2011 (WP 187). En pratique l'utilisateur pourrait faire face à une augmentation du nombre de fenêtres (cookies) sollicitant son consentement. Cela rendra l'utilisation du réseau internet moins agréable du fait des nombreuses interruptions engendrées [725].

861 Le Règlement pose un principe d'interdiction du traitement des données sensibles (art. 9, al. 1 RGPD). Par exception, le traitement de ces données est autorisé avec le consentement explicite des personnes physiques. Cependant ce consentement doit être « explicite » et donné « pour une ou plusieurs finalités spécifiques », sauf lorsque le droit de l'union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la

723. art. 2, h) de la directive 95/46/CE.
724. art., 4, al. 11 RGPD.
725. Härting, *Datenschutz-Grundverordnung*, p. 91.

personne concernée [726].

Des conditions encore plus strictes prévalent pour le traitement de données à caractère personnel concernant un mineur, en application de l'article 8 du Règlement [727]. Ainsi « lorsque l'enfant est âgé de moins de 16 ans, le traitement de données n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans ». 862

A titre d'exception, aucun consentement n'est requis pour les « services de prévention ou de conseil proposés directement à un enfant (art. 38, al. 3 RGPD)». 863

Concernant les adultes, il est indiqué dans l'article 7, al. 2 du Règlement, que « si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ». 864

La directive 95/CE imposait déjà que le consentement pour être valide devait être donné librement. art. 7 let a) de la directive 95/46/CE). 865

Le Règlement ajoute « qu'au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ». 866

En outre, la personne concernée peut retirer son consentement à tout moment et il doit être aussi simple de retirer son consentement que de la donner (art. 7, al. 3 RGPD). 867

Le Règlement inverse la charge de la preuve. La légalité du traitement doit être démontrée par le responsable du traitement. Il documentera donc le consentement de la personne concernée de ma- 868

726. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 256.
727. *Ibidem.*

nière minutieuse. Les personnes concernées ont en effet le droit de retirer leur consentement en tout temps [728]. C'est pourquoi l'autorité de contrôle britannique (Information Commissionner Office) a qualifié le consentement de consentement dynamique [729].

869 Le consentement doit être demandé sans équivoque, d'une manière distincte des autres questions, sous une forme compréhensible et aisément accessible pour la personne concernée [730]. La personne concernée doit être consciente du consentement qu'elle donne et de sa portée. Si la personne concernée prend connaissance des conditions générales, au moment du recueil du consentement, elle ne doit pas être induite en erreur.

870 Avant de donner son consentement, la personne concernée a le droit de connaître l'identité du responsable du traitement et la/les finalité(s) pour laquelle / lesquelles ses données dont collectées [731].

871 De même, elle doit être informée de la possibilité de retirer son consentement et de l'effet de ce retrait avant de consentir (art. 7, al. 3 RGPD) [732].

872 Si la personne concernée retire son consentement, ce retrait n'a pas d'effet rétroactif. Le retrait du consentement ne compromet pas rétroactivement la licéité du traitement.

873 Pour Tim Wybitul, le retrait du consentement vaut uniquement pour l'avenir et n'a pas de valeur rétroactive [733]. Selon lui, un droit à la suppression et à l'effacement des données à caractère personnel s'applique en vertu de l'article 17, al. 1, b) du Règlement.

874 Le consentement doit être donné librement. « Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est su-

728. art. 7, al. 3 RGPD.
729. Avis de l'Information Commissionner Office relative au consentement sur ICO, *Consent*, in : ICO (https://ico.org.uk/), Wilmslow s.a., p. « https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ » (07/12/2018).
730. Consid. 42 RGPD et art. 7, al. 2 RGPD.
731. Consid. 42, al.3 à 5 RGPD.
732. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 262.
733. *Ibidem.*

bordonnée au consentement au traitement de donnéees à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat [734]».

Il importe de se demander si la validité du consentement pourra être remise en question, quand la prestation d'un service ou l'exécution d'un contrat est subordonnée au consentement de la personne concernée au traitement des données, alors que ce consentement n'est pas nécessaire à l'exécution du contrat. En application de l'article 7, al. 4 du Règlement, il semble que ce consentement ne sera pas valable car il ne ne constitue pas une manifestation de volonté libre [735]. 875

Ainsi une présomption de non consentement pourra être invoquée, si un consentement distinct ne peut être donné à différentes opérations de traitement des données à caractère personnel, bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonné au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution [736]. 876

Ceci est confirmé par l'interprétation de Tim Wybitul dans son manuel sur le Règlement général sur la protection des données. Selon lui, le Règlement diffuse à travers les articles une interdiction de corrélation (« Koppelunggsverbot ») du fait de l'article 7, al. 4 et du considérant 43. Il confirme que si le consentement est donné sans être libre, alors celui-ci ne serait pas valable [737]. 877

Il existe une contradiction entre l'article 7, al. 4 et le considérant 44 du Règlement. Ce dernier dispose que « le traitement devrait être considéré comme licite, lorsqu'il est nécessaire dans le cadre d'un contrat ou de l'intention de conclure un contrat ». Il est important de rappeler que seuls les articles du Règlement ont une valeur obligatoire et non pas les considérants. Par conséquent, l'article 7, al. 4 du Règlement semble s'appliquer de façon prioritaire. 878

Lorsqu'il existe un déséquilibre manifeste entre la personne concer- 879

734. art. 7, al. 4 RGPD.
735. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 260.
736. Consid. 43 RGPD.
737. Wytibul Tim, *Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte ? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen*, in : Zeitschrift für Datenschutz (ZD) 2016/5, pp. 203-208.

née et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique, le consentement ne sera pas valable car la condition d'un consentement libre n'est pas remplie. De même, dans le cadre de relations de travail, l'existence du contrat de travail [738] suppose un lien de subordination et induit dès lors un lien de dépendance envers l'employeur [739]. Cette perspective est partagée par le WP-29 [740].

880 Le consentement donné librement semble signifier que celui-ci doit être donné sans contrainte [741]. L'évolution technologique comme l'utilisation d'objets connectés (ex. : le smartphone) permet de collecter des renseignements sur la santé d'une personne de manière indirecte [742]. Certains chercheurs scientifiques s'interrogent sur la disparition du consentement libre et éclairé notamment pour des études cliniques, conséquence de l'enregistrement systématique de toutes les traces numériques diffusées, volontairement ou non, par les individus. Ceci est dû à la croissance des moyens de calculs numériques alliée à celle des masses de données accessibles [743].

881 « Le consentement n'est juridiquement valable que s'il intervient librement ». Cela suppose une liberté d'action (Handlungsfreiheit) et d'expression de la volonté. Cette exigence s'accomode difficilement d'un lien d'autorité [744], comme un lien hiérarchique. La personne concernée doit en outre être en capacité de consentir. La validité du consentement d'un mineur peut être remise en cause du fait de sa vulnérabilité. Pour les adultes, le Préposé fédéral à la protection des données relève, à titre d'exemple, « qu'il n'y a de volonté librement exprimée, que si le preneur d'assurance peut choisir entre différents modèles d'assurance et qu'il ne subit aucune pression fi-

738. Sur la notion d'une interdiction du consentement initialement proposée par la Commission européenne, voir art. 7, al. 4 de la proposition. Cf. également Fasnacht, *Die Einwilligung im Datenschutzrecht*, p. 177.
739. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 260.
740. Article 29 Data Protection Working Party, *Opinion 02/2017 of Article 29 Data Protection Working Party*.
741. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 259.
742. Wachter Sandra / Mittelstadt Brent Daniel, *A right to reasonable inferences : re-thinking data protection law in the age of Big Data and AI*, in : Columbia Business Law Review 2018, p. 575.
743. Besse Philippe / Castets-Renard Céline / Garivier Aurélien, *Loyauté des Décisions Algorithmiques*, in : HAL Archives-Ouverts 2017, p. « https://hal.archives-ouvertes.fr/hal-01544701 » (13/12/2019).
744. Dupont Anne-Sylvie, *Les données confiées aux assureurs sociaux*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019, p. 6.

nancière. Les différences de prix ne peuvent donc pas être telles que le preneur d'assurance se sente contraint d'opter pour un modèle moins cher [745] ».

Bien que la technologie facilite la collecte du consentement des personnes concernées, le consentement ne semble pas la meilleure option pour le responsable du traitement. Du fait de la gestion délicate du consentement, en particulier du droit de retrait du consentement et de la question de sa validité, le motif de licéité d'un traitement de données à caractère personnel doit être mûrement réfléchi. Ceci est d'autant plus vrai que la charge de la preuve incombe au responsable du traitement. 882

En Suisse, la collecte des données personnelles par le groupe Helsana, sans consentement des personnes concernées a été déclarée illicite par le Tribunal fédéral administratif [746]. 883

Les entreprises devront s'assurer que le consentement de la personne concernée, donné préalablement à l'entrée en vigueur du Règlement, est valable. A titre d'exemple, la CJUE a précisé dans un arrêt « Schwarz » que le consentement ne constituait pas une base légale valable pour « légitimer la collecte d'empreintes digitales, dès lors que la délivrance d'un passeport, document indispensable pour voyager hors de l'Union européenne, lui était subordonné [747] ». 884

À défaut de consentement valable, un nouveau consentement, remplissant les conditions du Règlement, devra être obtenu. Si cela s'avère impossible, le responsable du traitement devra pouvoir justifier le traitement des données à caractère personnel sur un autre fondement juridique. Ceux-ci sont examinés ci-après. 885

Le choix de l'opt-out ne remplit pas les conditions de validité du consentement qui nécessite une déclaration d'assurance positive (« positive Erklärung »). Cependant, le Règlement n'impose aucun formalisme particulier (« Formfreiheit »). Il existe cependant une obligation pour le responsable du traitement d'apporter la preuve du consentement (« Nachweispflicht »). Cette obligation est l'expression du principe de responsabilité du responsable du traitement (art. 5, al. 2 RGPD) et démontre que le Règlement poursuit un 886

745. PFPDT, *Explications relatives aux capteurs fitness en lien avec les assurances.*
746. TAF, 19/03/2019, A-3548/2018, consid. 4.9.
747. Arrêt CJCE du 17 octobre 2013, *Michael Schwarz c. Stadt Bochum*, C—291/12, ECLI :EU :C :2013 :670, consid. 32.

double objectif préventif et répressif. Pour apporter la preuve du consentement, le responsable du traitement doit pouvoir démontrer le contenu du consentement (ce qu'il pourra établir en application des principes de documentation et d'archivage). Il s'agit d'une règle de procédure autonome (selbständige Verfahrensvorschrift).

B. Le traitement nécessaire pour des finalités déterminées

887 De même que l'article 7 de la directive 95/46/CE, l'article 6 du Règlement pose un principe d'interdiction du traitement des données personnelles. Il prévoit cependant des cas particuliers pour lesquels le traitement est justifié et donc licite. Il s'agit du concept de « Verbot mit Erlaubnisvorbehalt » présenté par la doctrine [748].

888 L'article 6 du Règlement expose six finalités qui rendent licite le traitement de données à caractère personnel. Le consentement a été examiné au préalable. Il reste à analyser les cinq autres exceptions.

(a) Le traitement nécessaire à l'exécution d'un contrat avec la personne concernée ou à l'exécution de mesures préparatoires à un tel contrat (article 6, al. 1 b) du Règlement)

889 Le Règlement confirme le principe de la directive 95/46/CE sur ce point. Il doit s'agir d'un contrat conclu directement entre le responsable du traitement et la personne concernée. Cette exception présente l'avantage de dispenser le responsable du traitement du besoin de recueillir le consentement de la personne concernée pour chaque cas unique. Plus concrètement, il s'agit de comprendre dans ce cas de figure, que le traitement des données à caractère personnel est effectué dans l'intérêt de la personne concernée. À titre d'exemple, il pourra s'agir de la conclusion d'un contrat d'achat par la personne concernée sur internet et de la collecte des informations personnelles de l'acheteur (nom, prénom, adresse). Cette collecte est nécessaire au vendeur pour honorer les obligations issues du contrat entre l'acheteur et le vendeur [749].

890 Le traitement des données revêt un caractère nécessaire (« Erforderlichkeit ») et doit être proportionné (« Verhältnismässigkeits-

748. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 240.
749. *Idem*, p. 242.

prüfung ») [750].

Par exemple, ne sera pas considéré comme nécessaire à la conclusion du contrat, le traitement de données à caractère personnel de clients dans un objectif publicitaire ultérieur. De même, ne sera pas nécessaire à la conclusion du contrat, le fait pour un responsable du traitement de communiquer les données à caractère personnel de ses clients sur un fournisseur de Cloud, car cette opération ne figure pas habituellement dans le contrat liant un responsable du traitement et la personne concernée [751]. Le transfert de données vers un tiers sera bien entendu licite si le contrat le mentionne explicitement. 891

Le Tribunal fédéral a publié le 27 juin 2019 l'arrêt 2C_1083/2017 dans lequel il affirme que « le professionnel externe chargé de la conservation et de la protection à distance des données informatiques » est un auxiliaire de l'avocat (c. 7.3). L'avocat peut ainsi lui transmettre des données clients sans violer son secret. Il doit néanmoins le choisir soigneusement et veiller à ce qu'il respecte le secret professionnel (c. 7.2). De plus, l'avocat doit s'assurer que l'auxiliaire ne fasse pas « exécuter par un tiers tout ou partie des tâches qu'il s'est engagé à lui fournir (situation de sous-délégation) » (c. 7.4). Cette analyse risque de s'appliquer également aux banques suisses qui désirent passer au Cloud banking. 892

De façon générale, il importe que le traitement respecte les principes en lien avec la protection des données tels que définis, à l'article 5, al. 1 du Règlement. Le responsable du traitement veillera en particulier à respecter les principes de transparence, de minimisation des données et de bonne foi [752]. Une approche critique de la minimisation des données est cependant nécessaire dans un modèle économique et sociétal fondé sur le traitement algorithmique des données [753]. Une raréfaction des données pourrait créer de nouveaux risques, encore sous-estimés aujourd'hui (par ex. dans le do- 893

750. *Idem*, p. 242.
751. Hornung Gerrit / Sädler Stephan, *Europas Wolken — Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing*, in : Computer Und Recht : Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation 2012 28/10, p. 638 et 641 ; Spindler Gerald / Schuster Fabian (édit.), *Recht der elektronischen Medien : Kommentar*, 3e éd., München 2015, al. 28 BDSG Rn.5.
752. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 243.
753. Domingos, *The Master Algorithm*, p. xv.

maine médical).

(b) Le traitement nécessaire au respect d'une obligation légale (article 6, al. 1 c) du Règlement)

894 Ce principe n'est pas nouveau. Il figurait déjà dans la directive 95/46/CE.

895 Selon ce principe, un traitement de données personnelles est licite, si deux conditions cumulatives sont réunies.

896 Tout d'abord, les États membres sont en droit de justifier le traitement des données à caractère personnel, pour une raison qui leur est propre [754]. Il s'agit ainsi d'une clause dérogatoire en faveur de Etats membres de l'UE (« Öffnungsklausel »).

897 Ensuite, si le Règlement n'impose pas une loi pour justifier le traitement [755], la base juridique doit toutefois mentionner la finalité du traitement [756] et « les conditions de licéité du traitement (types de données, personnes concernées, destinataire des données...) [757] ».

898 La base juridique d'un traitement doit être « claire et précise » et son application prévisible pour ses destinataires [758]. « Ceci s'inscrit dans l'esprit du principe de légalité, tel qu'il ressort de la jurisprudence de la Cour de Justice de l'UE et de la Cour Européenne des droits de l'homme ».

899 À titre d'exemple, la doctrine considère qu'à défaut d'une autorisation explicite dans l'article 6, al. 1, c) du Règlement, les conventions collectives ne constituent pas une base légale suffisante pour justifier le traitement de données à caractère personnel [759].

(c) Le traitement nécessaire à la sauvegarde des intérêts vitaux de la personne (article 6, al. 1 d) du Règlement)

900 « Il s'agit des traitements nécessaires à la protection des intérêts vitaux d'une personne concernée ou d'une autre personne, y compris l'intégrité physique ou la vie, quand la personne concernée est

754. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 243 ; Les situations présentées à l'article 85 ss du Règlement s'inscrivent dans cette logique.
755. Consid. 45 RGPD.
756. art. 6, al. 3, consid. 2 RGPD.
757. art. 6, al. 3 RGPD et consid. n° 41 et 45.
758. Consid. 41 et 45 RGPD.
759. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 244.

incapable de consentir au traitement [760]».

Le Règlement ne définit pas la notion des intérêts vitaux de la personne. 901

Le Règlement suggère que « ce fondement puisse s'appliquer au traitement nécessaire à des fins humanitaires ou dans les cas d'urgence humanitaire [761]». Selon ce considérant, « si des données sont traitées dans l'intérêt vital d'une autre personne que la personne concernée, il est permis de se baser sur ce fondement, seulement si aucune autre base légale n'est disponible ». 902

Cet article sera vraisemblablement utile pour les organisations internationales. Le considérant 112, précise notamment que « tout transfert vers une organisation humanitaire internationale de données à caractère personnel d'une personne concernée qui se trouve dans l'incapacité physique ou juridique de donner son consentement, en vue d'accomplir une mission relevant des conventions de Genève ou de respecter le droit humanitaire international applicable dans les conflits armés, pourrait être considéré comme nécessaire pour des motifs importants d'intérêt public ou parce que ce transfert est dans l'intérêt vital de la personne concernée [762]». 903

(d) La mission d'intérêt public (article 6, al. 1, let e), du Règlement)

Le Règlement précise que ce fondement ne s'appliquera que lorsque la mission d'intérêt public exécutée, ou la qualité « d'autorité publique » du responsable du traitement, trouve sa source dans le droit de l'union ou de l'État membre auquel le responsable du traitement est soumis [763]. 904

Le Règlement formalise ainsi la jurisprudence de la CJUE qui a légitimé dans son arrêt « Worten contre ACT [764]», « l'accès à des données personnelles sans requérir le consentement de la personne concernée, lors de l'exercice d'une mission de service public ». La CJUE a posé comme condition que le traitement soit « nécessaire 905

760. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016.*
761. Consid. 46 RGPD.
762. Consid. 112 RGPD.
763. art. 6, al. 3 et consid. 45 RGPD.
764. Arrêt CJUE du 30 mai 2013, *Worten contre ACT*, C—342/12, ECLI :EU :C :2013 :355.

à l'accomplissement de l'obligation de service public ». En application du principe de proportionnalité [765], la collecte doit répondre à des « finalités déterminées, explicites et légitimes et les données doivent être adéquates, pertinentes et non-excessives au regard des finalités poursuivies [766] ».

(e) Le traitement nécessaire aux fins d'intérêts légitimes (article 6, al. 1, f) du Règlement)

906 Le Règlement reprend un fondement de la directive 95/46/CE. Il privilégie une pesée des intérêts en présence [767].

907 Le Règlement préconise la licéité du traitement de données personnelles lorsque celui-ci est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant » (art. 6 RGPD).

908 La jurisprudence confirme cet élément dans un arrêt du 4 mai 2017 [768] : « [...] il convient de relever que l'âge de la personne concernée peut constituer l'un des éléments dont il convient de tenir compte dans le cadre de [la] pondération [à effectuer entre l'intérêt de la personne concernée et l'intérêt légitime du responsable du traitement lorsque celui-ci souhaite s'en prévaloir pour fonder son traitement] ».

909 Le critère des intérêts légitimes [769] poursuivis par le responsable du traitement est exclu pour les traitements effectués par les autorités publiques dans l'exécution de leur mission.

910 Pour la doctrine, cet article confère une insécurité juridique du fait de sa formulation large et imprécise [770]. Elle est qualifiée par cer-

765. EDPS, *EDPS Guidelines on assessing the proportionality*, p. 6 ss.
766. CJCE 20 mai 2003, *Österreichischer Rundfunk*, C—465/00, C-138/01 et C-139/01, consid. 66.
767. Docquir, *Vers un droit européen de la protection des données ?*, p. 97.
768. Arrêt CJUE du 4 mai 2017, *Rigas Satiksme*, C—13/16, ECLI :EU :C :2017 :336
769. art. 6, al.1, f) RGPD.
770. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 245 ; Frenzel Eike Michael, *Grundsätze - Rechtmäßigkeit der Verarbeitung*, in : Paal Boris P. / Pauly Daniel A. (édit.), *Datenschutz - Grundverordnung*, 2e éd., München 2017, art. 6 Rn. 31.

tains de disposition générale ou « Auffangstatbestand ».

Sont considérés comme des traitements de données à caractère personnel, « nécessaire » à l'intérêt légitime d'un responsable du traitement : 911

- le traitement à des fins de prospection ou de prévention de la fraude [771] ;
- la transmission de données à caractère personnel au sein d'un groupe d'entreprises à des fins administratives internes, y compris des données de clients ou d'employés [772] (dans ce cas les exigences relatives aux transferts internationaux demeurent applicables) ; et
- le traitement aux fins de garantir la sécurité du réseau et des informations, y compris, empêcher l'accès non autorisé à des réseaux de communications électroniques et faire cesser les dommages touchant les systèmes de communication informatique et électronique [773].

Les responsables du traitement devraient tenir compte des attentes des personnes concernées pour évaluer si leurs intérêts légitimes l'emportent sur les intérêts des personnes concernées ; Les intérêts et droits fondamentaux des personnes concernées pourraient en particulier prévaloir sur celui du responsable du traitement lorsque les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur [774]. 912

Lorsqu'une organisation se fonde sur « des intérêts légitimes, les individus devront désormais en être explicitement informés [775]». 913

Le groupe de travail de l'Article 29 de la Commission européenne précise que « pour être pertinent au regard de l'article 7, consid. f), un intérêt légitime » doit être licite (c'est-à-dire conforme au droit en vigueur dans l'union et dans le pays concerné), être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment précis) et constituer 914

771. Consid. 47 RGPD.
772. Consid. 48 RGPD.
773. Consid. 49 RGPD.
774. Consid. 47 RGPD.
775. art. 13, d) RGPD.

un intérêt réel et présent [776].

915 Le responsable du traitement doit s'abstenir de tout traitement qui ne serait pas « nécessaire à la réalisation de l'intérêt légitime » du responsable du traitement.

916 La CNIL a rendu deux décisions relatives au test de la balance des intérêts qui viennent préciser la notion d'intérêt légitime et les garanties à apporter par le responsable du traitement [777].

917 Les garanties données par le responsable du traitement pourront être les suivantes [778] :

- Limitation stricte des données traitées ;
- Mesures techniques et organisationnelles (voir paragraphe 941) ;
- Techniques d'anonymisation ou de pseudonymisation ;
- Agrégation des données ;
- Transparence renforcée ;
- Droit d'opposition général et inconditionnel ;
- Gestion contractuelle ; et
- Mécanisme permettant au client d'accéder à ses propres données et de les modifier.

918 Les entreprises pourront en outre demander l'application du considérant 47 du Règlement qui se rapproche de la jurisprudence américaine concernant la notion de protection de la sphère privée [779]. Dans un arrêt « Katz vs. United States [780]», la Cour suprême américaine retient l'application du critère du test des « attentes raisonnables à la vie privée [781]».

919 Outre le caractère légitime de l'intérêt poursuivi, il est précisé que

776. Groupe de Travail de l'Article 29, *Avis 06/2014 du Groupe de travail de l'Art. 29.*
777. Avignon Céline, *Règlement UE protection des données et balance des intérêts*, in : Lexing - Alain Bensoussan Avocats (https ://www.alain-bensoussan.com/), Paris 2017, p. « https://www.alain-bensoussan.com/avocats/reglement-ue-protection-donnees-balance-des-interets/2016/09/14/ » (07/12/2018).
778. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 90.
779. Härting, *Datenschutz-Grundverordnung*, p. 107.
780. Arrêt de la Cour suprême américaine du 18 décembre 1967, Az. 389 U.S. 347.
781. "Reasonable expectations of privacy test".

le traitement doit être nécessaire à la (ou aux) finalité(s) visée(s) (...) [782].

Il doit donc exister un lien entre le traitement et l'intérêt poursuivi par le responsable du traitement, afin de garantir que le traitement des données fondé sur l'intérêt légitime ne débouche pas sur une interprétation trop large de la nécessité de traiter des données. Cela signifie qu'il y a lieu d'examiner s'il existe d'autres moyens plus respectueux de la vie privée susceptibles de servir la même finalité [783]. 920

Cela rejoint l'avis du groupe de travail de l'Article 29 de la Commission européenne qui a rappelé le caractère essentiel de la protection des intérêts de la personne concernée, en ces temps où croit le déséquilibre « du pouvoir de l'information », à l'heure ou administrations et entreprises amassent des volumes sans précédent de données concernant les individus et se donnent de plus en plus les moyens de constituer des profils détaillés qui prédiront leurs comportements futurs (au risque de renforcer encore le déséquilibre informationnel et d'amoindrir l'autonomie des citoyens [784]. 921

En l'absence d'intérêt légitime, la personne concernée peut faire valoir son droit d'opposition au traitement [785]. A la réception d'un courrier informant le responsable du traitement de l'opposition de la personne concernée au traitement de ses données personnelles, le responsable du traitement est obligé d'interrompre le traitement [786]. La durée de l'interruption est fonction du temps nécessaire au responsable du traitement pour justifier le traitement des données [787]. 922

L'excellence dans le respect des procédures internes est devenu un thème essentiel depuis l'entrée en vigueur du Règlement. 923

(f) Les autres fondements

Les États membres sont autorisés à introduire d'autres motifs justifiant le traitement de données à caractère personnel, dans les domaines du journalisme, des relations de travail, de la recherche ou 924

782. Groupe de Travail de l'Article 29, *Avis 06/2014 du Groupe de travail de l'Art. 29*, p. 32.
783. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 89.
784. Groupe de Travail de l'Article 29, *Avis 06/2014 du Groupe de travail de l'Art. 29*, p. 33.
785. art. 21, al. 1 RGPD.
786. Härting, *Datenschutz-Grundverordnung*, p. 121.
787. art. 18, al. 1, d) RGPD.

des statistiques [788]. L'harmonisation visée par la Règlementation ne sera donc pas complète dans ces secteurs au sein de l'UE.

II. La limitation des finalités

925 Les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités [789] ».

926 Toute finalité incompatible avec la finalité annoncée est dès lors interdite sauf exception pour les finalités historiques, statistiques ou scientifiques [790].

927 La personne concernée est informée des finalités du traitement, avant la collecte des données à caractère personnel [791]. Les finalités du traitement doivent être clairement énoncées. Ces finalités doivent en outre être légitimes.

928 En vertu du principe de proportionnalité, les traitements de données à caractère personnel à effectuer doivent être adéquats, pertinents et non excessifs au regard des finalités poursuivies, ce qui suppose que le moyen utilisé soit adéquat et nécessaire pour réaliser l'objectif poursuivi [792]. Cependant, le législateur laisse au responsable du traitement le soin de définir à partir de quel moment le traitement pourrait être jugé excessif. Cette appréciation au cas par cas apporte de la souplesse au responsable du traitement, mais constitue également une insécurité juridique.

929 Selon le principe de qualité des données, les données doivent être exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées. Cet élément est fondamental lorsque les données sont utilisées par des algorithmes pour effectuer des diagnostics, des recommendations, ou prendre des décisions.

930 Enfin, les données ne peuvent être conservées indéfiniment. Les

788. Consid. 50 RGPD.
789. art. 5, al. 1, b) RGPD.
790. art. 5, al. 1, b) RGPD.
791. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 229.
792. art. 5, al. 1, c) RGPD.

données doivent être supprimées dès lors que leur conservation excède la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées [793]. En pratique, le responsable du traitement devra renoncer à conserver les données personnelles pour des projets futurs ultérieurs dont les finalités seront potentiellement incompatibles avec la finalité de la collecte initiale.

Le Règlement impose notamment au responsable du traitement de prendre en considération certains facteurs pour déterminer si une finalité est compatible avec la finalité pour laquelle les données ont été initialement collectées, lorsque le traitement a une autre fin que celle pour laquelle les données ont été collectées [794]. 931

Ces facteurs sont les suivants : 932

- « L'existence éventuelle d'un lien entre la finalité initiale et la nouvelle finalité proposée ;
- Le contexte dans lequel les données ont été collectées (en particulier la relation entre les personnes concernées et le responsable du traitement) ;
- La nature des données (en particulier si elles sont des données sensibles ou des données judiciaires) ;
- Les conséquences possibles du traitement envisagé ; et
- L'existence de garanties (y compris le chiffrement ou la pseudonymisation) [795] ».

Le Règlement offre un régime dérogatoire pour les traitements effectués à des fins de recherche scientifiques. La finalité du traitement des données personnelles n'a pas besoin d'être définie de manière spécifique pour les traitements effectués à des fins de recherche scientifique au moment. Dans ces circonstances, le consentement sera réputé comme étant valable même en présence de finalités imprécises. Le considérant 33 RGPD précise ainsi que « les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet [796] ». 933

793. art. 5, al. 1, e) RGPD.
794. art. 6, al. 4 RGPD.
795. art. 6, al. 4 RGPD.
796. Consid. 33 RGPD.

III. La minimisation des données (article 5, al. 1er, c du Règlement)

934 « Les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

935 La conservation des données doit également être limitée au strict minimum [797]. Enfin, les données à caractère personnel ne doivent être traitées que si la finalité du traitement ne peut être obtenue d'une autre manière [798].

936 Se pose la question de savoir comment concilier le principe de minimisation des données avec les technologies de l'ère digitale comme le Big Data ? Les entreprises devront être particulièrement vigilantes dans la conception et la mise en œuvre de nouveaux projets technologiques afin de s'assurer de leur conformité juridique au nouveau droit européen de la protection des données.

937 « Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités auxquelles les données à caractère personnel sont traitées [799]».

938 Le Règlement précise, à l'article 89, que : « le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent Règlement, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles (voir paragraphe 941, en particulier pour assurer le respect du principe de minimisation des données ». Par exemple, la pseudonymisation des données.

797. Consid. 39 RGPD.
798. Consid. 39 RGPD.
799. art. 5, al. 1, e) RGPD

IV. Le principe d'exactitude des données (article 5, al. 1er, d du Règlement)

Les données à caractère personnelle doivent être « exactes et tenues à jour ». 939

La notion d'exactitude signifie que les données doivent être intrinséquement correctes (« sachlich richtig ») et tenues à jour [800]. Le responsable du traitement doit prendre des mesures raisonnables pour garantir que les données a caractère personnel inexactes, eu égard aux finalités auxquelles elles sont traitées, soient effacées ou rectifiées sans délai [801]. 940

V. Le principe d'intégrité et de confidentialité (article 5, al. 1er, f du Règlement)

Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction, ou les dommages d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. 941

Le Règlement impose aux organisations de sécuriser leurs données. Cela signifie que des mesures appropriées de nature technique et organisationnelle [802] doivent être prises pour réduire le risque de violation des données à caractère personnelle et répondre aux obligations du Règlement. Les organisations doivent documenter l'existence de ces mesures afin de pouvoir prouver qu'une gouvernance des données a été mise en place et que les risques sont examinés de façon appropriée. 942

Les mesures techniques et organisationnelles doivent tenir compte « de l'État des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». 943

L'évaluation du niveau de sécurité approprié tient compte en particulier des risques que présente le traitement, résultant notamment de la destruction, la perte ou l'altération, la divulgation non auto- 944

800. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 232.
801. *Ibidem.*
802. art. 32 RGPD.

risée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral pour la personne concernée.

945 Le Règlement recommande l'utilisation de techniques « adaptées au risque » comme :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des mesures garantissant la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement ;
- des moyens de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; et
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

946 Un élément important à considérer pour les organisations est la possibilité de recourir à l'application d'un code de conduite approuvé ou à un mécanisme de certification pour démontrer le respect des exigences de sécurité prévues. Cependant, la question de la responsabilité des organismes certificateurs se pose. Selon Mark Thompson, Head of Global Privacy de KPMG, rencontré à Londres en mai 2017 lors d'une formation sur le Règlement général sur la protection des données organisée par l'IAPP, l'industrie dans son ensemble n'offrait pas un niveau de conformité suffisant pour qu'une certification en matière de sécurité des données soit délivrée. KMPG ne proposait donc pas de service de certification à cette date. Cette situation a changé depuis l'entrée en vigueur du Règlement et l'amélioration du niveau de maturité des organisations dans le domaine de la protection des données personnelles.

947 L'existence d'un mécanisme de sanctions spécifiques offre des garanties pour la mise en œuvre effective du Règlement européen dans les pays de l'UE tant en laissant de la liberté aux responsables du traitement, qui peuvent recourir à des mécanismes de Soft Law. Ce double système d'incitation et de contrôle est nécessaire pour bénéficier de mécanismes de régulation qui fonctionnent en pra-

tique [803].

La conduite d'audits réguliers en matière de protection des données, la préparation d'analyses d'impact, l'adoption de mesures de « privacy-by-design », la désignation d'un délégué à la protection des données, effectivement indépendant, sont des éléments essentiels d'une gouvernance des données effectives. La documentation de ces éléments sera un gage de confiance pour les autorités de contrôle et l'ensemble des partenaires de l'organisation, notamment les sous-traitants. 948

Les exigences de sécurité sont également à considérer dans le cadre d'autres instruments juridiques comme le Règlement e-privacy ou la directive-Cadre [804] et la directive 2016/1148/UE du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'union [805]. 949

Cette directive SRI a été adoptée dans l'UE et doit être transposée en droit national pour les pays membres de l'UE, depuis le 9 mai 2018. 950

Des obligations de sécurité accrues s'imposent donc aux opérateurs de services essentiels et aux fournisseurs de services numériques dans l'UE. Examinons tout d'abord ce qu'est un service essentiel avant de traiter la question du service numérique. 951

Un service essentiel est indispensable au maintien d'activités sociétales et/ou économiques critiques, dont la fourniture est tributaire des réseaux et des systèmes d'information, sur lequel un incident aurait un effet disruptif important sur la fourniture dudit service. Il est laissé à la charge des États membres d'identifier les opérateurs de services essentiels que peuvent être les secteurs de l'énergie, du transport, de la banque, de la bourse, les services publics et les soins 952

803. Wright David / de Hert Paul (édit.), *Enforcing Privacy : Regulatory, Legal and Technological Approaches*, 1e éd., Cham 2016, p. 7.

804. Parlement européen et Conseil de l'UE, *Directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2002, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0021&from=SV » (27/03/2020), pp. 33-50.

805. Ci-après « directive SRI pour sécurité des réseaux et systèmes d'information ».

de santé [806].

953 Quant au service numérique, il se définit comme tout service rendu normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Le destinataire de services pourra être une place de marché en ligne, des moteurs de recherche en ligne, ou un service informatique en nuage. Les entreprises en ligne doivent auto-évaluer si elles sont visées par les règles de cette directive.

954 Les fournisseurs des opérateurs de service essentiels sont également concernés par les obligations des opérateurs. Tous doivent se conformer à la loi de l'État membre où ils sont établis. Des différences entre États sont donc à prévoir.

VI. Le principe de loyauté et de transparence (article 5, al. 1, a) du Règlement)

955 L'article 5, al. 1, a) présente deux principes : le principe de loyauté et le principe de transparence.

956 Tout d'abord, le principe de loyauté (en allemand « Treu und Glauben », en anglais : « fairness ») renvoie à des considérations éthiques. Ainsi le traitement de données à caractère personnel doit correspondre aux finalités annoncées à la personne concernée. Des mesures appropriées aux risques doivent également être prises par le responsable du traitement.

957 Ensuite, ce principe de loyauté fait également référence au concept juridique de proportionnalité, en ce sens que seules les données nécessaires à la finalité du traitement doivent être collectées [807].

958 L'article 5, al. 1, a) traite d'un second principe : le principe de transparence. Celui-ci oblige le responsable du traitement à informer les personnes concernées du traitement de leurs données (art. 12 à 14 RGPD). Le Règlement précise la liste des informations à fournir à la personne concernée ou à son représentant légal (art. 13 et consid. 39 RGPD).

959 Les informations communiquées à la personne concernée doivent l'être de manière concise, transparente, compréhensible et doivent

806. Springer, *Encyclopedia of Cyber Warfare*, p. 138.
807. EDPS, *EDPS Guidelines on assessing the proportionality*, p. 3.

être aisément accessibles en des termes clairs et simples. Une attention particulière sera portée aux informations communiquées à des enfants [808].

L'application du principe de transparence nécessite une pesée des intérêts en présence [809]. 960

VII. Les données sensibles et judiciaires

Comme nous l'avons déjà évoqué précédemment, le Règlement prévoit des conditions spécifiques pour le traitement de certaines catégories de données [810]. 961

En principe, le Règlement interdit le traitement de ces données. Plus précisément, l'article 9, al. 1 du Règlement « interdit le traitement des données qui relève l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données concernant la santé, la vie, ou l'orientation sexuelle et le traitement des données génétiques et des données biométriques aux fins d'identifier une personne physique de manière unique ». 962

Par exception, le traitement de ces catégories de données est limité à certains fondements qui sont précisés à l'art. 9, al. 2 du Règlement. 963

Les États membres ont également le droit de poser d'autres conditions relatives aux données génétiques, biométriques ou de santé [811]. Les organisations qui traitent ces catégories particulières de données devront donc effectuer une veille juridique précise de l'évolution des droits nationaux [812]. 964

Le traitement des données concernant des enfants est soumis à une protection renforcée et à des conditions particulières [813]. Cet article exige l'obtention du consentement parental pour des services de la société de l'information offerts directement à un enfant âgé 965

808. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 157.
809. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 228.
810. art. 9, al. 2 RGPD.
811. art. 9, al. 4 RGPD.
812. Epiney Astrid, *Besonders schützenswerte Personendaten : zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage*, in : Mélanges en l'honneur de Paul-Henri Steinauer 2013, pp. 97-112.
813. art. 8 RGPD.

de moins de 16 ans. Ce plafond peut toutefois être fixé à un minimum de treize ans par un État membre et ne s'applique que lorsque le consentement serait fondé sur le consentement de l'enfant. Le consentement d'un mineur de moins de 13 ans ne peut donc pas être considéré comme valable.

966 Pour vérifier l'expression de l'autorité parentale, le responsable de traitement doit mettre en place des moyens techniques raisonnables afin de s'assurer de l'existence d'une telle expression [814].

967 Le recours à des technologies digitales comme l'intelligence artificielle permet de déduire des bases de données initiales certains attributs protégés.

968 Le traitement de données sensibles à l'ère digitale soulève deux types de défis. Tout d'abord, si des données non sensibles peuvent devenir des données sensibles, sur la base de la capacité à établir des déductions, alors la question se pose se savoir sous quelles conditions les données personnelles non-sensibles devraient être classifiées en tant que données sensibles [815]. Sandra Wachter propose de considérer comme premier critère l'intention de déduire de l'analyse des données personnelles des attributs sensibles. Elle propose ensuite de considérer la capacité attribuée aux données sources à permettre la déduction de données sensibles. Ces deux critères apparaissent pertinents. La création d'un index permettant de quantifier la confiance dans les bases de données utilisées serait particulièrement pertinente.

969 La multiplicité des technologies digitales et des méthodes d'accès aux données, par exemple le « web scrapping » rendent la conformité au Réglement difficile en pratique. Le web scrapping est un outil facilitant l'accès à des données personnelles pour en déduire un profilage de la personne concernée : par exemple, habitudes de vie, relations sociales, maladies par le biais de l'accès et l'analyse de ses données personnelles collectées par des objets connectés à Internet (données de géolocalisation enregistrées sur Iphone, IPad), ou des médias sociaux (contenus).

970 La licéité de la collecte revêt un caractère essentiel du fait de l'évolution des technologies digitales. La classification des données en

814. art. 8, al. 2 RGPD.
815. Wachter / Mittelstadt, *A right to reasonable inferences*, p. 567.

tant que données « sensibles » ou non perd en pertinence du fait de l'émergence d'un nouveau risque issu d'analyses déductives sur la base de la mise à disposition d'un grand nombre de données et de leur analyse par des technologies d'intelligence artificielle.

971 Ces analyses fondées sur les technologies d'intelligence artificielle facilitent les connexions entre individus sur la base de schémas non intuitifs. Elles augmentent le risque de discriminations [816], de dommages moraux (dans le domaine de la sphère privée, de la réputation) ou financiers, en particulier pour les minorités éthniques. Des logiciels d'intelligence artificielle sont spécifiquement développés sur la base de la reconnaissance faciale pour identifier l'éthnie des individus [817]. Cet exemple introduit l'idée d'une dimension collective de la vie privée. La discrimination pouvant toucher des groupes d'individus. Le droit européen relatif aux discriminations est uniquement applicable à des groupes définis par des attributs protégés historiquement (éthnicité, religion). Des individus regroupés de manière ad hoc sur la base de similarités (ex. : carte génomique, centres d'intérêts, réseaux sociaux...) n'entrent pas dans le champ d'application du droit européen relatif aux discriminations et peuvent donc être traités de manière discriminatoire. La reconnaissance d'un « droit à des déductions raisonnables » (en anglais reasonnable interferences) proposé par Sandra Wachter, pourrait constituer une solution contre les nouvelles formes de discrimination de l'ère digitale et contribuer à une protection de la sphère privée des groupes minoritaires. A condition que l'action civile soit facilitée pour ceux-ci [818].

972 Pour Sandra Wachter, le « droit à des déductions raisonnables » comblerait l'écart de responsabilité que posent actuellement les « déductions à risque élevé », c'est-à-dire celles tirées de l'analyse des Big Data qui portent atteinte à la vie privée ou à la réputation, ou qui ont une faible vérifiabilité au sens où elles sont prédictives ou fondées sur des opinions tout en étant utilisées dans des décisions

816. Mais il existe des garanties constitutionnelles en droit suisse, Thouvenin Florent, *Privatversicherungen : Datenschutzrecht als Grenze der Individualisierung ?*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019, p. 24.

817. Wang Cunrui, *Facial feature discovery for ethnicity recognition*, in : Wiley Interdisciplinary Reviews : Data Mining and Knowledge Discovery 2019 9/1, pp. 1-17.

818. Wachter / Mittelstadt, *A right to reasonable inferences*, p. 494-620.

importantes. Ce droit aux déductions raisonnables exigerait que le responsable du traitement des données fournisse une justification ex ante pour établir si une inférence est raisonnable. Cette justification porterait sur les points suivants :

1. pourquoi certaines données constituent-elles une base normalement acceptable pour tirer des conclusions ;
2. pourquoi ces conclusions sont pertinentes et normalement acceptables pour la finalité de traitement choisi ou le type de décision automatisée ; et
3. si les données et les méthodes utilisées pour tirer les conclusions sont exactes et statistiquement fiables.

La justification ex ante est renforcée par un mécanisme ex post supplémentaire permettant de contester les inférences effectuées considérées déraisonnables par la personne concernée [819].

973 Le Règlement pose des principes généraux dont la violation pourra justifier l'ouverture d'une action civile en responsabilité, comme le précise le paragraphe 1294. Cependant, il aurait été plus efficace de dégager un ou deux principes à partir desquels les opérateurs ajustent leur propre comportement [820].

819. *Ibidem.*
820. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. 28.

Deuxième partie

Les modalités de mise en œuvre extraterritoriale du règlement général sur la protection des données

Le Règlement européen vise à moderniser le cadre européen de la protection des données à caractère personnel afin de prendre en compte les avancées technologiques et de réduire les écarts juridiques entre les différentes législations des États membres de l'Union européenne. Il vise à renforcer la confiance des personnes concernées tout en encourageant l'innovation, l'activité économique et le développement des entreprises européennes. Il consacre de nouveaux concepts et impose aux organismes de revoir leur politique de conformité en matière de protection des données. 974

Enfin, le Règlement met en place un nouveau système de gouvernance des autorités de contrôle, basé sur le consensus et la coopération. Intégré dans le fond et décentralisé sur la forme, ce système permet aux autorités de contrôle de se saisir d'un dossier chaque fois qu'un de ses résidents est affecté par un traitement de données à caractère personnel. Les autorités adoptent des décisions conjointes aussi bien au stade de la mise en conformité qu'en matière répressive, sur les traitements transfrontaliers. Leur action est crédibilisée par des sanctions renforcées, jusqu'à 4 % du chiffre d'affaires mondial consolidé. 975

Le Règlement est composé de onze chapitres. Ces onze chapitres traitent des dispositions générales, des principes du Règlement, des droits de personne concernée, des obligations des responsables du traitement et des sous-traitants, de la sécurité du traitement et de l'analyse d'impact relative à la protection des données, du rôle du délégué à la protection des données, du rôle des codes de conduite et de la certification. Le Règlement aborde également la problématique du transfert de données vers des pays tiers ou des organisations internationales. Il précise le rôle des autorités de contrôle indépendantes et la façon dont elles coopèrent. Un chapitre entier est consacré aux voies de recours, régimes de responsabilités et sanctions. 976

Il est directement applicable pour les États membres de l'Union européenne. Son champ d'application extraterritorial constitue une nouveauté majeure, qui impacte aussi la Suisse. 977

Chapitre 1: L'analyse du cadre juridique spécifique entre la Suisse et l'Union européenne

§1 Les accords bilatéraux

I. Les aspects historiques

Comme en atteste le dialogue relatif à l'accord-cadre institutionnel entre la Suisse et l'UE [821], la Suisse entretient des liens étroits avec les États membres de l'UE, sans être membre de l'UE. Sa politique européenne est fondée sur des accords bilatéraux sectoriels. Ces accords bilatéraux sont essentiels pour la Suisse car ils préservent son accès au marché intérieur pour le commerce de biens et de services. Ils facilitent les échanges d'informations avec l'UE dans le domaine de la recherche et stimulent la compétitivité des entreprises suisses. En 2016, les exportations suisses vers l'Union européenne représentent plus de 43 % du total des exportations [822]. Cela signifie que la prospérité économique de la Suisse dépend de la qualité de sa coopération avec les États membres de l'UE. 978

Depuis l'accord de libre-échange de 1972, la Suisse poursuit une politique d'ouverture et de coopération avec les États de l'UE, sur la base d'accords bilatéraux. 979

II. La présentation des accords bilatéraux

La Suisse a conclu plusieurs accords bilatéraux. 980

Les premiers accords bilatéraux (I) datent de 1999. Lors d'une votation populaire, le peuple suisse a approuvé ces accords à 67 % des voix en date du 21 mai 2000. Ces accords sont entrés en vigueur 1er juin 2002 et contiennent sept accords. Ils concernent les 981

821. DFAE, *Politique européenne de la Suisse - Accord institutionnel*, in : Le Conseil fédéral (https ://www.dfae.admin.ch/), Berne 2019, p. « https://www.dfae.admin.ch/dea/fr/home/verhandlungen-offene-themen/verhandlungen/institutionelles-abkommen.html » (08/06/2019).

822. *Ibidem.*

domaines de la libre circulation des personnes, les transports terrestres, le transport aérien, les obstacles techniques au commerce, les marchés publics, la recherche et l'agriculture.

982 Le 26 octobre 2004, les Accords bilatéraux II ont été signés puis ratifiés par le Parlement suisse le 17 décembre 2004. Il s'agissait de huit accords, dont sept ont été soumis au référendum facultatif [823].

983 Ces accords traitent des domaines spécifiques suivants : Schengen / Dublin, l'échange automatique de renseignements en matière fiscale, la lutte contre la fraude, les produits agricoles transformés, l'environnement, la statistique, les pensions, l'éducation, la formation professionnelle et la jeunesse.

984 Depuis 2004, 6 accords bilatéraux ont été signés dans les domaines de la coopération policière et de justice (Europol et Eurojust), de la collaboration avec l'Agence européenne de défense, la Coopération entre les autorités en matière de concurrence, la navigation par satellite (Galileo et Egnos), et le Bureau européen d'appui en matière d'asile (EASO) [824].

985 Tous ces accords sont entrés en vigueur, à l'exception de l'accord sur la lutte contre la fraude.

986 Assurer la libre circulation des personnes entre l'Union et la Suisse sans harmoniser la législation sur la protection des données en Suisse est problématique à double titre : tout d'abord, les accords bilatéraux entre la Suisse et l'UE ont pour fondement l'obligation de reprendre en droit suisse les dispositions spécifiques des accords bilatéraux. En outre, le droit de l'UE pourrait être considéré comme une source d'inspiration pour le droit suisse de la protection des données (création de nouveaux instruments et développement ul-

823. DAE, *Politique européenne de la Suisse - Accords bilatéraux II*, in : Le Conseil fédéral (https ://www.eda.admin.ch/), Berne 2004, p. « https://www.eda.admin.ch/dea/fr/home/europapolitik/politique-europeenne/bilaterale-2.html » (30/10/2017).

824. DAE, *La politique européenne de la Suisse*, in : Le Conseil fédéral (https ://www.eda.admin.ch/), Berne 2020, p. « https://www.eda.admin.ch/dam/dea/fr/documents/fs/00-FS-Europapol-lang_fr.pdf » (27/03/2020).

térieur du droit de la protection des données en Suisse) [825].

Pour les traitements de données tombant dans le champ d'application des accords Dublin et Schengen, la Suisse a l'obligation de reprendre le corpus de règles de l'UE en matière de protection des données. En ce sens, le Règlement européen étend l'acquis communautaire de Dublin et Schengen [826]. 987

Les accords bilatéraux se fondent sur les deux principes suivants : 988

1. l'adéquation des législations entre la Suisse et l'UE (p. ex. suppression des obstacles techniques au commerce ou marchés publics)
2. la reprise de l'acquis communautaire (p. ex. transport aérien et Accords Schengen / Dublin).

Le Règlement sur la protection des données est uniquement applicable aux États membres de l'UE. Par conséquent, le Règlement n'est pas directement applicable à la Suisse. 989

La Suisse a cependant pris l'engagement de modifier sa loi fédérale sur la protection des données et de la mettre en conformité avec le Règlement, afin de conserver le bénéfice de la décision d'adéquation rendue par la Commission européenne. Cette décision rend licites tous les transferts de données à caractère personnel entre la Suisse et l'UE. La Suisse a également fait ce choix afin de ratifier le protocole de la Convention 108 sur le traitement des données automatisées. 990

La Suisse s'est engagée à transposer la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, en application des principes de la reprise de l'acquis communautaire [827]. 991

825. Kern Markus / Epiney Astrid, *Durchsetzungmechanismen im EU - Recht und ihre Implikationen für die Schweiz*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015, p. 43.
826. *Idem*, p. 44.
827. Conseil fédéral, *Accord du 26 octobre 2004 entre la Confédération suisse,*

§2 Les acquis de Schengen et de Dublin

992 Le 5 juin 2005 le peuple suisse a approuvé l'association de la Suisse aux coopérations de Schengen / Dublin par 54,6 % des voix [828]. La collaboration effective a débuté le 12 décembre 2008 et concerne les domaines de la justice, de la police, des visas et de l'asile.

993 Si les États membres de l'UE sont membres de Schengen, le Danemark, l'Irlande et le Royaume-Uni disposent d'un statut particulier. Quant à la Suisse, elle est qualifiée d'État associé avec l'Islande, le Liechtenstein et la Norvège.

I. L'acquis de Schengen

994 L'accord d'association à Schengen supprime d'une part les contrôles des personnes aux frontières intérieures de l'espace Schengen (sauf en cas de soupçon justifié) et renforce, d'autre part, l'efficacité de la lutte contre la criminalité grâce à une meilleure collaboration internationale dans les domaines de la justice et de la police [829]. Il facilite les voyages entre la Suisse et l'Union européenne (UE).

995 Les gardes-frontière suisses peuvent toutefois encore pratiquer des contrôles douaniers.

996 Une politique commune en matière de visas de courte durée a été instaurée pour harmoniser les critères de délivrance des visas.

997 Un système d'information sur les visas (VIS) a été mis en place en 2005. Il enregistre les empreintes digitales et la photographie des demandeurs.

998 Le système d'information Schengen (SIS) contient 63 millions d'en-

l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen (RS 0.362.31), in : Conseil fédéral (https ://www.admin.ch/), Berne 2004, p. « https://www.admin.ch/opc/fr/classified-compilation/20042363/index.html » (23/04/2017).

828. DAE, *Votation populaire du 5 juin 2005 - Arrêté fédéral portant approbation et mise en oeuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin*, in : Le Conseil fédéral (https ://www.eda.admin.ch/), Berne 2005, p. « https://www.eda.admin.ch/dea/fr/home/europapolitik/abstimmungen/schengen-dublin.html » (23/04/2017).

829. DAE, *Politique européenne de la Suisse - Accords et mise en oeuvre*, in : Le Conseil fédéral (https ://www.eda.admin.ch/), Berne 2018, p. « https://www.eda.admin.ch/dea/fr/home/bilaterale-abkommen/abkommen-umsetzung.html » (27/03/2020).

trées et favorise l'échange de renseignements entre juridictions. Cette base de données facilite la recherche d'objets et de personnes.

La protection des données du SIS et l'accès au système font l'objet de règles strictes dont le respect est vérifié par des autorités de contrôle nationales et cantonales indépendantes. Seul un cercle restreint de personnes est autorisé à accéder à ces informations [830]. 999

Le SIS enregistre tout traitement de données (accès, ajout ou suppression de données). Les données sont effacées lorsque le motif de signalement disparaît, et à l'expiration d'un délai fixe. Un droit d'information est octroyé à toute personne dont les données sont traitées dans le SIS. Elle peut demander l'effacement de son signalement et contester son exactitude. 1000

Le Règlement européen ne traite pas des aspects de protection des données du SIS. Ceux-ci sont abordés par la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. 1001

II. L'acquis de Dublin

L'accord d'association à Dublin garantit qu'une demande d'asile déposée par un demandeur n'est examinée que par un seul État dans l'espace Dublin pour faciliter le traitement des demandes. 1002

La base de données Eurodac collecte les empreintes digitales de tous les demandeurs d'asile. Les questions relatives au traitement des données relèvent de la directive (UE) 2016/680 et non du Règlement européen. 1003

Les accords bilatéraux ne peuvent être modifiés que d'un commun accord : ils ne font pas l'objet de modifications automatiques. Dans le cas des accords fondés sur l'équivalence des législations, les par- 1004

830. DFAE / DFE, *Schengen / Dublin*, in : Le Conseil fédéral (https ://www.sem.admin.ch/), Berne 2008, p. « https://www.sem.admin.ch/dam/data/sem/eu/fza/personenfreizuegigkeit/factsheets/2008/081211-fs2-f.pdf » (04/10/2017). Il s'agit de la police, du corps des gardes-frontière, des représentations suisses à l'étranger, des autorités chargées des migrations, du ministère public et des services des automobiles.

ties ont un intérêt commun à maintenir cette équivalence en cas d'évolution de leur droit. La reprise des développements de l'acquis communautaire pertinent pour un accord est généralement nécessaire pour garantir des conditions de concurrence égales pour les opérateurs des deux parties. En outre, la reprise est motivée par l'intérêt de maintenir les mêmes standards dans les domaines de la sécurité, de la santé, de l'environnement.

1005 Il apparaît cohérent de soutenir la doctrine de Dietrich Schindler qui considère que « la reprise de l'acquis communautaire impliquerait aussi la reprise de l'acquis jurisprudentiel, qui ferait partie de la substance normative [831] ».

1006 Sur le plan juridique, en matière de protection des données, la Suisse a fait le choix de donner la priorité à la révision de sa législation fédérale sur la protection des données. Elle vise ainsi à donner un cadre juridique uniforme, indépendamment des différences sectorielles des accords bilatéraux, dans un objectif de sécurité juridique. La Suisse vise à appliquer les dispositions de la Convention 108 et à ratifier son protocole additionnel, du fait de leur valeur juridique contraignante. Le Règlement général sur la protection des données et la directive européenne sur la protection des données se fondent sur les mêmes principes que la Conv. 108 modernisée et que son protocole. L'avant-projet de révision de la LPD s'inscrit en cohérence avec ces deux derniers textes. Cette stratégie de mise en conformité de la législation suisse avec la Convention 108 modernisée et avec le Règlement européen facilitera le maintien de la décision d'adéquation rendue par la Commission européenne et ainsi l'accès au marché européen pour les entreprises suisses.

III. La reprise du Règlement européen en droit suisse

1007 Cette offre de la mise en conformité du droit suisse ne se fait pas par une reprise de l'intégralité du Règlement européen.

1008 La question se pose de savoir pour quelle raison le Règlement eu-

831. Schindler Dietrich, *Die Europaverträglichkeit des schweizerischen Rechts*, 1e éd., Zürich 1990, p. 14 ; Pescatore Pierre, *Aspects judiciaires de l'acquis communautaire*, in : Revue trimestrielle de droit européen 1981 17/4, pp. 617-651.

ropéen n'est pas repris dans son intégralité en droit suisse [832].

Il nous semble en effet peu probable que la Suisse puisse conserver la décision d'adéquation à long terme, si elle n'adapte pas complètement sa législation interne au Règlement européen. La raison de cette opinion est le succès rencontré à ce jour par le Règlement européen au niveau international, le fait que selon notre appréciation, ce succès va aller en s'amplifiant, et que l'UE deviendra plus exigeante pour les décisions d'adéquation. 1009

Le Règlement européen devient en effet progressivement un standard de référence au niveau mondial [833]. Preuve en est le projet de loi fédérale sur la protection des données aux États-Unis, la révision de la loi californienne sur la protection des données et la reconnaissance d'une décision d'adéquation de la Commission européenne en faveur du Japon en 2019. 1010

La Suisse s'est trouvée confrontée à une situation similaire lors de l'adoption du Règlement européen relatif aux normes comptables IFRS (International Financial Reporting Standards) [834] qui modifiait les normes comptables suisses [835]. 1011

Avec beaucoup d'hésitations et de la réticence, la Suisse a adopté un droit très proche de ces normes comptables, après leur reprise par l'UE sous forme de Règlement. Ces normes normalisaient la présentation des comptes et étaient fondées sur de grands principes (« true and fair view » pour la présentation des comptes), comme avec le RGPD s'agissant du traitement des données. Elles visaient à augmenter la transparence et la comparaison mondiale des comptes 1012

832. Kern / Epiney, *Durchsetzungmechanismen im EU*, p. 44.
833. Deroudille Alexis / Fatah Farid, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, in : Revue du marche commun et de l'Union Européenne 2019, p. 442.
834. Commission européenne, *Règlement (UE) 2016/2067 du 22 novembre 2016 modifiant le règlement (CE) n° 1126/2008 portant adoption de certaines normes comptables internationales conformément au règlement (CE) n° 1606/2002 du Parlement européen et du Conseil, en ce qui concerne la norme internationale d'information financière IFRS 9*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R2067 » (31/12/2019), pp. 1-164.
835. Stiftung FER (édit.), *Swiss GAAP FER 2014/15 : Fachempfehlungen zur Rechnungslegung*, Zürich 2015 ; Voir aussi ATF 136 II 88, consid. 3.4.

annuels.

1013 L'absence de reprise du Règlement européen en droit suisse peut également s'expliquer par une absence de procédure de notification à la Suisse.

1014 Cette absence de reprise du Règlement européen en droit suisse peut se comprendre : l'UE a estimé qu'il ne s'agissait pas d'un développement de l'acquis de Schengen et que le principe d'adéquation des législations ne s'appliquait pas strictement.

1015 Si le Règlement (UE) 2016/1624 a été notifié à la Suisse le 22 septembre 2016 en tant que développement de l'acquis de Schengen, aucune notification n'a été envoyée à la Suisse concernant le Règlement européen. Le Parlement suisse a accepté le projet de reprise en droit interne du règlement (UE) 2016/1624 relatif au corps européen de garde-frontières et de garde-côtes, le 15 décembre 2017 et adopté une ordonnance d'exécution après sa notification. Il n'a pas procédé ainsi avec le Règlement européen.

1016 Cette absence de notification permet à la Suisse de justifier une lente adaptation de la LPD, tout en limitant le risque d'une décision de la Commission européenne de retirer sa décision d'adéquation octroyée à la Suisse de manière unilatérale.

1017 Les milieux économiques comme le Préposé fédéral à la protection des données se sont prononcés en faveur de la révision de la LPD et de l'harmonisation avec le Règlement européen [836].

836. Economiesuisse, *La coexistence de plusieurs normes en matière de protection des données pèse sur les entreprises suisses*, in : Economiesuisse (https://www.economiesuisse.ch/), Genève 2019, p. « https://www.economiesuisse.ch/fr/articles/la-coexistence-de-plusieurs-normes-en-matiere-de-protection-des-donnees-pese-sur-les » (20/06/2019).

Chapitre 2: Les éléments principaux

§1 Les acteurs

Le Règlement prévoit des obligations à la charge des responsables du traitement et des sous-traitants du secteur privé ou public établis dans l'UE, dès lors qu'ils traitent des données à caractère personnel. Dans le secteur privé, le Règlement s'applique aux entreprises privées, associations, fondations, syndicats et groupements d'intérêts économiques [837]. 1018

La vérification de la conformité à ces obligations se fait, selon le Règlement, *a posteriori* uniquement. Les personnes physiques concernées ne disposent en effet d'aucun élément préalable certifiant la qualité des traitements effectués par un responsable du traitement, lorsqu'elles partagent leurs données personnelles avec un acteur économique. Aucune autorisation explicite n'est octroyée par une autorité de contrôle. Si cela est compréhensible pour les traitements à faible risque, cela l'est moins pour les traitements présentant un risque élevé. 1019

Indépendamment du niveau de risque du traitement, tant le responsable du traitement que le sous-traitant, sont responsables conjointement et solidairement en cas de violation des obligations du Règlement. Il en résulte un changement de paradigme concernant le régime de responsabilité [838]. 1020

La directive 95/46/CE ne prévoyait pas de disposition spécifique pour le sous-traitant, permettant d'engager sa responsabilité. L'article 17 paragraphe 2 de la directive prévoyait uniquement que « le responsable du traitement [...] doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et doit veiller au respect de ces mesures ». En application de cet article, les obligations du sous-traitant étaient liées aux dispositions 1021

837. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 23.
838. Nerbonne Sophie, *Le nouveau rôle des autorités de contrôle*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 382.

contractuelles entre le maître du fichier et le sous-traitant.

1022 Avec le Règlement européen, le régime de responsabilité place les responsables du traitement et les sous-traitants sur un pied d'égalité en cas de litige et de sanctions [839]. Le sous-traitant peut être attaqué directement, comme le précise le paragraphe 1294. Et il peut également être demandé au responsable du traitement de s'acquitter du paiement de l'intégralité d'une sanction prononcée à l'encontre du sous-traitant, charge ensuite au responsable du traitement de se retourner contre son sous-traitant.

1023 Si le sous-traitant est basé en dehors de l'Union européenne, la responsabilité du responsable du traitement demeure engagée de la même manière (art. 3, al. 1 et 2 RGPD.). Cela est d'une importance pratique considérable. En effet, les sous-traitants établis en Suisse, ont un intérêt commercial à se mettre en conformité avec le Règlement afin de conserver leurs parts de marché dans l'UE et leurs contrats avec des responsables de traitement établis dans l'UE.

1024 Par conséquent, tant le responsable du traitement que le sous-traitant doivent prendre connaissance de la politique de protection des données de chacun. Ils doivent également vérifier la conformité des contrats au Règlement.

1025 En 2016, le programme britannique « care data », annoncé en 2013, a été abandonné. Il avait pour but de « faciliter l'accès à des données médicales personnelles, pseudonymisées, issues des médecins généralistes et leur interconnexion avec des données des hôpitaux, à des fins de recherche ». L'abandon de ce programme est dû au défaut de garanties dans le domaine de la « sécurité des données et des conditions de leur partage avec des parties tierces [840] ».

1026 Outre leur légalité, l'acceptabilité de tels projets est conditionnée par leur :

- « fiabilité, véracité, crédibilité des acteurs pour mériter la confiance, et
- accountability, responsabilité des décisions, et la capacité à

839. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 24.
840. Ministère français de l'Europe et des affaires étrangères, *Clap de fin pour le programme Care Data du NHS England*, in : Service ESRI (https://uk.ambafrance.org/), London 2017, p. « https://uk.ambafrance.org/Clap-de-fin-pour-le-programme-Care-Data-du-NHS-England » (01/08/2019).

en rendre compte [841]».

§2 Le renforcement des droits des personnes concernées

Le Règlement reprend les principes de la directive 95/46/CE et de la jurisprudence de la CJUE. Il renforce les droits existants [842] et attribue de nouveaux droits (« droit à l'oubli » et droit à la portabilité des données). Il octroie aux personnes physiques une maîtrise accrue sur leurs données personnelles. 1027

Ces droits seront exercés*a posteriori* par la personne concernée, après la réalisation du traitement et la connaissance d'une irrégularité, voire d'un dommage éventuel. Les conditions de l'action civile et la facilité d'accès à la justice sont donc des éléments déterminants de l'effectivité du droit à la protection des données. 1028

Les règles encadrant les droits des personnes sont définies aux art. 12, 13 et 34 RGPD pour les éléments de procédure [843]. 1029

Une organisation spécifique à la protection des données est donc requise ce qui nécessite des ressources humaines, financières et informatiques. 1030

« Le responsable du traitement doit notifier à chaque destinataire auquel les données ont été communiquées toute rectification ou tout effacement ainsi que toute limitation du traitement effectué, sauf si cela est impossible ou nécessite des efforts disproportionnés [844]». L'identité des destinataires à qui ses données à caractère personnel ont été divulguées peut être demandée par la personne concernée. 1031

Selon Mark Thompson, Global Privacy Chief de KPMG, rencontré à Londres, l'obligation de répondre aux demandes d'accès dans le délai d'un mois pourrait occasionner un dommage de réputation pour les entreprises concernées. Recevant un nombre élevé de demandes 1032

841. Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*, p. 4.
842. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016*, Chapitre III.
843. Kühling Jürgen / Buchner Benedikt (édit.), *Datenschutz - Grundverordnung / BDSG : Kommentar*, 2e éd., München 2018, p. 369.
844. art. 19 RGPD.

d'accès, elles ne pourraient pas répondre dans le temps imparti et pourraient être sanctionnées.

I. Le droit à l'effacement des données (« droit à l'oubli »)

1033 Le Règlement introduit un nouveau droit intitulé le droit à l'oubli (« Right to be forgotten ») [845]. Ce principe constitue une extension des dispositions de la directive 95/46/CE et une reconnaissance de la jurisprudence de la CJUE.

1034 La CJUE a décidé dans un arrêt C-131/12 sur renvoi préjudiciel des juridictions espagnoles, que « l'exploitant d'un moteur de recherche sur internet est responsable du traitement des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers [846] ».

1035 Mario Costeja Gonzalès, citoyen espagnol, a introduit une réclamation auprès de l'autorité espagnole pour la protection des données (AEPD) à l'encontre de la société Google. Quand un internaute recherchait le nom du plaignant dans le moteur de recherche Google, celui-ci affichait des liens vers deux pages d'un quotidien mentionnant une vente aux enchères d'immeubles pour recouvrir les dettes du plaignant. Ce dernier demanda à Google de supprimer ces données afin qu'elles disparaissent des résultats de recherche et du site du quotidien. L'AEPD a refusé la réclamation contre le quotidien, mais l'a admise concernant Google. Ce dernier a recouru contre cette décision, demandant son annulation [847].

1036 La CJUE a reconnu un droit à l'oubli. Elle précise qu'un « traitement licite de données exactes peut devenir (...) avec le temps incompatible avec la directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé ».

1037 Dans cette affaire, la question du droit à l'oubli se posait pour les moteurs de recherche. La CJUE a décidé que des moteurs de re-

845. art. 17 RGPD.
846. Arrêt CJUE du 13 mai 2014, *Google Inc. contre Agencia Española de Protección de Datos (AEPD)*, C-131/12, ECLI :EU :C :2014 :317, consid. 41.
847. *Idem*, consid. 2.

cherche pouvaient être qualifiés de responsables du traitement lorsqu'ils répertorient des informations contenant des données à caractère personnel et les « mettent à disposition » de leurs utilisateurs sous forme de liste de résultats de leur recherche [848].

La CJUE retient également que l'exploitant du moteur de recherche est responsable dès lors qu'il détermine les finalités et les moyens du traitement de données à caractère personnel. 1038

Selon cette jurisprudence, il n'est pas nécessaire que le moteur de recherche modifie ou soit conscient du fait que l'information est une donnée à caractère personnel. Le droit à l'oubli s'applique aussi si l'information est publiée initialement par un tiers. La décision de la CJUE précisait que les moteurs de recherche devaient supprimer les liens vers les données des personnes concernées sans que la personne concernée n'ait besoin de demander la suppression des liens à l'éditeur initial. L'arrêt Google Spain est un arrêt fondamental qui reconnaît le droit à l'effacement des données des individus selon des conditions particulières. 1039

En créant de nouveaux droits, Mme Anne Frison-Roche note avec justesse que la jurisprudence de la CJUE s'inscrit dans le cadre d'un contrôle ex ante, et que les acteurs économiques ont dû modifier leur comportement et s'adapter à cette jurisprudence. 1040

« La puissance de ce droit subjectif ad hoc est qu'il n'est pas besoin d'un dommage et que toute personne en tant de « sujet de droit actif » peut l'activer contre tout sujet de droit passif, ici toute personne par laquelle l'information est trouvable. En cela, un droit subjectif est par nature non limité par un territoire, est opposable à tous, peut être activé contre tous les titulaires passifs. C'est pourquoi la création de nouveaux droits subjectifs est prometteuse, les internautes ayant beaucoup utilisé leur droit à l'oubli [849] ». 1041

A contrario, le Règlement offre un contrôle *a posteriori* avec l'intervention des autorités de contrôle et l'ouverture d'actions en responsabilité. Il répond à une logique de réaction uniquement pour 1042

848. Arrêt CJUE du 13 Mai 2014, *Google Spain SL, Google Inc. V Agencia Espanola de Proteccion de Datos (AEPD)*, C-131/12, ECLI :EU :C :2014 :317.

849. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. « https://mafr.fr/fr/article/lapport-du-droit-de-la-compliance-dans-la-gouverna/ » (07/03/2020).

résoudre un problème spécifique.

1043 Le Règlement consacre formellement le droit à l'oubli, qui est un droit subjectif, « inventé par une juridiction parce qu'il était nécessaire pour sauvegarder la personne [850] ».

1044 Le groupe de travail de l'Article 29 de la Commission européenne a publié un avis sur ce thème, pour reconnaître l'importance de cette jurisprudence, et renforcer l'importance de cet arrêt [851].

1045 La proposition d'un droit à l'oubli automatique, c'est-à-dire d'un droit à l'oubli par défaut, a été formulée dans différentes cercles politques, institutonnels ou académiques pour accorder aux personnes concernées un droit automatique à l'oubli après expiration d'un certain délai [852].

1046 À quelles conditions et dans quel cadre temporel l'effacement des données peut-il avoir lieu ?

1047 L'article 17 répond à cette question. Il est d'une importance pratique considérable. « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement*dans les meilleurs délais*, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel *dans les meilleurs délais* » lorsque l'une des conditions suivantes est remplie :

(a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

(b) la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juri-

850. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. 62.

851. Article 29 Data Protection Working Party, *Update of Opinion 8/2010 of Article 29 Data Protection Working Party on applicable law in light of the CJEU judgement in Google Spain - Adopted on 16 December 2015 (WP 179 Update)*, in : European Commission (https ://ec.europa.eu/), Brussels 2015, p. « https : / / ec . europa . eu / justice / article - 29 / documentation / opinion - recommendation/files/2015/wp179_en_update.pdf » (27/03/2020), pp. 1-12.

852. de Terwangne Cécile, *Droit à l'oubli, droit à l'effacement ou droit au déréferencement ? Quand le législateur et le juge européen dessinent les contours du droit à l'oubli numérique*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 272.

dique au traitement ;

(c) la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;

(d) les données à caractère personnel ont fait l'objet d'un traitement illicite ; et

(e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis.

Cela signifie que le responsable du traitement a le devoir de supprimer les données personnelles sur demande explicite de la personne concernée ou non [853]. 1048

Même en l'absence d'une demande explicite, le responsable du traitement a le devoir de supprimer les données personnelles pour les cas cités à l'art. 17 al. 1 a, d et e. Lorsqu'il existe une raison de supprimer les données, la personne concernée peut demander la limitation du traitement sur la base de l'art. 18 RGPD en lieu et place du droit à l'effacement des données [854]. 1049

En juin 2019, Microsoft a supprimé plusieurs milliers de photos stockées dans des bases de données, car aucun consentement n'avait été demandé aux personnes concernées, ou bien, car les données étaient biaisées, ou encore les choix proposés aux personnes concernées étaient restrictifs ou orientés en vue d'une segmentation socialement dommageable [855]. Il avait été sensibilisé à la protection des données en 2017. En octobre 2017, l'autorité de contrôle néerlandaise avait en effet accusé la société Microsoft d'avoir omis « d'informer clairement » les utilisateurs de Windows 10 que ce système collecte en permanence des données personnelles [856]. 1050

Le Règlement précise que le droit à l'oubli n'est pas applicable si le traitement est nécessaire : 1051

853. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 441.
854. *Ibidem.*
855. Murgia Madhumita, *Microsoft quietly deletes largest public face recognition data set*, in : Financial Times (https ://www.ft.com/), London 2019, p. « https: / / www . ft . com / content / 7d3e0d6a - 87a0 - 11e9 - a028 - 86cea8523dc2 » (07/06/2019).
856. AWP, *Windows 10 accusé de violer la loi sur les données personnelles*, in : Bilan (http://www.bilan.ch/), Geneva 2017, p. « http://www.bilan.ch/entreprises /windows-10-accuse-de-violer-loi-donnees-personnelles » (28/02/2018).

(a) « à l'exercice du droit à la liberté d'expression et d'information ;

(b) pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

(c) pour des motifs d'intérêt public dans le domaine de la santé publique ;

(d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du-dit traitement ; ou

(e) à la constatation, à l'exercice ou à la défense de droits en justice ».

1052 Le Règlement adopte une interprétation large du droit à l'oubli et l'autorise dans un plus grand nombre de cas. L'arrêt Google Spain se limitait aux moteurs de recherche et aux recherches nominatives (sur la base du nom de la personne concernée).

1053 Ainsi, avec la mise en œuvre du Règlement, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant [857].

1054 Le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais [858].

1055 L'art. 19 RGPD introduit une obligation pour le responsable du traitement d'informer les tiers de l'effacement des données [859] « à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés ».

1056 Cet article est nuancé par l'art. 17 du Règlement qui précise que « le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables

857. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 450.
858. *Ibidem.*
859. *Idem*, p. 451.

du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci ».

Cet article appelle les remarques suivantes : 1057

- Si une personne concernée demande l'effacement des données collectées la concernant, en arguant qu'elles ne sont plus nécessaires aux finalités justifiant la collecte, le responsable du traitement devra prouver l'existence d'un rapport direct (« unmittelbar Zusammhang ») entre la conservation des données et la finalité de l'utilisation des données [860].
- Si le responsable du traitement parvient à justifier l'existence d'une finalité, qui rend licite la conservation des données, alors il n'existera plus d'obligation d'effacement des données [861].

La personne concernée pourra demander l'effacement de ses données lorsque le traitement est illicite. Les responsables du traitement auront intérêt à suivre avec attention la jurisprudence sur cette question pour être informés de la façon dont la CJUE interprète cette possibilité d'effacement et quels fondements pourront servir à l'effacement des données à caractère personnel. Une donnée inexacte ou encore le fait de ne pas avoir communiqué un élément d'information pertinent à la personne concernée pourrait potentiellement rendre le traitement des données illicite et donner lieu à l'effacement de ces données. 1058

Les obligations du responsable du traitement ne sont pas à minimiser. Si le responsable du traitement a publié les données à caractère personnel et qu'il est tenu de les effacer, il doit, compte tenu des technologies disponibles et du coût de mise en œuvre, prendre des mesures raisonnables, y compris d'ordre technique, pour informer les nouveaux responsables du traitement qui traitent ces données à caractère personnel de la demande d'effacement. 1059

Une notification publique sera-t-elle nécessaire ? Ce qui soulève la question du secret des affaires et de la protection de la sphère privée. 1060

Si l'objectif initial était d'effacer le nom d'une personne pour que celui-ci n'apparaisse pas dans la sphère publique, nous ne pouvons 1061

860. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 325.
861. *Ibidem.*

pas exclure que l'article 17 du Règlement augmente finalement la visibilité de la personne concernée du fait de la procédure de notification aux tiers, à qui les données de la personne concernée ont été communiquées. Les conséquences pratiques de cette notification videraient ainsi l'art. 17 du Règlement de son fondement initial.

1062 Le Règlement précise que le responsable du traitement initial n'est tenu de prendre que des «mesures raisonnables, compte tenu des technologies disponibles et des coûts de mise en œuvre».

1063 Comment interpréter cette notion ? Cette disposition autorise-t-elle le responsable du traitement initial à ne pas notifier les autres responsables du traitement ayant eu accès aux données ? Nous ne le pensons pas [862].

1064 En outre, les tiers conservent une obligation d'effacement des données personnelles lorsque l'une des conditions de l'art. 17 al. 1 du Règlement est remplie [863].

1065 La doctrine soulève enfin la question de savoir si la reconnaissance d'un droit à l'oubli ne va pas à l'encontre d'un droit « de mémoire » et d'un droit « d'accès à l'information ». Du fait de la structure décentralisée de l'Internet, « l'oubli » serait utopique [864] et les rappels aisés (sous forme de requêtes).

1066 En pratique, compte tenu de la structure mondiale du réseau internet et du champ d'application territorial du Règlement européen, la mise en œuvre effective du droit à l'oubli et à l'effacement des données sera vraisemblablement imparfaite [865].

1067 Le Règlement prévoit quelques exceptions au principe d'effacement des données [866] :

— si le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information ;

862. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 449.
863. *Idem*, p. 454
864. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 223.
865. *Ibidem* ; Arrêt CJUE du 24 septembre 2019, *GC e.a. contre Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, ECLI :EU :C :2019 :773 et Arrêt CJUE du 24 septembre 2019, C-507/17, ECLI :EU :C :2019 :772.
866. art. 17, al. 3 RGPD.

— pour respecter une obligation légale de l'Union ou d'un État membre ;

— pour respecter une mission d'intérêt public ou nécessaire à l'exercice d'une autorité publique ;

— pour des raisons de santé publique ;

— pour des raisons archivistiques, de recherche scientifique ou statistique (si toutes les conditions pour ce type de traitement sont remplies) ; et

— pour la constatation, l'exercice ou la défense de droits en justice.

En conclusion, lorsqu'une personne ne souhaite plus que les données qui la concernent soient traitées, et dès lors qu'aucun motif légitime ne justifie pas leur conservation, ces données doivent être supprimées. Cette logique s'inscrit en cohérence avec le principe de minimisation des données. Des exceptions sont cependant prévues par le Règlement, par exemple pour les données de recherche, pour l'exercice de la liberté d'expression et d'information, pour des motifs d'intérêt public dans le domaine de la santé publique, etc. (art. 17, al. 3 RGPD). 1068

II. Droit d'accès, art. 15 RGPD

Le Règlement reconnaît un droit d'accès des personnes concernées à leurs données personnelles [867]. Selon le Règlement, la personne concernée a le droit d'obtenir du responsable du traitement « la confirmation que des données à caractère personnel la concernant sont traitées, et lorsqu'elles le sont, l'accès à ces données ». Le responsable du traitement lui indique également les garanties appropriées en cas de transfert à l'étranger. Il fournit une copie des données à la personne concernée. La jurisprudence allemande vient de préciser qu'une synthèse pouvait être communiquée à la personne concernée et non pas la copie des documents [868]. 1069

Les informations communiquées doivent l'être formulées de ma- 1070

867. art. 15, al. 1 RGPD.

868. Elteste Ulrike / Van Quathem Kristof, *German court decides on the scope of GDPR right of access*, in : Inside Privacy (https://www.insideprivacy.com/), Washington D.C. 2019, p. « https://www.insideprivacy.com/international/european-union/german-court-decides-on-the-scope-of-gdpr-right-of-access/ » (10/08/2019).

nière claire et compréhensible, ce qui est parfois difficile en pratique, notamment pour la communication des fichiers logs. Ceux-ci contiennent des informations précieuses, mais sont difficilement compréhensibles pour des non-spécialistes. Les personnes concernées ont le droit d'obtenir une copie de leurs données, de la part du responsable du traitement.

1071 En droit suisse, le droit d'accès est déjà reconnu par la Loi fédérale du 19 juin 1992 sur la protection des données (R.S 235.1) [869].

1072 Ce droit comme l'ensemble des droits des personnes concernées est exercé à titre gratuit [870]. Cependant, le responsable du traitement est en droit de demander le paiement de toute copie supplémentaire, pour couvrir les coûts administratifs.

1073 Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour répondre aux demandes des personnes concernées dans le délai d'un mois (art. 12 RGPD).

1074 Le responsable du traitement doit informer la personne concernée et motiver sa décision si elle ne peut pas respecter le délai d'un mois. « Elle doit informer la personne concernée de son droit d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel [871] ». Une prolongation de délai de deux mois supplémentaires est possible si le dossier est complexe ou si l'entreprise reçoit de nombreuses demandes. L'entreprise peut aussi demander un complément d'information pour vérifier l'identité de la personne concernée [872].

III. Droit à l'information

1075 La personne concernée dispose d'un droit à l'information [873]. Afin de s'assurer que les données sont traitées de manière loyale et transparente, les responsables du traitement des données doivent communiquer un certain nombre d'informations aux personnes concernées relatives au traitement de leurs données à caractère person-

869. art. 8 de la LPD.
870. art. 12, al. 5, RGPD., sauf lorsque les demandes sont manifestement infondées ou excessives.
871. art. 12 RGPD.
872. art. 12, al. 6 RGPD.
873. art. 15, al. 1 a) à h) RGPD.

nel. Le Règlement précise les informations à fournir aux personnes concernées [874].

La personne concernée a le droit d'obtenir des informations concernant : 1076

- Les finalités du traitement ;
- Les catégories de données concernées ;
- Les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans les pays tiers ou les organisations internationales ;
- La durée de conservation des données à caractère personnel envisagée, ou à défaut les critères utilisés pour déterminer cette durée ;
- Toute information disponible quant à la source des données lorsque ces données ne sont pas collectées auprès de la personne concernée ; et
- L'existence d'une prise de décision automatisée (y compris un profilage), et dans ce cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

La personne concernée devra également être informée du traitement de ses données lors d'une nouvelle finalité non couverte par la notification initiale. 1077

Le devoir d'information doit se comprendre comme l'expression d'un traitement de données personnelles équitable et transparent [875]. 1078

Le Règlement précise que le responsable du traitement doit pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant. Ce droit doit s'exercer dans le respect des droits et libertés d'autrui, notamment le respect du secret des affaires ou la propriété intellectuelle. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informa- 1079

874. art. 15, al. 1 a) à h) RGPD.
875. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 180.

tions à la personne concernée [876]. Lorsque le responsable du traitement traite une grande quantité de données, il devrait pouvoir demander à celle-ci de préciser, avant de lui fournir les informations, sur quelles données ou quelles opérations de traitement sa demande porte. Notons que les considérants n'ont pas de force juridique contraignante et n'ont valeur que de recommandation.

1080 Lorsque les données de la personne concernée sont transférées vers un pays tiers, ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées offertes par le destinataire, concernant ce transfert [877].

1081 Les informations doivent être fournies sous une forme concise, transparente, compréhensible et aisément accessible, en utilisant des termes clairs et simples. Cela peut également se faire au moyen d'icônes normalisées [878].

1082 Si les données sont collectées auprès d'un tiers et non pas auprès de la personne concernée, celle-ci doit être informée de la source des données [879].

1083 Le Règlement prévoit cependant que la personne concernée ne pourra pas être informée si cette information représente pour le responsable du traitement une obligation impossible ou nécessiterait un effort disproportionné [880].

1084 Dans cette hypothèse, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles [881].

1085 Le Règlement pose également une exception à l'obligation de notification de la personne concernée, dans le cas où l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis [882]. Cette exception vaut également

876. Consid. 63 RGPD.
877. art. 15, al. 2 RGPD.
878. art. 12 et consid. 39 RGPD.
879. art. 14, al. 2, g) RGPD.
880. art. 14, al. 5 RGPD.
881. art. 14, al. 5 b) RGPD.
882. Paal / Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, p. 181.

pour les cas pour lesquels les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membres [883].

Le Règlement européen prévoit d'autres limitations à l'exercice de ce droit d'information, si le traitement est effectué à des fins journalistiques, scientifiques, artistiques ou littéraires (art. 85 al. 2 RGPD). 1086

À titre d'exemple, Microsoft pratique une politique très protectrice des droits des consommateurs. En avril 2016, la société Microsoft déposa une plainte à l'encontre du gouvernement américain, sur le fondement qu'il avait le droit d'informer les personnes concernées lorsque les agences du gouvernement américain demandaient l'accès à des documents personnels situés sur des serveurs distants. Cette démarche s'ajoute à celle de Microsoft d'informer les utilisateurs de courriers électroniques lorsque leurs comptes ont fait l'objet d'un accès par les gouvernements [884]. Ces démarche soulèvent la question de l'équilibre difficile à trouver entre les impératifs de cybersécurité, de sécurité nationale et des droits à la protection des données et de la vie privée. 1087

En l'absence d'exception, la violation du principe d'information de la personne concernée sera punissable d'une amende (art. 83. al. 5 RGPD). Une attention particulière doit être portée aux traitements ultérieurs effectués pour des finalités compatibles avec les finalités de la collecte initiale. Ce sera l'exemple des scoring, recommandations, diagnostics, prédictions et décisions automatisées. La personne concernée doit être informée de tout traitement ultérieur [885]. 1088

Cela ne vaut que si la personne concernée ignore ce traitement ultérieur. D'où l'importance de rédiger une déclaration sur la protection des données qui soit la plus exhaustive possible. 1089

Les personnes concernées sont informées des données traitées, mais aussi des méta-données [886]. Elles sont également informés de leurs droits et notamment de leur droit de recours [887]. Ce devoir d'infor- 1090

883. art. 14, al. 5, c) et d) RGPD.
884. Springer, *Encyclopedia of Cyber Warfare*, p. 180.
885. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 189.
886. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 421.
887. *Idem*, p. 423.

mation correspond aux art. 13 al. 2 b et d RGPD et art. 14 al. 2 c et e RGPD.

IV. Droit à la rectification des données

1091 Le Règlement donne le droit aux personnes concernées d'exiger du responsable du traitement qu'il rectifie, dans les meilleurs délais, des données à caractère personnel qui sont inexactes [888].

V. Droit à la portabilité des données

1092 Le Règlement prévoit un droit à la portabilité des données [889]. Ce droit ne peut être exercé que pour les traitements dont la licéité est fondée sur le consentement ou l'exécution d'un contrat [890].

1093 Les personnes concernées ont donc le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par une machine. Les personnes concernées ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données ont été communiquées y fasse obstacle.

1094 Il sera ainsi plus aisé pour les personnes concernées de transférer les données personnelles d'un prestataire de services, par exemple un réseau social, à un autre.

1095 Le droit d'accès permet déjà aux personnes concernées d'exiger que leurs données soient fournies sous une forme électronique fréquemment utilisée. La jurisprudence de la CJUE précise qu'il doit s'agir d'un « format intelligible permettant effectivement à la personne concernée de prendre connaissance des données, d'en vérifier l'exactitude et la conformité du traitement à la loi [891] ».

1096 Les informations seront livrées dans un « format structuré, couramment utilisé et lisible par machine ». La transmission des informations à un autre responsable du traitement est effectuée directement par l'entreprise ce qui crée un coût supplémentaire et néces-

888. art. 16, al. 1 RGPD. et consid. 65 RGPD.
889. art. 20 RGPD.
890. Consid. 68 RGPD.
891. Vérification de conformité à la directive 95/46/CE ; Arrêt CJUE du 17 juillet 2014, *Y.S. contre minister voor Immigratie*, C—141/12, C-315/2, ECLI :EU :C :2014 :2081 et ECLI :EU :C :2013 :838, consid. 57.

site le développement de nouveaux processus internes. La compatibilité des formats structurés, aussi appelée l'interopérabilité, entre les responsables du traitement pourrait poser des problèmes pratiques. Ce droit favorise la compétition en faveur de technologies favorables à la protection des données [892]. La concurrence entre acteurs économique est accrue et réduit le principe d'emprisonnement des données par un acteur économique (« lock-in effect ») [893].

Les codes de conduites sectoriels pour harmoniser les formats structurés et les rendre inter-opérables les uns envers les autres sont une « bonne pratique », facilitant la portabilité effective des données [894]. 1097

Dans le respect du principe de proportionnalité, le Règlement précise que le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés de tiers [895]. 1098

Le Règlement exclut le droit à la portabilité des données pour les responsables du traitement qui traitent les données à caractère personnel dans le cadre de leurs missions publiques [896]. 1099

Il ne devrait pas non plus s'appliquer lorsque le traitement des données à caractère personnel est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. 1100

Il est important de souligner que le droit à la portabilité des données ne porte pas atteinte au droit de la personne concernée d'obtenir l'effacement des données à caractère personnel. 1101

Le groupe de travail de l'Article 29 de la Commission européenne a publié des lignes directrices le 13 décembre 2016 sur le droit à la portabilité des données [897]. Ces lignes directrices précisent les conditions d'application de ce nouveau droit et fournissent des exemples 1102

892. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 243.
893. *Idem*, p. 244.
894. Consid. 68 RGPD.
895. art. 20, al. 4 RGPD.
896. art. 20, al. 4 RGPD.
897. Groupe de Travail de l'Article 29, *Lignes directrices sur la portabilité des données - Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017 (WP 242 rev.01)*, in : CNIL (https ://www.cnil.fr/), Paris 2016, p. « https: / / www . cnil . fr / sites / default / files / atoms / files / wp242rev01 _ fr . pdf » (29/12/2019).

concrets. Elles soulignent que ce droit ne se limite pas aux informations communiquées par la personne elle-même, mais doit se comprendre également de l'ensemble des informations « générées par ses activités ». Ce nouveau droit ne saurait ainsi se limiter à restituer les informations personnelles de la personne concernée.

1103 Compte tenu des volumes de données concernés, il faut que l'entreprise développe des processus internes permettant l'automatisation des demandes de portabilité des données.

1104 Le débat sur la portabilité des données soulève de nombreuses questions. Les représentants de l'industrie des technologies numériques en Europe ont dénoncé par exemple le manque de sécurité juridique, les coûts élevés de mise en œuvre de ce droit [898] La Suisse refusait d'intégrer ce droit dans son projet de LPD révisé, mais a finalement intégré ce droit en août 2019 lors des discussions devant la Commission des Institutions politiques du Conseil National (CIP-CN).

VI. Droit à la limitation du traitement

1105 Le Règlement introduit un nouveau droit à la limitation du traitement des données [899]. Ce droit intervient également *a posteriori* c'est-à-dire après la réalisation du traitement. Il n'existe aucun contrôle ex ante de la part des pouvoirs publics pour vérifier que le traitement ne fait pas courir de risques pour les personnes concernées, et ce quel que soit le niveau de risque des traitements effectués. La confiance est faite aux acteurs économiques de se comporter de manière loyale, responsable et de prendre les mesures de confiance, techniques et organisationnelles adaptées au niveau de risque des traitements de données à caractère personnel.

1106 En cas de manquement ou de violation de ce devoir de diligence (duty of care), la personne concernée peut faire valoir son droit à la minimisation du traitement. Celui-ci n'est cependant pas absolu et dans certains domaines spécifiques comme la recherche, ce droit ne

898. DigitalEurope, *Digitaleurope's views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242)*, in : DigitalEurope (https ://www.digitaleurope.org/), Brussels 2017, p. « https : / / www . digitaleurope . org / resources / position - paper - digitaleuropes - views - on - article - 29 - working - party - draft - guidelines - on - the - right - to - data - portability-wp-242/ » (15/12/2019).

899. art. 18 RGPD.

peut pas être mis en œuvre, dans une logique de pesée des intérêts.

Ce droit s'applique lorsque : 1107

- L'exactitude des données est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
- Le traitement est illicite et la personne concernée s'oppose à l'effacement et exige la limitation de leur utilisation ;
- Le responsable n'a plus besoin des données à caractère personnel aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice, ou la défense de droits en justice ; et
- La personne s'est opposée au traitement de ses données en vertu de l'art. 21, al. 1, RGPD. et le responsable du traitement a besoin de temps pour vérifier si ses motifs légitimes prévalent sur ceux de la personne concernée.

Une personne qui a obtenu la limitation du traitement est informée par le responsable du traitement avant la levée de cette limitation [900]. 1108

La limitation du traitement peut consister en un déplacement temporaire des données vers un autre système de traitement, en une suppression d'accès aux utilisateurs ou en un retrait temporaire des données publiées d'un site internet [901]. 1109

Les moyens techniques favorisent la traçabilité du traitement et limitent le risque d'un traitement ultérieur illicite à l'insu de la personne concernée. Cependant, seule une action civile ultérieure de la personne concernée ou d'un groupe de personnes voire une autosaisine de l'autorité de contrôle pourra effectivement contrôler le respect de cette obligation. 1110

Si la personne exerce son droit à la limitation des données, le responsable du traitement peut conserver les données « mais ne pourra pas utiliser ces données pour des traitements ultérieurs, à moins d'avoir obtenu le consentement de la personne concernée, ou si le 1111

900. art. 18, al. 3 RGPD.
901. Consid. 67 RGPD.

traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice ».

1112 Cependant, les données peuvent faire l'objet d'un traitement ultérieur « pour protéger les droits d'une autre personne physique ou morale ou pour des motifs importants d'intérêt public ».

1113 En pratique, la mise en œuvre de ce droit impose au responsable du traitement qu'il notifie à « chaque destinataire auquel les données ont été communiquées, que le traitement est limité, sauf si ceci est impossible ou nécessite un effort manifestement disproportionné [902] ». Les entreprises soulèveront vraisemblablement cette exception pour contourner cette notification.

VII. Droit d'opposition

1114 Le Règlement accorde aux personnes concernées un droit d'opposition. Il ne s'agit cependant pas d'un droit général. Le Règlement autorise les personnes concernées à s'opposer au traitement de leurs données à caractère personnel dans trois situations spécifiques uniquement [903].

1115 La *première* situation concerne les données à caractère personnel qui sont traitées à des fins de prospection. Dans cette situation, la personne a le droit de s'opposer à tout moment au traitement des données la concernant à de telles fins de prospection (y compris au profilage, dans la mesure où il est lié à une telle prospection).

1116 La *seconde* situation concerne le traitement à des fins de recherche scientifique, historique ou à des fins statistiques. La personne concernée ne dispose pas ici d'un droit absolu. Elle doit justifier qu'elle a des raisons tenant à la situation particulière de la personne concernée. Le responsable du traitement pourra s'y opposer et continuer le traitement des données, au motif que le traitement est nécessaire pour l'exécution d'une mission d'intérêt public. Ceci constitue une nouveauté RGPD.

1117 La *troisième* situation concerne le traitement pour des motifs légitimes [904] ou parce qu'il est nécessaire pour remplir une mission

902. art. 19 RGPD.
903. art. 21 RGPD.
904. art. 6, al. 1, f) RGPD.

d'intérêt public [905]. La personne concernée doit démontrer qu'elle dispose de raisons particulières spécifiques au cas d'espèce qui justifient une dérogation [906]. Il ne s'agit pas d'un droit absolu. Le responsable devra interrompre le traitement, à moins qu'il ne démontre des motifs légitimes et impérieux qui prévalent sur les intérêts de la personne concernée ou si le traitement nécessaire est pour la constatation, l'exercice ou la défense de droits en justice.

Ce droit s'exerce uniquement *a posteriori* après constatation d'une irrégularité ou réalisation d'un dommage. Ni l'autorité de contrôle ni la personne concernée ne disposent d'un droit d'opposition ex ante, avant le traitement. Pour les applications à risques élevés comme la mise sur le marché de voitures autonomes ou de diagnostics médicaux fondés sur l'analyse de données, une autorité de sûreté qui délivre les autorisations (Service des automobiles ou Swissmedic) pourrait se concerter avec l'autorité de contrôle dans le domaine de la protection des données pour vérifier si les conditions légales sont remplies (consentement, information, privacy-by-design...), préalablement au traitement. 1118

Certaines garanties sont offertes aux personnes concernées lors d'une action civile *a posteriori*. Ainsi, la charge de la preuve est inversée par rapport à la directive 95/46/CE. Il incombe désormais au responsable du traitement de démontrer qu'il dispose de motifs fondés juridiquement pour continuer le traitement. À défaut, il doit interrompre le traitement. 1119

Le considérant 70 précise que « lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment et sans frais, de s'opposer à ce traitement, y compris le profilage. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information ». 1120

La doctrine considère que le droit d'opposition est un droit absolu, qui peut être exercé à tout moment [907]. « Dès que la personne concernée s'y oppose, le traitement des données doit être inter- 1121

905. art. 6, al. 1, e) RGPD.
906. Schneider, *Datenschutz*, p. 204.
907. *Ibidem.*

rompu ».

1122 Cependant, la jurisprudence de la CJUE considère qu'il faut « tenir compte de manière plus spécifique de toutes les circonstances entourant la situation de la personne concernée [908]». Elle rappelle ainsi l'importance du principe de proportionnalité et d'une pesée des intérêts en présence.

VIII. Profilage et décisions automatisées

1123 Le Règlement définit le profilage comme étant : « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser, ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation, ou les déplacements de cette personne physique [909]».

1124 Quant aux décisions automatisées, elles sont définies à l'article 22 du Règlement par la négative : « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ».

1125 Le Groupe de travail de l'Article 29 de la Commission européenne a publié des lignes directrices sur le thème des décisions prises sur une base automatisée et sur le profilage, en octobre 2017, pour faciliter l'interprétation des dispositions du Règlement [910].

A. La notion de décision automatisée

1126 Le groupe de travail de l'art. 29 de la Commission européenne a confirmé dans ses lignes directrices :

908. Arrêt CJUE du 9 mars 2017, *Salvatore Manni*, C—398/15, consid. 47, ECLI :EU :C :2017 :197.
909. art. 4, al. 4, RGPD.
910. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - Adopted on 3 October 2017, Last Revised and Adopted on 6 February 2018 (WP 251 rev.01)*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 » (29/10/2018).

— le principe d'interdiction des décisions prises sur une base uniquement automatisée, y compris en matière de profilage.

— l'existence d'exceptions au principe.

— la nécessité de mettre en place des mesures pour sauvegarder les droits des personnes concernées, leurs libertés et intérêts légitimes.

(a) Le principe d'interdiction

Le Règlement pose le principe d'interdiction des décisions prises sur une base automatisée. Ce principe n'est applicable que lorsque la décision est uniquement fondée sur un processus automatisé (profilage compris), a un effet juridique ou affecte un individu de manière significative [911]. 1127

De nombreuses décisions affectant les individus sont prises sur une base automatisée : évaluation de la capacité de crédit, embauche et licenciements [912] et peuvent représenter un risque pour la dignité humaine.[913] Le groupe Amazon est attaqué pour avoir licencié certains salariés sur la base de décisions automatisées sans intervention humaine [914]. 1128

(b) Les exceptions

« Le responsable du traitement ne doit pas prendre de décision sur une base uniquement automatisée, à moins que certaines conditions soient remplies et le caractère nécessaire, interprété stricte- 1129

911. Veale Michael / Van Kleek Max / Binns Reuben, *Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making*, in : Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York 2018, p. 440.
912. Kaminski Margot E., *Binary Governance : Lessons from the GDPR's Approach to Algorithmic Accountability*, in : Southern California Law Review 2019 92/6, p. 138 ss.
913. *Idem*, p. 138.3.
914. Favre Cléa, *Comment les employés d'Amazon peuvent être virés par un robot*, in : RTS (https ://www.rts.ch/), Genève 2019, p. « https://www.rts.ch/info/economie/10403387-comment-les-employes-d-amazon-peuvent-etre-vires-par-un-robot.html » (07/06/2019).

ment, démontré [915]».

1130 En application de la jurisprudence constante de la CJUE, le responsable du traitement doit pouvoir démontrer que le profilage est nécessaire et qu'il respecte le principe de proportionnalité et la pesée des intérêts en présence. Il doit également considérer l'existence d'autres méthodes moins intrusives, du point de vue de la protection de la sphère privée [916].

1131 Plus précisément, il ressort du Règlement (art. 22, al. 2 RGPD) que : « les décisions prises sur une base complètement automatisée seront valables lorsqu'elles sont nécessaires à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement » ; Ces décisions prises sur une base complètement automatisée seront également valables lorsqu'elles sont « autorisées par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ».

1132 Les décisions automatisées sont autorisées pour « contrôler et prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des institutions de l'Union ou des organes de contrôle nationaux, et lorsqu'elles visent à assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement (consid. 71 RGPD) ».

1133 Elles sont également licites lorsque la personne a consenti à cette prise de décisions sur une base uniquement automatisée. La lecture et la compréhension des contrats sont donc essentielles. Sur ce point, les lignes directrices du groupe de travail de l'art. 29 soulignent la nécessité que le consentement soi confirmé par une dé-

915. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 12 ; Groupe de Travail de l'Article 29, *Avis 06/2014 du Groupe de travail de l'Art. 29.*

916. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 12 ; EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data : A Toolkit*, in : EDPS (https ://edps.europa.eu/), Brussels 2017, p. « https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf » (24/04/2017).

claration formelle.

Le règlement consacre un « véritable droit subjectif de la personne de ne pas faire l'objet d'une décision automatisée, dès lors qu'elle serait négative ». On passe donc d'une interdiction à la reconnaissance d'un véritable droit [917]. Cependant, ce droit s'exerce *a posteriori* et aucun contrôle des autorités n'est effectué ex ante pour vérifier que les responsables du traitement respectent ce droit. La personne concernée dispose de peu d'éléments à ce jour, pour évaluer la loyauté des traitements de données personnelles des entreprises. Par conséquent, il existe une insécurité juridique sur ce point précis et un effort de transparence est recommandé par les entreprises pour communiquer sur cet élément essentiel à la construction de la confiance. Les codes de conduite approuvés par l'autorité de contrôle revêtent ainsi une grande importance. 1134

Le responsable du traitement peut communiquer aux personnes concernées que des « mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée »ont été prises (art. 22, al. 3 RGPD). La doctrine confirme que cette obligation doit « au moins » se traduire par le respect du « droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision [918]». L'art. 22 RGPD consacre ainsi le droit à une intervention humaine en cas de décisions prises sur une base automatisée. En outre, une forme de principe de contradictoire est instauré au travers du droit d'exprimer son point de vue et contester la décision. Ce principe sera cependant dépendant du respect de l'obligation d'information de la personne concernée. Il faut en effet que la personne concernée sache au préalable qu'elle a fait l'objet d'un traitement automatisé, avant de pouvoir exercer ses droits. L'article 15 h RGPD reconnaît le droit d'être informé de l'existence d'une prise de décision automatisée. 1135

Rolf Weber propose l'inscription d'un droit à l'information dans la Constitution [919]. La consécration d'un droit à l'information, au sens d'un droit de savoir pour les personnes concernées, au niveau constitutionnel, serait un pré-requis nécessaire à l'exercice 1136

917. Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*, p. 9.
918. *Ibidem.*
919. Weber Rolf H., *Internet of things : Privacy issues revisited*, in : Computer law & security review 2015 31/5, pp. 618-627.

des autres droits [920]. Inversement, la reconnaissance d'un droit de ne pas savoir, au niveau constitutionnel, renforcerait pour les personnes physiques, l'effectivité du droit à l'auto-détermination informationnelle, en particulier dans le domaine de la santé (diagnostics médicaux).

1137 La question de savoir si cet article 22 RGPD consacre un droit d'explication est discutée en doctrine [921]. Il est cependant essentiel de reconnaître ce droit [922].

1138 La transparence des algorithmes, revendiquée par certains a pour but d'offrir des garanties de protection aux individus á l'encontre de systèmes opaques capables de prendre des décisions ayant un impact juridique ou significatif, en toute autonomie. A contrario, obliger les acteurs économiques à expliquer la logique des algorithmes pourrait constituer une violation forcée du secret d'affaire [923].

(c) Les garanties à mettre en place pour le responsable du traitement

1139 Comme aucun contrôle ex ante n'est imposé aux responsables du traitement préalablement au traitement de données personnelles, contrairement à d'autres activités (autorisation de mise sur le marché des médicaments, des véhicules automobiles...), le Règlement impose au responsable du traitement de respecter non seulement certains principes (art. 5 RGPD) [924] mais aussi de prendre des mesures spécifiques pour garantir le respect des droits, des libertés et des intérêts légitimes des personnes concernées (consommateurs,

920. Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*, p. 9.

921. Goodman Bryce / Flaxman Seth, *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"*, in : AI magazine 2017 38/3, p. 53 ; Wachter Sandra / Mittelstadt Brent Daniel / Floridi Luciano, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in : International Data Privacy Law 2017 7/2, p. 99 ; Selbst Andrew D. / Powles Julia, *Meaningful information and the right to explanation*, in : International Data Privacy Law 2017 7/4, p. 196.

922. Pégny Maël / Thelisson Eva / Ibnouhsein Issam, *The Right to an Explanation : An Interpretation and Defense*, in : Delphi - Interdisciplinary Review of Emerging Technologies 2019 2/4, pp. 1-7.

923. Picht Peter Georg / Loderer Gaspare, *Framing Algorithms – Competition Law and (Other) Regulatory Tools*, in : Max Planck Institute for Innovation & Competition Research Paper 2018, p. 10.

924. Voir point 848.

citoyens).

Cela ressort du considérant 71 : « un traitement de ce type devrait être assorti de garanties appropriées : 1140

- information spécifique de la personne concernée,
- droit d'obtenir une intervention humaine,
- droit d'exprimer son point de vue,
- droit d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation,
- droit de contester la décision.
- Cette mesure ne devrait pas concerner un enfant ».

Ces éléments sont en outre mentionnés dans les lignes directrices du groupe de travail de l'art. 29 de la commission européenne, ce qui leur confère une force contraignante supplémentaire. 1141

Concrètement le groupe de travail de l'art. 29 de la Commission européenne impose trois obligations au responsable du traitement : 1142

- il doit dire à la personne concernée que l'organisation recourt à ce type d'activité (profilage, décisions automatisées) ;
- il doit fournir à la personne concernée des renseignements significatifs à propos de la logique utilisée dans le processus de prise de décision ; et
- il doit expliquer la signification et les conséquences envisagées pour ce type de traitement.

Ces éléments peuvent figurer dans un code de bonnes pratiques sur la protection des données. 1143

Concernant la logique utilisée, le groupe de travail de l'art. 29 de la Commission européenne, exige du responsable du traitement « qu'il trouve un moyen simple de dire à la personne concernée quel est le raisonnement utilisé ou les critères sous-jacents à la prise de décision, sans pour autant recourir à une explication complexe des algorithmes utilisés, ni révéler l'algorithme entier. L'information communiquée doit cependant être utile à la personne concer- 1144

née [925]».

1145 L'état de l'art ne permet pas encore d'expliquer la logique de certains algorithmes de deep learning. Certaines décisions peuvent donc être prises par des algorithmes opaques. La question de la transparence des algorithmes est au cœur d'enjeux de confiance. Les algorithmes d'IA se fondent en effet sur des corrélations et non pas sur des causalités, dont le résultat ne peut être ni prédit ni expliqué [926]. La communauté scientifique se sent concernée par cette problématique [927]. Le droit de contestation est donc d'une importance cruciale, car l'effectivité du droit d'explication dépendra de la capacité technologique à explorer le lien entre les inputs et les outputs des systèmes d'apprentissage machine [928].

1146 Agata Ferreti distingue trois types d'opacité : l'opacité quant à l'existence même d'une décision prise sur une base automatisée, l'opacité en lien avec l'interprétabilité du système de prise de décision automatisée et l'opacité épistémologique [929].

1147 Résoudre l'opacité des algorithmes constitue un défi majeur pour que les décisions prises sur une base automatisée soient interprétables. Il s'agit d'un défi technique aux enjeux politiques majeurs [930]. Afin de renforcer la confiance de l'ensemble des acteurs, il serait souhaitable que ces systèmes dynamiques et exploratoires reçoivent un label de qualité et soient associés à une notation afin d'en évaluer le degré de transparence [931].

1148 Le groupe de travail de l'art. 29 de la Commission européenne précise dans ses lignes directrices que le concept de « décisions prises

925. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 14.
926. Aha David W. / Darrell Trevor / Pazzani Michael / Sammut Claude / Stone Peter, *Workshop on Explainable AI*, in : IJCAI 2017, Melbourne 2017.
927. Bugnion Edouard / Mogenet Emmanuel / Salathé Marcel, *Panel de discussion à la conférence des 30 et 31 janvier 2017*, in : Applied Machine Learning Days 2017, Lausanne 2017.
928. Thelisson Eva, *Towards Trust, Transparency, and Liability in AI/AS Systems*, in : Proceedings of the 26th International Joint Conference on Artificial Intelligence, Melbourne 2017, pp. 5215-5216.
929. Ferretti Agata / Schneider Manuel / Blasimme Alessandro, *Machine Learning in Medicine : Opening the New Data Protection Black Box*, in : European Data Protection Law Review 2018/4, pp. 320-332.
930. Pégny / Thelisson / Ibnouhsein, *The Right to an Explanation*, p. 2.
931. Thelisson, *Towards Trust, Transparency, and Liability*, pp. 5215-5216.

uniquement sur une base automatisée » signifie qu'il n'y a aucune intervention humaine dans le processus de prise de décision [932]. Cette intervention humaine doit avoir du sens et « ne saurait se limiter à un geste symbolique ». La personne désignée doit avoir « l'autorité et la compétence pour changer la décision sur la base d'une analyse des données entrantes (input) et des données sortantes (output) ».

1149 Le Règlement reconnaît qu'une décision prise sur une base automatisée peut avoir des effets « juridiques » ou des « effets significatifs » pour la personne concernée. Le Règlement ne définit pas ces deux notions. Les lignes directrices du groupe de travail de l'art. 29 de la Commission européenne apportent des précisions. Ainsi, un « effet juridique » suggère « une activité de traitement qui a un impact sur les droits d'une personne, tels que le droit de s'associer avec autrui, le droit de vote ou encore le droit d'intenter une action en justice [933]». Un effet juridique peut également affecter le statut juridique d'une personne, ou ses droits. Les lignes directrices citent l'exemple d'une personne qui se verrait déconnectée automatiquement de son service de téléphonie (rupture de contrat) pour avoir oublié de payer son abonnement de téléphone, avant son départ en vacances. Si la décision automatisée ne produit aucun effet juridique, elle peut cependant entrer dans le champ d'application de l'article 22, dès lors qu'elle produit un effet équivalent ou significatif sur les personnes concernées. La décision doit avoir le potentiel d'influencer significativement les « circonstances, les comportements et les choix » des personnes concernées. Dans le pire des cas, la décision pourra avoir pour conséquence de créer des « effets discriminatoires » ou donner lieu à « l'exclusion des personnes concernées ».

1150 Ces dispositions ne consacrent pas directement des principes éthiques de transparence des décisions automatisées ou de loyauté des algorithmes. Si le règlement général consacre un droit d'explication, celui-ci est limité du fait des exceptions de l'art. 22, al.2. Le Règlement européen consacre une obligation de rendre compte du fait de son article 5 RGPD. Il reconnaît un principe de transparence ou

932. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 9.

933. op.cit., lignes directrices Art. 29, WP 251.

loyauté algorithmique, mais qui n'est pas absolu [934].

1151 La seule référence à un « droit d'explication » peut être trouvée au considérant 71 ce qui pourrait à l'avenir fonder une interprétation extensive de l'article 22. Également, l'article 15 h) précité prévoit que la personne concernée a le droit d'obtenir du responsable de traitement des informations sur l'existence d'une prise de décision automatisée, y compris un profilage, visé à l'article 22, paragraphes 1 et 4, mais aussi « au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». On peut donc dire que le règlement général sur la protection des données n'aborde pas directement le principe de transparence algorithmique.

1152 La notion de Big Data ne figure pas explicitement dans le Règlement. Il existe donc une contradiction dans le texte. Le Règlement entend réglementer les décisions prises uniquement sur une base automatisée, mais non pas les données de grande dimension (Big Data) ni les traces laissées par les personnes privées lors de l'utilisation des technologies digitales, sur la base desquelles des décisions personnalisées sont prises.

1153 En principe, le traitement de données anonymisées est exclu du champ d'application du Règlement [935]. Cependant, si la technologie permet la ré identification des données anonymisées, les dispositions du Règlement seront applicables [936] et la responsabilité du responsable du traitement demeure engagée en cas de litige. Celui-ci devra prouver la conformité de ses traitements de données personnelles au Règlement en cas de doute concernant la ré identification ultérieure des données.

934. Goodman / Flaxman, *Right to Explanation*, p. 53 ; Goodman Bryce W., *A Step Towards Accountable Algorithms ? : Algorithmic Discrimination and the European Union General Data Protection*, in : 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona 2016, pp. 1-9 ; Hildebrandt Mireille, *The New Imbroglio - Living with Machine Algorithms*, in : Janssens Liisa (édit.), *The Art of Ethics in the Information Society*, 1e éd., Amsterdam 2016, pp. 55-60 ; Wachter / Mittelstadt / Floridi, *Why a right to explanation of automated decision-making does not exist*, p. 99.

935. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 364.

936. *Ibidem.*

B. La spécificité du profilage effectuée sur la base du consentement explicite ou d'un contrat

Lorsque le profilage est effectué sur la base du consentement explicite de la personne concernée ou de l'exécution d'un contrat, le responsable du traitement doit prendre « des mesures appropriées pour la sauvegarde des intérêts légitimes de la personne concernée ». 1154

La personne concernée peut exiger une «intervention humaine» pour comprendre la décision prise à son encontre et éventuellement la contester en exerçant son droit d'être entendu avant de s'y opposer. 1155

C. Traitement automatisé licite

Le responsable du traitement doit pouvoir démontrer que des garanties sont offertes aux personnes concernées dans le cas des traitements effectués lors d'activités étatiques. C'est notamment le cas des traitements de données ayant pour finalité la « prévention des fraudes et de l'évasion fiscale ». La sauvegarde des intérêts légitimes des personnes concernées doit également être prise en considération dans la logique du principe de proportionnalité et de pesée des intérêts en présence de la jurisprudence de la CJUE [937]. 1156

D. Les données sensibles

Si des données sensibles sont analysées sur une base automatique et engendrent la prise de décisions automatisées, alors le consentement explicite de la personne concernée est impératif, à moins de justifier de motifs d'intérêt public importants, sur la base du droit de l'Union ou d'un État membre. 1157

À titre d'exemple, Dubai a pour objectif d'effectuer le séquençage d'ADN de tous ses résidents pour des motifs d'intérêt public (projet Dubai Genomics) [938]. Si des acteurs privés accèdent aux données, comme des compagnies d'assurance, alors le risque de pratiques discriminatoires, sur la base de la carte génétique de la personne concernée, est à prendre au sérieux. Si des fournisseurs de ser- 1158

937. Consid. 71 RGPD.

938. Dubai Genomics, *What is Dubai Genomics ?*, in : Dubai Genomics (https://www.dha.gov.ae/), Dubai 2019, p. « https://www.dha.gov.ae/en/Pages/DubaiGneomicsAbout.aspx » (02/08/2019).

vices de stockage comme Amazon, Google ou Microsoft revendent ces données à des tiers, le risque de dommage pour les personnes concernées pourrait également être élevé.

E. Le cas spécifique des mineurs

1159 Le législateur européen prévoit des dispositions spécifiques pour les mineurs de moins de 16 ans. Le responsable du traitement doit obtenir le le consentement des parents pour tout traitement de données personnelles lors de services en ligne. Cette limite d'âge est indicative et peut être modifiée par les responsables du traitement. Dès l'âge de 13 ans, il peut donner son consentement de manière valable.

F. Les applications Blockchain

1160 En application du principe de neutralité technologique [939], consacré en droit suisse, les droits des personnes concernées ne devraient pas varier en fonction de la technologie utilisée.

1161 Les données stockées sur une plateforme décentralisée comme la Blockchain (voir partie 1.2.2) de même que les clefs publiques constituent des données personnelles [940].

1162 Si en principe, chaque personne concernée peut exercer ses droits envers chaque « noeud » de le Blockchain, ces nœud ne peuvent pas traiter des demandes de rectification ou de suppression de données [941]. De même, le consentement via la Blockchain semble difficile à obtenir en pratique (art. 4, al. 11 RGPD).

1163 La mise en œuvre du principe de minimisation des données (art. 5, al. 1, b RGPD) paraît difficilement applicable avec cette technolo-

939. CNUDCI, *Loi type de la CNUDCI sur le commerce électronique (1996) avec article 5 bis tel qu'ajouté en 1998 - Adopté le 12 juin 1996 (le nouvel article 5 bis a été adopté en 1998)*, in : CNUDCI (https ://uncitral.un.org/), Vienne 1996, p. « https://uncitral.un.org/fr/texts/ecommerce/modellaw/electronic_commerce » (29/03/2020), p. 17.

940. Cavoukian Ann / Tapscott Don, *Who knows : safeguarding your privacy in a networked world*, 2e éd., New York 1997, pp. 1-233 ; Finck, *Blockchains and Data Protection in the EU*, p. 28 ; STOA, *Blockchain and the General Data Protection Regulation*, in : European Parliament (https ://www.europarl.europa.eu/), Brussels 2019, p. « https : / / www . europarl . europa . eu / stoa / en / document / EPRS _ STU(2019) 634445 » (06/08/2019).

941. Finck, *Blockchains and Data Protection in the EU*, p. 28.

gie. Les données stockées sur la Blockchain sont enregistrées définitivement sur la chaîne de blocs. À chaque création d'un bloc additionnel, le volume de données stockées augmente. Des copies intégrales de la chaîne sont d'ailleurs stockées à chaque nœud du réseau. Il s'agit donc d'une technologie qui par sa structure même, s'oppose au concept de minimisation des données.

Enfin, aucune modification ou suppression de données n'est possible sur la Blockchain. La mise en œuvre effective des droits des personnes concernées dépend aussi de la technologie utilisée et les principes du Règlement ne sont pas toujours applicables. Cet exemple démontre la limite du principe de neutralité technologique. Les recherches progressent cependant pour tenter de construire des Blockchain qui préservent la sphère privée [942]. 1164

§3 La responsabilité des responsables du traitement et des sous-traitants

Le Règlement pose explicitement le principe de responsabilité du responsable du traitement et du sous-traitant [943]. 1165

Ce principe de responsabilité trouve son fondement dans le fait que les traitements de données à caractère personnel peuvent entraîner des risques pour les droits et libertés des individus. 1166

Pour limiter ces risques, « le responsable du traitement et le sous-traitant doivent prendre des mesures techniques et organisationnelles » appropriées et effectives [944]. 1167

Ces mesures doivent tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci représente pour les droits et libertés des personnes physiques [945]. 1168

« Il ne s'agit pas d'une simple obligation formelle. Ils doivent appor- 1169

942. Onik Md Mehedi Hassan, *Privacy-aware blockchain for personal data sharing and tracking*, in : Open Computer Science 2019 9/1, pp. 80-91.
943. art. 5, al. 2 RGPD.
944. art. 24 RGPD et consid. 74 RGPD ; Van Asbroeck Benoît / Debussche Julien, *Les obligations de « compliance » des entreprises*, in : Docquir Benjamin (édit.), *Vers un droit européen de la protection des données ?*, 1e éd., Bruxelles 2017, p. 105.
945. art. 24 RGPD.

ter la preuve de l'efficacité des mesures prises [946]». Celles-ci s'inscrivent dans son engagement socialement responsable (« Corporate Social Responsibility »).

1170 Ce principe de responsabilité s'explique par l'absence de contrôle ex-ante des traitements de données personnelles par une autorité de contrôle.

1171 Il constitue l'élément central pour que les personnes concernées puissent mettre en cause la responsabilité des responsables du traitement et des sous-traitants (acteurs privés et publics) en cas de dommage ou de violation des dispositions du Règlement. En ce sens, il constitue une innovation centrale.

1172 La charge de la preuve incombe au responsable du traitement qui doit démontrer son comportement diligent et la confiance qui peut lui être octroyée. Les personnes concernées partagent leurs données à caractère personnel avec le responsable du traitement principalement pour accéder aux services et aux biens proposés par le responsable du traitement, pour beaucoup sans connaître la culture d'entreprise concernant les traitements de données personnelles. De nombreuses personnes valident la charte sur la protection des données de l'entreprise en question, sans la lire et sans en comprendre les enjeux. Leurs données personnelles, enregistrées dans un compte personnel, sont ainsi transférées à des tiers à l'international pour être analysées. Des profils de personnalité sont établis sur cette base et des décisions prises. Quant aux données, elles sont stockées sur des Clouds sans garantie de confidentialité [947]. Les États-Unis ont adopté le Cloud Act [948], pour avoir accès aux données personnelles dans le cadre d'un contentieux avec Microsoft [949]. Sur la base du Cloud Act, les données à caractère personnel de citoyens américains peuvent être obtenues dans le cadre d'accords bilatéraux lors d'enquêtes pénales. En vertu du principe de réciprocité, les États tiers auront également la possibilité d'obtenir

946. Consid. 74 RGPD.

947. Ion Iulia, *Home is safer than the cloud ! : privacy concerns for consumer cloud storage*, in : Proceedings of the Seventh Symposium on Usable Privacy and Security 2011, pp. 1–13.

948. EPIC, *The CLOUD (Clarifying Lawful Overseas Use of Data) Act*, in : EPIC (https://epic.org/), Washington D.C. 2018, p. « https://epic.org/privacy/cloud-act/ » (10/06/2019).

949. Arrêt Cour suprême américaine du 17 avril 2018, *United States v. Microsoft*, 16-402, in : EPIC (https://epic.org/), Washington D.C. 2018, p. « https://epic.org/amicus/ecpa/microsoft/ » (07/06/2019).

des données de leurs propres citoyens conservées aux États-Unis, dès la signature d'accords bilatéraux [950]. Des interceptions des communications en temps réel sont également possibles [951].

La Suisse examine l'opportunité de l'élaboration d'un accord bilatéral avec les États-Unis [952]. Le Conseil de l'UE a quant à lui donné mandat à la Commission européenne de négocier un accord international sur les évidences en matière pénale, qui inclut les considérations en lien avec le Cloud Act [953]. 1173

Le principe de responsabilité permet d'engager la responsabilité des entreprises et des États. La plupart des États déploient actuellement une stratégie de cyberadministration centrée sur l'analyse des données et l'intelligence artificielle. La Commission européenne recommande de porter les investissements publics et privés dans l'IA à 20 milliards d'EUR par an au cours de la prochaine décennie [954]. 1174

950. EPIC, *The CLOUD Act.*

951. *Ibidem.*

952. Parlement suisse, *Heure des questions : Question Glättli Balthasar du 11 mars 2019, Renforcer la Suisse en tant que centre de calcul dans le contexte du Cloud Act au moyen d'un accord bilatéral d'entraide judiciaire avec les Etats-Unis*, in : Parlement suisse (https ://www.parlament.ch/), Berne 2019, p. « https://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=45404 » (16/12/2019) ; Department of Justice, *The CLOUD Act Resources - Statement of Richard W. Downing*, in : US DoJ (https ://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american » (29/03/2020) ; Department of Justice, *Justice Department Announces Publication of White Paper on the CLOUD Act*, in : US DoJ (https ://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/opa/pr/justice-department-announces-publication-white-paper-cloud-act » (16/12/2019).

953. Conseil de l'UE, *Le Conseil donne mandat à la Commission pour négocier des accords internationaux concernant les preuves électroniques en matière pénale - Communiqués de presse du 6 juin 2019*, in : Conseil de l'UE (https ://www.consilium.europa.eu/), Bruxelles 2019, p. « https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/ » (09/12/2019) ; Conseil de l'UE, *Déclaration conjointe UE-États-Unis à l'issue de la réunion ministérielle UE-États-Unis consacrée à la justice et aux affaires intérieures - Communiqués de presse du 19 juin 2019*, in : Conseil de l'UE (https ://www.consilium.europa.eu/), Bruxelles 2019, p. « https://www.consilium.europa.eu/fr/press/press-releases/2019/06/19/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/ » (09/12/2019).

954. Commission européenne, *Un plan coordonné dans le domaine de l'intelligence artificielle - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des*

Les traitements de données personnelles vont donc augmenter de manière exponentielle. Dans ce contexte, le principe de responsabilité est central pour les citoyens suisses et les personnes concernées.

1175 Afin de démontrer son comportement responsable, le responsable du traitement doit prendre des mesures techniques et organisationnelles qui seront documentées.

1176 Ces mesures visent à « garantir l'intégrité et la confidentialité des données collectées ». Ces mesures sont précisément listées dans le Règlement [955].

1177 Parmi ces mesures figurent :

- la pseudonymisation des données,
- le chiffrement,
- la capacité à garantir la disponibilité, l'intégrité, la confidentialité et la résilience constantes des systèmes et des services de traitement.

1178 La disponibilité consiste en « la possibilité d'utiliser en tout temps les systèmes et les services informatiques [956]». Le responsable du traitement doit avoir la capacité de « restaurer la disponibilité et l'accès aux données en cas d'interruption physique ou technique exceptionnelle [957]».

1179 La résilience consiste pour les systèmes et les services à « avoir une capacité de résistance et une fiabilité élevées ». Il s'agit de la tolérance des systèmes ou services à supporter des disfonctionnements [958].

1180 « Le responsable du traitement veillera à élaborer une procédure interne pour contrôler et évaluer sur une base régulière, l'efficacité des mesures techniques et organisationnelles, pour garantir la sécurité du traitement des données (art. 32, al 1 d RGPD.) ».

1181 En pratique, il faut mettre en place un système de contrôle interne,

régions du 7 décembre 2018 (COM(2018) 795 final), in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2018, p. « https://ec.europa.eu/transparency/regdoc/rep/1/2018/FR/COM-2018-795-F1-FR-MAIN-PART-1.PDF » (10/12/2019).

955. art. 32, al. 1 RGPD.
956. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 658.
957. *Idem*, p. 659.
958. *Idem*, p. 659.

afin de créer des processus spécifiques dédiés à la gestion des risques (sécurité informatique, protection des données, etc.), incluant un audit ou un programme de certification, le développement ou l'adhésion à des codes de conduite approuvés, la documentation des décisions prises dans le domaine de la protection des données, des analyses d'impact, et de la formation des collaborateurs [959].

Un contrôle interne régulier et des tests d'intrusion informatiques, constituent des éléments qui démontrent la diligence du responsable du traitement [960]. 1182

La documentation constitue un élément de conformité essentiel. Elle indique la liste des mesures prises pour maintenir un niveau de sécurité approprié au niveau de risques des traitements [961]. Le responsable du traitement a également la responsabilité de prévenir les données de « toute perte, destruction ou dommage involontaire, ou de tout traitement illicite [962] ». 1183

Si la responsabilité du responsable du traitement et du sous-traitant est engagée, alors des mesures administratives [963], des sanctions pénales éventuelles [964], et des demandes en dommages et intérêts [965] peuvent être prononcées. Ces mesures interviennent cependant *a posteriori*. Aucune autorisation préalable au traitement n'est requise du RGPD. En cas de défaillance survenue *a posteriori*, les sanctions financières sont cependant très élevées. L'autorité de contrôle peut prendre des amendes administratives (art. 83 RGPD). En cas de violation des obligations incombant au responsable du traitement et au sous-traitant, une amende administrative d'un montant de 2 pour cent du chiffre d'affaires mondial pour les entreprises ou 10 millions d'euros d'amende peut être prononcée. Concernant les infractions plus graves liées à la mauvaise application ou au non-respect du Règlement (défaut de licéité, non-respect des droits des personnes concernées, transferts transfrontaliers illicites, non-respect d'une 1184

959. EDPB, *Onzième séance plénière : lignes directrices sur les codes de conduite, annexe des lignes directrices sur l'agrément, annexe des lignes directrices sur la certification*, in : EDPB (https ://edpb.europa.eu/), Bruxelles 2019, p. « https://edpb.europa.eu/news/news/2019/european-data-protection-board-eleventh-plenary-session-guidelines-codes-conduct_fr » (07/06/2019).
960. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 661.
961. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 371.
962. art. 5, al. 1 RGPD.
963. art. 58 RGPD.
964. art. 83 RGPD.
965. art. 82 RGPD.

injonction), l'amende administrative peut atteindre 4 pour cent du chiffre d'affaires mondial s'agissant des entreprises ou 20 millions d'euros d'amende.

1185 Ainsi, les conditions d'accès de l'action civile sont déterminantes pour l'effectivité de la protection des données, et le principe de responsabilité est au cœur de la protection de la sphère privée.

1186 « Le responsable du traitement et le sous-traitant peuvent être solidairement responsables [966] ». Cette notion de responsabilité solidaire et conjointe constitue une innovation majeure du Règlement.

1187 Si le seul et unique prestataire de l'entreprise est établi hors de l'UE, qu'il n'est pas conforme au Règlement et n'est pas certifié par l'autorité de contrôle, alors deux options sont envisageables pour cette entreprise : soit elle continue de recourir à ce prestataire en sachant qu'elle engage sa responsabilité en cas de non-respect des dispositions du Règlement par le prestataire, soit elle cesse ses activités avec ce prestataire [967].

1188 Les entreprises établies dans l'UE font désormais face à un risque de sanctions financières dissuasives. La première sanction financière a été infligée à un hôpital portugais, pour un montant de EUR 400 000 en raison de sa politique d'accès aux données de ses patients [968]. La CNIL a infligé quant à elle une amende de 50 millions d'euros à l'entreprise Google [969]. Cette sanction est motivée par « le manque de transparence, une information insatisfaisante et une absence de consentement valable pour la personnalisation de la publicité ». Il est possible de connaître le montant des sanctions prononcées par chaque autorité par le biais d'un outil en ligne [970]. En juillet 2019, l'autorité de contrôle britannique a infligé une sanction de plus de 183 millions de pounds à British Airways sur le fondement

966. art. 26 RGPD.
967. art. 26, al. 1 RGPD.
968. Monteiro Ana Menezes, *First GDPR fine in Portugal issued against hospital for three violations*, in : IAPP (https ://iapp.org/), Portsmouth 2019, p. « https: //iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ » (07/06/2019).
969. CNIL, *La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC*, in : Commission Nationale de l'Informatique et des Libertés (https ://www .cnil.fr/), Paris 2019, p. « https: / / www . cnil . fr / fr / la - formation - restreinte - de - la - cnil - prononce - une - sanction-de-50-millions-deuros-lencontre-de-la » (17/06/2019).
970. GDPR Enforcement Tracker, p. « http://www.enforcementtracker.com/ » (26/06/2019).

du Règlement dans le contexte d'une violation de données à caractère personnel. L'autorité de contrôle a retenu que British Airways n'avait pas pris les mesures de sécurité suffisantes pour protéger les données personnelles de ses clients [971].

Pour décider de l'octroi éventuel d'une amende et de son montant, l'autorité de contrôle vérifie si des mesures techniques et organisationnelles ont été mises en œuvre [972]. 1189

Ces mesures doivent être adaptées au risque et s'inscrivent dans une démarche dynamique, qui vaut pour toute la durée du traitement. 1190

D'où l'importance pour le responsable du traitement de conserver une documentation rigoureuse et de bonne qualité attestant de la conformité de l'organisation au Règlement européen. Celle-ci constituera indéniablement un avantage en cas de contentieux [973]. 1191

Cela suppose que les organisations définissent et mettent en œuvre une véritable gouvernance des données et allouent les ressources financières, techniques et humaines appropriées. Les délégués à la protection des données remplissent un rôle essentiel, pour conseiller l'organisation et faciliter sa mise en conformité [974]. 1192

Le rôle du délégué à la protection des données (DPO) est comparable au responsable de la conformité bancaire. Tout comme les banques, les entreprises traitant des données personnelles dans l'UE sont soumises à une obligation de diligence (art. 5 RGPD.), qui les oblige à rendre des comptes sur leur gestion des risques concernant le traitement des données personnelles, sur la base d'un système d'autorégulation. Tout comme les banques qui reportent leurs risques à une autorité de contrôle spécifique (ex. : Autorité des mar- 1193

971. ICO, *Intention to fine British Airways £183.39m under GDPR for data breach*, in : ICO (https ://ico.org.uk/), Wilmslow 2019, p. « https://ico.org.uk/about-the - ico / news - and - events / news - and - blogs / 2019 / 07 / ico - announces - intention-to-fine-british-airways/ » (19/07/2019).

972. art. 84, al. 2 e) RGPD.

973. Härting, *Datenschutz-Grundverordnung*, p. 39.

974. Wiewiórowski Wojciech, *Preparing DPOs to lead by example : DPO-EDPS meeting in Tallinn*, in : EDPS (https ://edps.europa.eu/), Brussels 2017, p. « https://edps.europa.eu/node/4221 » (23/06/2017) ; EDPS, *Position paper on the role of Data Protection Officers of the EU institutions and bodies*, in : EDPS (https ://edps.europa.eu/), Brussels 2018, p. « https : / / edps . europa . eu / sites / edp / files / publication / 18 - 09 - 30 _ dpo _ position _ paper _ en . pdf » (16/12/2019).

chés financiers en France), les responsables du traitement ont désormais l'obligation de rendre des comptes à l'autorité de contrôle nationale dans le domaine de la protection des données personnelles, en particulier sur la licéité de leurs traitements et la gestion des risques de conformité au Règlement. Il s'agit d'un changement de paradigme.

1194 Le responsable du traitement doit apporter les preuves de sa conformité lorsque l'autorité de contrôle prendra des mesures administratives [975] à l'encontre du responsable du traitement, ou lorsqu'une personne concernée fera valoir des droits en justice à l'encontre du responsable du traitement [976] ou lors de la détermination d'amendes ou de sanctions par l'autorité de contrôle [977].

1195 Il est fortement recommandé aux entreprises de développer des lignes directrices dédiées à la protection des données et que le respect de ces lignes directrices soit documenté lors de chaque traitement [978].

1196 Source de coût à court terme, cette documentation est un gage de qualité et de confiance pour l'ensemble des parties prenantes (salariés, clients, partenaires), et un outil de différenciation pour la concurrence.

1197 En particulier, le responsable du traitement et le sous-traitant veilleront à la mise en œuvre des principes de « *Privacy-by-Default* » et « *Privacy-by-Design* » [979].

1198 La Communication de la Commission européenne intitulée « Une stratégie numérique pour l'Europe » faisait mention de ce concept : Le droit à la protection de la vie privée et des données personnelles est, dans l'Union européenne, un droit fondamental qu'il faut faire respecter effectivement, en ligne aussi, par tous les moyens possible, depuis l'application généralisée du principe de « respect de la vie privée assuré dès la conception » dans les TIC concernées,

975. art. 58 RGPD.
976. art. 82 RGPD.
977. art. 83 RGPD.
978. Härting, *Datenschutz-Grundverordnung*, p. 40.
979. Domingo-Ferrer Josep, *Privacy and data protection by design - from policy to engineering*, Heraklion 2014, p. 42.

jusqu'aux sanctions dissuasives si nécessaire.

Ce principe signifie que la protection de la vie privée et des données personnelles est prise en compte tout au long du cycle de vie des technologies, depuis le stade de leur conception jusqu'à leur déploiement, utilisation et élimination définitive [980]. 1199

Depuis le 25 mai 2018, tout projet informatique doit, dès la phase de conception du projet, intégrer la dimension de la protection des données. Les responsables du traitement devront adopter des mesures techniques et organisationnelles qui répondent aux principes de la protection des données par défaut, dès la définition des moyens de traitement des données [981]. 1200

Selon le rapporteur du Parlement européen sur la réglementation de la protection des données, Jan Philipp Albrecht, « la protection des données dès la conception et par défaut est saluée comme la grande innovation de la réforme [982] ». 1201

I. Le concept de Privacy-by-Design

Le Règlement pose le principe du respect de la vie privée dès la conception du projet (Privacy-by-Design) [983]. Il s'agit d'une obligation légale et la responsabilité du responsable du traitement pourra être engagée, si cette mesure de confiance n'a pas été mise en œuvre de manière réelle et efficace. Le concept de Privacy-by-Design s'inscrit dans la recherche d'une pesée des intérêts en présence. Si la collecte de données personnelles intervient sans autorisation préalable d'une autorité de contrôle et si la protection repose uniquement sur de grands principes, (principe de loyauté, principe de bonne foi (en Suisse)), le législateur européen instaure des garde-fous avec le Règlement, qui protègent les personnes concernées d'un usage 1202

980. Commission européenne, *Une stratégie numérique pour l'Europe - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions du 19 mai 2010 (COM(2010) 245 final)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2010, p. « https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FR:PDF » (29/03/2020), consid. 2.3.

981. art. 25, al. 2 RGPD.

982. Rapport sur la proposition de Règlement, Jan Philipp Albrecht, Exposé des motifs, Doc. A7-0402-2013 du 21 novembre 2013, p. 225.

983. art. 25 RGPD.

abusif de leurs données personnelles.

1203 Le concept de Privacy-by-Design trouve son origine dans les travaux de la Commissaire de l'information et à la protection de la vie privée de l'État d'Ontario (Canada), Ann Cavoukian. Partant du principe que le cadre légal n'offrait pas toutes les garanties nécessaires à l'effectivité de la protection des données, Ann Cavoukian a proposé d'intégrer des garanties de respect de la vie privée, dans la conception et le fonctionnement des systèmes et réseaux informatiques, mais également dans l'élaboration de pratiques responsables.

1204 Ann Cavoukian a développé *sept* principes fondamentaux sur lesquels repose la protection de la vie privée dès la conception :

1. *Prendre des mesures proactives et non réactives*

   Ce principe consiste à prévoir et à prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent. Il révèle la nécessité pour l'équipe dirigeante de l'organisme de s'engager réellement dans la prévention des atteintes à la vie privée.

2. *Assurer la protection implicite de la vie privée*

   Selon ce principe, la protection de la vie privée est intégrée dans le système, implicitement. Il s'agit d'offrir le maximum de protection de la vie privée à la personne concernée. Cette protection n'est pas optionnelle, en effet un utilisateur doit bénéficier d'une protection maximale sans aucune intervention de sa part.

   La notion de « protection implicite » définit la protection des données à caractère personnel comme une convenance qui vise à protéger l'intérêt individuel de chacun, une forme de savoir-vivre ou de bienséance numérique.

   Ce second principe est aujourd'hui connu sous le nom de *Privacy by Default* et repris à l'article 25 du projet de Règlement européen.

3. *Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques*

   Cela signifie que la protection de la vie privée fait partie intégrante du système sans porter atteinte à ses fonctions. Plus encore, ce principe suggère que les organisations doivent tenir compte de la protection des données dans la stratégie et la pratique des organisations.

4. *Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle*
   Ce principe suppose de tenir compte de tous les intérêts des partenaires de l'organisation dans une vision positive et constructive. La protection des données doit être considérée comme une valeur positive intrinsèque, gage de confiance et de bonne réputation pour l'entreprise.
5. *Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements*
   Cette mesure permet d'assurer la conservation sécurisée des données puis leur destruction sécurisée à la fin de la période de conservation.
6. *Assurer la visibilité et la transparence*
   Afin de conserver un haut climat de confiance, les éléments intégrés aux systèmes inhérents à la protection des données à caractère personnel doivent rester visibles et transparents en cas de vérification indépendante.
7. *Respecter la vie privée des utilisateurs* [984]
   Ce principe a été reconnu comme norme internationale de protection de la vie privée. Il suppose de concevoir les systèmes informatiques avec une approche centrée sur l'utilisateur (Human-Centered Design).

Il ressort de ces principes que la protection des données dès la conception englobe la protection des données par défaut. 1205

En pratique, le responsable du traitement doit mettre en œuvre, « tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent Règlement et de protéger les droits de la personne concernée » (art. 25 RGPD). 1206

Afin de respecter le principe de proportionnalité, consacré par la CJUE, le législateur européen souligne que le responsable du traitement tient compte de « l'État des connaissances, des coûts de mise 1207

984. Cavoukian Ann, *Privacy by design : The 7 foundational principles. Implementation and mapping of fair information practices*, in : Information and Privacy Commissioner of Ontario 2010/5, pp. 1-11.

en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques ».

1208 Dès la conception du produit, les exigences de protection des données seront prises en considération et non pas *a posteriori* sous forme de complément [985].

1209 Le principe de Privacy-by-Design « vise à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent. Ce principe devrait également être pris en compte dans le cadre des marchés publics [986]».

1210 Les responsables du traitement et les sous-traitants ont une *obligation de moyen* renforcée en matière de sécurité. En pratique, l'obligation de protection des données nécessite la mise en œuvre des actions de sécurité prévues par l'article 32 RGPD.

1211 Afin d'être en mesure de démontrer qu'ils respectent le Règlement, les responsables du traitement doivent adopter des règles internes et mettre en œuvre des mesures qui respectent les principes de protection des données dès la conception ou de protection des données par défaut.

1212 En quoi consistent ces mesures ?

1213 Plusieurs possibilités existent.

1214 Tout d'abord, les responsables du traitement peuvent recourir à la technique de la pseudonymisation. Il s'agit d'une nouveauté du Règlement et un des moyens de protéger les données. Cette technique permet de ne plus associer les données à une personne physique précise sans avoir recours à des informations complémentaires [987]. Il s'agit d'un exemple de mesure technique et organisationnelle prévue à l'art. 32 du Règlement pour garantir la sécurité.

1215 Ensuite, le responsable du traitement doit respecter le principe de

985. IAPP, *European Data Protection*, in : IAPP (https://iapp.org/), Portsmouth 2017, p. « https://iapp.org/resources/article/european-data-protection/ » (29/10/2018), p. 88.
986. Consid. 78 RGPD.
987. Bensoussan, *Règlement européen sur la protection des données (1e éd.)* p. 192.

minimisation des données [988]. Cette mesure consiste à ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement [989].

Pseudonymiser les données dès que possible, réduire à un minimum le traitement des données à caractère personnel sont deux garanties, essentielles, à intégrer au système informatique dès la conception d'un projet (principes de pseudonymisation et de minimisation des données) [990]. 1216

Ann Cavoukian a publié un guide en décembre 2012, pour faciliter la mise en œuvre effective du principe de protection des données dès la conception [991]. 1217

La CNIL a lancé un laboratoire « données et design » pour mettre en œuvre le principe de privacy-by-design [992]. 1218

II. Le concept de Privacy by Default

« La protection de la vie privée par défaut consiste à prendre les mesures techniques et organisationnelles, pour garantir que par défaut, seules les données qui sont nécessaires au regard de la finalité spécifique du traitement sont traitées [993]». Ann Cavoukian est également à l'origine de ce principe. 1219

Celui-ci est mentionné à l'article 23 du Règlement : « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, *par défaut*, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ». 1220

Ce principe « s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. » Il s'agit de la consécration du principe de minimisation des données, bien que les responsables 1221

988. art. 5 RGPD.
989. art. 5 RGPD.
990. Bensoussan, *Règlement européen sur la protection des données (1e éd.)*, p. 192.
991. Cavoukian Ann, *Operationalizing privacy by design : A guide to implementing strong privacy practices*, in : Information and Privacy Commissioner (https ://gpsbydesign.org/), Ontario 2012, pp. 1-5.
992. Données & Design, *Les concepts clés*, in : LINK-CNIL (https://design.cnil.fr/), Paris s.a., p. « https://design.cnil.fr/concepts/ » (10/06/2019).
993. art. 25, al. 1 RGPD.

du traitement puissent considérer que « toutes les données sont nécessaires » à la finalité du traitement.

1222 En particulier, ces mesures garantissent que, *par défaut*, « les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».

1223 Si un choix est possible entre plusieurs paramètres, « l'option la plus protectrice en termes de protection des données doit être activée par défaut ». L'utilisateur pourra réduire la protection des données en ayant accès à son compte. La responsabilité de l'augmentation du risque relatif au traitement de ses données à caractère personnel incombe ainsi à l'utilisateur qui choisit de modifier les paramètres de protection. Cette stratégie offre la souplesse de s'adapter aux souhaits d'utilisateurs aux sensibilités variées dans le domaine de la protection des données et laisse la possibilité de partager ses données dans le but de recevoir des biens ou des services personnalisés.

1224 Par défaut, « l'accès aux données à caractère personnel est limité au strict nécessaire et le responsable du traitement ne traite que les données nécessaires. Pour déterminer le caractère nécessaire, le responsable du traitement prendra en considération les critères suivants : la finalité du traitement, le volume des données collectées, l'étendue du traitement et la période de conservation [994] ».

1225 Un mécanisme de certification pourra servir d'élément pour démontrer le respect de ce principe [995].

1226 Le principe de Privacy-by-Default s'applique à la « quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée [996] ».

1227 Privacy-by-Design et Privacy-by-Default constituent des garanties à mettre en œuvre également lors des « transfert de données personnelles vers des pays qui ne disposent pas de décision d'adéqua-

994. art. 25, al. 2 RGPD.
995. art. 25, al. 3 RGPD.
996. art. 25, al. 2 RGPD.

tion de la Commission européenne (consid. 108 RGPD) ».

Il se fondent sur la minimisation des données et la pseudonymisation ainsi que sur le principe de transparence [997]. 1228

Les deux principes de Privacy-by Design et de Privacy-by-Default ne se confondent pas avec la notion de « nudges ». 1229

Thaler & Sunstein définissent les « nudges » comme des « mises en forme de l'architecture de choix, qui altèrent le comportement des individus d'une manière prévisible, sans interdire ou modifier de manière significative les incitatifs économiques. Ils consistent à procurer un État de bien-être à l'individu avec lequel ils interagissent. Ils visent à modifier le comportement des individus via une interaction avec leurs facultés non délibératives. Ils interfèrent avec l'autonomie de ces derniers en induisant un comportement [998] ». 1230

Ann Cavoukian soutient désormais le concept d'éthique « by-design ». Il s'agirait d'appliquer les principes classiques de l'éthique normative (dignité, justice, loyauté,...) au contexte de l'ère digitale [999]. Il s'agit d'une réflexion sur les valeurs, les usages et la conception des technologies innovantes de l'ère digitale et sur leur impact social. Il s'agit d'une éthique appliquée, qui tient une place croissante dans la conception des technologies d'intelligence artificielle et des systèmes autonomes, en parallèle de la conception liée à la sécurité que sont les principes de « Safety- and Security-by-Design ». 1231

Vladimir Poutine a déclaré en 2017 : *"whoever leads AI will rule the world"* [1000]. Les enjeux de pouvoir et d'influence entre États combinés aux économies d'échelle et gains d'efficacité résultant de l'analyse de données á grand échelle, soulèvent la question de la place 1232

997. Consid. 78 RGPD.
998. Barton Adrien, *Définition et éthique du paternalisme libertaire*, in : Implications Philosophiques (http://www.implications-philosophiques.org/), s.l. 2013, p. « http://www.implications-philosophiques.org/actualite/une/definition-et-ethique-du-paternalisme-libertarien/}_ftn7 » (30/07/2017).
999. Dignum Virginia, *Responsible Autonomy*, in : Proceedings of the 26th International Joint Conference on Artificial Intelligence, Melbourne 2017, p. 6 ; Bryson Joanna / Winfield Alan, *Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems*, in : Computer 2017 50/5, pp. 116-119.
1000. Meyer David, *Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World*, in : Fortune (https ://fortune.com/), New York 2017, p. « https : / / fortune . com / 2017 / 09 / 04 / ai - artificial - intelligence - putin - rule-world/ » (16/12/2019).

de l'éthique [1001].

III. Le principe de transparence

1233 Le Règlement reconnaît le principe de transparence à l'article 5 : « Les données à caractère personnel doivent être traitées de manière licite, loyale, et transparente au regard de la personne concernée (licéité, loyauté, transparence) ».

1234 Ce principe impose ainsi une visibilité sur les opérations déterminantes relatives à la protection des données à caractère personnel, ce qui est difficilement conciliable avec les exigences de concision et de clarté [1002].

1235 Le principe de transparence a un champ d'application très large. Son champ d'application matériel comprend des informations sur les valeurs sous-jacentes à un système d'intelligence artificielle qui révèle son éthique digitale.

1236 Il est introduit dans le Règlement à plusieurs reprises et concerne :

- Les données : « elles doivent être traitées (...) de manière transparente (...) » (art. 5, al. 1, a) RGPD).
- L'information des personnes : « le responsable des traitements prend des mesures appropriées pour fournir toute information (...) en ce qui concerne le traitement à la personne concernée d'une façon (...) transparente (...) (art. 12, al. 1 RGPD) ».
- La garantie d'un traitement qualifié de transparent (art. 13, al. 2 et art. 14, al. 2 RGPD).
- Les modalités de la responsabilité conjointe : « les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives (...) [1003]».
- Les codes de bonne conduite peuvent préciser les modalités d'application du Règlement, telles que : « le traitement transparent [1004]».

1001. Floridi Luciano, *Tolerant paternalism : Pro-ethical design as a resolution of the dilemma of toleration*, in : Science and engineering ethics 2016 22/6, p. 20, Notion de paternalisme tolérant.
1002. Docquir, *Vers un droit européen de la protection des données ?*, p. 102.
1003. art. 26, al. 1 RGPD.
1004. art. 40, al. 2 a) RGPD.

— « Les mécanismes de certification mis en place par les responsables de traitements et sous-traitants de manière volontaire et accessible via un processus transparent » ainsi que « des procédures et structures transparentes [1005]».

Les considérants 39 et 58 précisent que « le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples ». 1237

Le principe de transparence est applicable aux « informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement. Il s'applique aussi aux informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement (consid. 39 RGPD) ». Le considérant recommande au responsable du traitement qu'il puisse « garantir que la durée de conservation des données soit limitée au strict minimum » et suggère « la fixation de délais pour leur effacement ou pour un examen périodique ». Le responsable du traitement doit prendre « toutes les mesures raisonnables pour que les données inexactes soient rectifiées ou supprimées(consid. 39 RGPD) ». Il s'agit donc d'une obligation de moyen et non de résultat. 1238

Dans le domaine de la sécurité informatique, le Règlement adopte une approche fondée sur le risque : « le traitement doit garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement ». 1239

Le Règlement encourage les mécanismes de certification, labels, et les marques en matière de protection des données (consid. 100 RGPD). 1240

« Le principe de transparence prend tout son sens dans des situations où la multiplication des acteurs et la complexité des technologies font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la 1241

1005. art. 42, al. 3 RGPD.

concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne ».

1242 Le Règlement offre une protection renforcée aux mineurs et aux employés (art. 88, al. 2 RGPD et consid. 58 RGPD).

IV. Le registre des activités de traitement

1243 Le Règlement impose au responsable du traitement, et le cas échéant au représentant du responsable du traitement (ex. : avocat implanté dans un pays membre de l'Union européenne pour les entreprises suisses), de tenir un registre des activités de traitement effectué sous leur responsabilité [1006].

1244 Cette obligation vient remplacer l'obligation de déclarer les fichiers auprès de l'autorité de contrôle. Il s'agit d'un changement de paradigme. Seules demeurent quelques déclarations préalables dans des secteurs spécifiques, comme les secteurs de la police et de la justice (demande d'avis). Les demandes d'autorisation se limitent à certains traitements de données de santé. Par conséquent, il n'existe pratiquement aucun contrôle a priori préalablement au traitement de données personnelles. Une logique de responsabilisation des acteurs est privilégiée sur la base de grands principes et d'un contrôle *a posteriori*.

1245 Le registre des activités de traitement s'inscrit dans ce cadre et permet au responsable du traitement de faire l'inventaire des traitements dans une logique de gestion des risques et de transparence.

1246 Les informations à répertorier [1007] sont les suivantes :

- Nom et coordonnées du responsable du traitement ou des sous-traitants, responsables conjoints du traitement, représentants et tout DPO.
- Description des catégories de personnes concernées et des données à caractère personnel.
- Les transferts de données en dehors de l'EEE, y compris l'identification des pays destinataires et les documents attestant de l'existence de garanties appropriées.

1006. art. 30 RGPD.
1007. art. 30, al. 1 et 2 RGPD.

— Une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

— Les délais prévus pour l'effacement des différentes catégories de données.

— Les « catégories » de destinataires qui ont reçu / recevront les données.

— Les finalités du traitement.

Toutes les entreprises de plus de 250 personnes sont soumises à cette obligation. Les entreprises de moins de 250 personnes en sont exemptées, sauf si elles effectuent des traitements susceptibles de comporter un risque pour les individus concernés, traitent des données sensibles ou judiciaires ou encore si le traitement n'est pas occasionnel [1008]. 1247

De nombreuses entreprises, des PME aux entreprises multinationales, ont l'obligation de créer et de tenir à jour un registre des traitements. Si un représentant est désigné par l'entreprise, il est de la responsabilité du représentant de créer et de tenir à jour le registre du traitement. 1248

V. Analyse d'impact

Le Règlement [1009] impose aux responsables du traitement d'effectuer une analyse d'impact (« Privacy Impact Assessment », PIA) quand des traitements sont susceptibles « d'engendrer un risque élevé » pour les droits et libertés des personnes physiques. 1249

L'analyse d'impact s'effectue préalablement au traitement de données personnelles. 1250

La conduite d'une analyse d'impact démontre le comportement diligent, loyal et responsable du traitement en cas d'enquête ou de contentieux postérieurement au traitement. Il permet au responsable du traitement d'apporter le preuve de la qualité de sa gouvernance des données, ce qui est fondamental pour éviter une amende administrative ou la mise en cause de sa responsabilité en cas de 1251

1008. art. 30, al. 5 RGPD.
1009. art. 35 RGPD.

contentieux.

1252 Si un DPO a été désigné, il conseille le responsable du traitement [1010].

1253 Une analyse d'impact est rendue obligatoire pour les trois cas suivants :

— « En cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques pour la personne concernée ou l'affectant de manière significative.

— En cas de traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 RGPD.

— En cas de surveillance systématique à grande échelle d'une zone accessible au public ».

1254 Dans de tels cas, une analyse d'impact doit être effectuée et documentée. Elle a pour but d'identifier les risques et d'offrir des garanties aux personnes concernées. La jurisprudence de la CJUE est très claire : « avant d'introduire une surveillance en continu des communications électroniques des salariés à leur insu, l'employeur doit par exemple se demander si une solution moins intrusive des droits et libertés des individus est envisageable ». Des garanties doivent être octroyées aux salariés : « ils doivent être informés de la nature et de l'étendue de la surveillance des individus ». Des motifs légitimes doivent justifier la mesure de surveillance. Quelles sont les conséquences et sont-elles compatibles avec « les finalités légitimes de la mesure [1011] ».

1255 Si un risque élevé ressort de l'analyse d'impact, alors l'autorité de contrôle doit en être informée. L'autorité de contrôle émettra un avis sur le caractère ou non pertinent des mesures proposées par le responsable du traitement, visant à réduire les risques pour les droits et libertés des personnes concernées. Le responsable du trai-

1010. art. 35, al. 2 RGPD.

1011. Arrêt CourEDH du 5 septembre 2017, *Barbulescu contre Roumanie*, requête n° 61496/08, consid. 138.

tement évaluera ensuite la gravité du dommage éventuel et la probabilité d'occurrence [1012].

Le responsable du traitement pourra décider de mettre en place une gradation du niveau des risques, mais le Règlement ne l'y oblige pas [1013]. 1256

Le champ d'application matériel de l'analyse d'impact comprend le respect des principes de l'art. 5 RGPD et l'analyse des mesures techniques et organisationnelles prises pour offrir des garanties aux personnes concernées. Sont pris en compte les aspects en lien avec « la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé accidentel ou illicite aux données ». Elle adopte une approche fondée sur le risque (chiffrement, pseudonymisation) et effectue un contrôle de qualité des solutions choisies. 1257

En pratique, le responsable du traitement doit examiner sur la base de critères objectifs [1014] les différents traitements et leurs finalités, identifier les personnes concernées, les catégories de données, et les risques pour les droits et libertés individuelles. Sont inclus tous les risques qui peuvent engendrer un dommage physique, matériel ou immatériel pour la personne concernée [1015]. Une analyse d'impact doit en particulier être conduite lors de l'emploi de nouvelles technologies ou lorsqu'indépendamment des technologies employées, les personnes concernées peuvent exercer leurs droits de manière plus limitée [1016]. C'est notamment le cas lors de traitements de données complexes et non transparents ou encore lorsque de nombreuses parties prenantes sont impliquées dans le traitement de données [1017]. 1258

Une analyse d'impact préalable au traitement doit être effectuée pour tous les traitements pouvant engendrer une « discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel, un renversement non autorisé du processus de pseudonymisation ou tout autre dommage écono- 1259

1012. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 371.
1013. *Idem*, p. 373.
1014. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 689.
1015. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 372.
1016. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 689.
1017. *Ibidem.*

mique ou social important » (consid. 75 RGPD).

1260 Une analyse d'impact est également requise pour tout traitement qui « priverait de leurs droits et libertés les personnes concernées ou les empêcherait d'exercer le contrôle sur leurs données à caractère personnel ».

1261 De même, les traitements de données sensibles [1018] ou judiciaires, les traitements effectuant une évaluation d'aspects personnels, conduisant à une prédiction d'éléments de santé, ou du rendement au travail, de la situation économique, ou des centres d'intérêts personnels, nécessitant une localisation ou un suivi des déplacements en vue de créer ou d'utiliser des profils individuels, constituent également des traitements risqués, nécessitant une analyse d'impact.

1262 Les traitements de données de personnes vulnérables et en particulier des enfants, ou tout traitement portant sur un volume important de données à caractère personnel qui touche un nombre important de personnes nécessitent une analyse d'impact [1019]. Il sera utile d'offrir un élément chiffré pour quantifier la notion de « volume important de données ».

1263 Cette analyse permet de contrôler que toutes les obligations découlant du Règlement comme celles précisées aux articles 25 (Principe de Privacy-by-Design), et 32 (Principe de sécurité) sont remplies [1020].

VI. La notification d'une violation de données à caractère personnel

1264 Le Règlement introduit pour le responsable du traitement une obligation de notification à l'autorité de contrôle, en cas de violation de données à caractère personnel [1021]. Cette obligation trouve sa source dans la directive 2002/58/CE « vie privée et communications

1018. art.9 RGPD ; Härting, *Datenschutz-Grundverordnung*, p. 128.
1019. United States / Executive Office of the President / Podesta, *Big data*,; Meyer Michelle, *Online Symposium on the Law, Ethics & Science of Re-identification Demonstrations*, in : Harvard Law - Bill of Health (https://blog.petrieflom.law.harvard.edu/), Cambridge 2013, p. « https://blog.petrieflom.law.harvard.edu/2013/05/13/online-symposium-on-the-law-ethics-science-of-re-identification-demonstrations/ » (12/07/2017).
1020. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 373.
1021. art. 33 RGPD.

électroniques » (art.4, al. 3).

Cette obligation d'annonce vise à responsabiliser les acteurs et à atteindre une pesée des intérêts en présence consacrée par la jurisprudence de la CJUE. 1265

La violation des données à caractère personnel est définie dans le Règlement comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » (art. 33 RGPD). 1266

Ainsi le législateur européen conçoit la violation de données avant tout comme une violation de sécurité des données et des systèmes informatiques [1022]. Le Règlement conçoit ainsi la protection des données comme une protection technique [1023]. Des mesures techniques et organisationnelles appropriées doivent être prises pour réduire le risque de violation de données. Par exemple, la pseudonymisation ou le chiffrement des données [1024]. 1267

Il pose une obligation de coopération entre le responsable du traitement et l'autorité de contrôle dans l'UE [1025]. Cette obligation de coopération a pour but de faciliter l'accomplissement des tâches de l'autorité de contrôle (art. 51 RGPD) [1026]. 1268

En application de cet article, le responsable du traitement doit notifier toute violation de données à caractère personnel dans les meilleurs délais, et au maximum 72 heures après avoir eu connaissance de la violation de données. Lorsque la violation n'a pas eu lieu, il convient de l'informer des motifs du retard. 1269

Le responsable du traitement notifiera la faille de sécurité à l'autorité de contrôle compétente, si la violation de données est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Notons que le Règlement ne définit pas la notion de 1270

1022. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 650.
1023. *Ibidem.*
1024. *Ibidem.*
1025. *Idem*, p. 644
1026. *Idem*, p. 645

risque et laisse au juge le soin de cette définition.

1271 La notification doit être faite dans les plus brefs délais.

1272 Le PFPDT considère qu'en cas de violation de données personnelles, le responsable du traitement doit uniquement informer les autorités compétentes européennes. La notification du PFPDT en Suisse est optionnelle. Elle deviendra obligatoire avec l'entrée en vigueur de la LPD révisée.

1273 Le responsable du traitement communiquera à l'autorité de contrôle les informations suivantes :

- La nature de la violation de données à caractère personnel y compris, si possible, des catégories et du nombre approximatif de personnes concernées par la violation et des catégories et du nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et des coordonnées du DPO, ou de tout contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Les conséquences probables de la violation de données à caractère personnel ;
- Les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

1274 Le Règlement autorise le responsable du traitement à communiquer les informations requises à l'autorité de contrôle de manière graduelle, si toutes les informations ne peuvent pas être livrées en même temps [1027].

1275 Le responsable du traitement doit en outre documenter la faille de sécurité, en décrivant les faits et les mesures prises, afin de permettre à l'autorité de contrôle de vérifier qu'il a bien respecté son obligation de notification.

1276 En pratique, il sera difficile pour les organisations de comprendre, en moins de 72 heures, quelle a été l'origine de la violation de données à caractère personnel. Il apparaît encore plus délicat de mesurer l'ampleur du risque associé à cette violation (risque pour les

1027. art. 33, al. 4 RGPD.

clients, pour l'entreprise, volume de données concernées, étendue du dommage) du fait du délai très court.

L'obligation de notifier sans délai et au maximum dans les 72 heures l'autorité de contrôle se justifie par la volonté du législateur d'intervenir à temps pour éviter « de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral ». Ces préjudices peuvent se traduire par une perte de contrôle sur les données à caractère personnel, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel, un dommage économique ou social important. 1277

Le Règlement pose une obligation de double notification de l'autorité de contrôle et de la personne concernée. Si les conditions de l'article 33 RGPD sont remplies, alors le responsable du traitement doit notifier la violation de données à caractère personnel à l'autorité de contrôle. Cependant, si la violation de données à caractère personnel est susceptible « d'engendrer un risque élevé pour les droits et libertés d'une personne physique », alors le responsable du traitement doit en outre informer la personne concernée de la violation de données à caractère personnel (art. 34 RGDP). Il importe de relever que le Règlement ne définit pas la notion de risque « élevé ». 1278

Des exceptions à la notification sont prévues à l'article 34 RGPD. 1279

Si les données volées ne sont pas lisibles, alors aucune notification n'est requise, puisqu'il n'existe pas de risque pour les personnes concernées [1028]. 1280

Aucune notification n'est requise si des mesures techniques ou organisationnelles rendent les données incompréhensibles (ex. : chiffrement des données) ou si les mesures prises par le responsable 1281

1028. Parlement européen, *Rapport (A7-0402/2013) du 22 novembre 2013 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)*, in : Parlement européen (https ://www.europarl.europa.eu/), Bruxelles 2013, p. « http : / / www . europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//FR » (29/10/2018), amendement 64, p. 477.

du traitement ont pour conséquence que le risque élevé pour les droits et libertés des personnes ne peut plus se matérialiser ou si la notification de la personne concernée nécessiterait des efforts disproportionnés, alors le responsable du traitement est dispensé de la notification des personnes concernées [1029].

1282 L'autorité de contrôle peut cependant exiger la notification des personnes concernées [1030].

1283 L'obligation de notification prévue aux art. 33 et 34 RGPD a pour objectif d'empêcher la réalisation d'un dommage physique, matériel ou immatériel pour la personne concernée [1031]. Ce dommage peut s'exprimer par une une perte de contrôle des données pour la personne concernée, une restriction de ses droits, une discrimination, un vol d'identité, une perte financière, ou une levée de la pseudonymisation [1032].

1284 Le responsable du traitement doit documenter tous les faits relatifs à la violation de données [1033] et les mettre à la disposition de l'autorité de contrôle, qui peut en exiger l'accès [1034].

1285 Il doit prouver qu'il a pris « toutes les mesures raisonnablement susceptibles d'être mises en œuvre pour éviter les violations de données ». Il doit également rapporter la preuve qu'il a correctement réagi aux violations survenues [1035]. Ces obligations s'appliquent à tous les responsables de traitement, c'est-à-dire à tout organisme qui « détermine les finalités et les moyens du traitement [1036] ».

1286 « Il est recommandé d'anticiper ce type d'incident et de développer une procédure interne spécifique à la notification des violations de données afin de réagir dans les délais très courts du Règlement. Cette procédure pourrait créer une cellule de crise et définir des mesures d'urgence pour remédier aux violations et en atténuer les

1029. art. 34, al. 3 RGPD.
1030. art. 34, al. 4 RGPD.
1031. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 501.
1032. *Ibidem.*
1033. art. 33, al. 5 RGPD.
1034. art. 58, al. 1, a) RGPD.
1035. art. 33, al. 5 RGPD.
1036. art. 4, al. 7 RGPD.

conséquences [1037]».

Toute violation de l'obligation d'annonce (art. 31 et 33, al. 1 RGPD) est punissable d'une amende administrative pouvant s'élever jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaire mondial de l'entreprise [1038]. La personne concernée peut en outre demander le versement de dommages et intérêts en réparation du préjudice subi sur la base de l'article 82 du Règlement. 1287

VII. Le contrôle *a posteriori* et les actions de mise en œuvre de ce contrôle

A. Éléments de procédure

Les autorités de contrôle

Tout d'abord, le Règlement donne le droit aux personnes lésées par un traitement de données personnelles d'introduire une réclamation auprès de l'autorité de contrôle (art. 77 RGPD). Ce droit se fonde sur le constat par le lésé de l'illicéité d'un traitement de données personnelles sur la base du Règlement. 1288

L'autorité de contrôle a le pouvoir d'infliger une amende administrative pour un montant allant de 10 à 20 millions d'euros ou, dans le cas d'une entreprise, de 2 à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. (art. 58 et 83 RGPD). L'article 83 précise que ces amendes doivent être « effectives, proportionnées et dissuasives » (art. 84 RGPD). 1289

Ensuite, le Règlement reconnaît également à la personne lésée par un traitement illicite de données personnelles le droit à un recours juridictionnel effectif contre une autorité de contrôle (art. 78 RGPD). Plus précisément, « toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne ». 1290

Dans un État de droit, la personne lésée peut toujours attaquer la décision administrative qui lui est défavorable. L'innovation du Règlement porte sur un autre aspect. Il s'agit pour les États soumis au RGPD de mettre en œuvre un recours juridictionnel effectif, c'est- 1291

1037. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 223.
1038. art. 83, al. 4 a) RGPD.

à-dire de faciliter l'accès à la justice pour les personnes physiques ou morales qui souhaitent effectuer un recours, comme le précise le paragraphe 1294. L'effectivité devient avec le Règlement une exigence juridique impérieuse pour les États. Comment procéder ? Le Règlement prévoit par exemple la reconnaissance du mécanisme de *class action* (art. 80 RGPD). Il autorise ainsi à la fois les personnes physiques individuelles, mais également les groupes à « agir collectivement en justice » (*class action*) pour engager la responsabilité d'un responsable du traitement et obtenir réparation d'un dommage [1039]. Il s'agit d'un aspect central du Règlement. Cette action en responsabilité devient un instrument efficace et facile à mettre en œuvre par l'introduction de la *class action*.

1292 L'autorisation des class action devrait augmenter le nombre de recours dans les pays de l'UE. En pratique, la preuve du dommage est difficile à apporter et un régime de responsabilité objective pourrait être envisagé.

1293 Si la *class action* est formellement prévue par le Règlement et constitue un moyen de garantir l'effectivité du recours juridictionnel imposée par le Règlement, d'autres mesures pourraient être envisagées. Par exemple, la gratuité de la représentation juridique lors d'une *class action* ou d'un recours individuel. Ce coût serait pris en charge par l'État dans le cadre de son obligation d'instaurer un recours juridictionnel effectif.

B. L'action en responsabilité contre le responsable du traitement et les sous-traitants

1294 En parallèle du contrôle *a posteriori* avec l'intervention des autorités de contrôle, la personne lésée peut également ouvrir une action en responsabilité à l'encontre du responsable du traitement ou du sous-traitant. En application de l'art. 79 RGPD, « chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement ».

1295 Cette innovation du Règlement constitue la contrepartie de la suppression du contrôle a priori. Le législateur manifeste ainsi sa volonté de ré-équilibrer les rapports de force entre les personnes concer-

1039. art. 79 RGPD.

nées et les responsables du traitement et les sous-traitants (acteurs privés ou États). Il met en place un mécanisme concret de protection des personnes concernées dont l'effectivité va dépendre des conditions de l'action civile, de manière similaire au droit de la concurrence [1040].

En quoi consiste cette responsabilité ? Le Règlement précise que « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement » (art. 24 RGPD). 1296

Le responsable du traitement doit établir que le traitement de données personnelles est effectué conformément au Règlement. Le fardeau de la preuve est inversé. Il incombe désormais au responsable du traitement d'apporter la preuve de la diligence de son comportement dans le traitement des données personnelles. 1297

En juin 2019, l'autorité de contrôle britannique a condamné British Airways au paiement d'une amende de 183 millions de pounds, au motif que les mesures de sécurité prises par l'entreprise étaient insuffisantes, c'est-à-dire inadaptées, au niveau de risque. 1298

Elizabeth Denham, Préposé britannique à la protection des données a indiqué que : « la perte de données personnelles » est « plus qu'un inconvénient ». Elle a déclaré que les entreprises devraient prendre les mesures appropriées « pour protéger le droit fondamental à la vie privée ». Les données personnelles des gens sont uniquement cela - personnelles. Lorsqu'une organisation ne parvient pas à les protéger contre la perte, les dommages ou le vol, c'est plus qu'un inconvénient. C'est pourquoi la loi est claire - quand on vous confie des données personnelles, vous devez vous en occuper. Ceux qui ne le font pas feront l'objet d'un examen minutieux de la part de mon bureau pour vérifier qu'ils ont pris les mesures appropriées pour protéger les droits fondamentaux à la vie privée [1041]. 1299

Le terme « approprié » provient du latin « appropriare », qui signifie : « faire sien ». Il s'agit pour le responsable du traitement de prendre les mesures de protection comme si les données per- 1300

1040. Hurni, *L'action civile en droit de la concurrence*, p. 20 ; Jacobs Reto, *Zivilrechtliche Durchsetzung des Wettbewerbsrechts*, in : Das revidierte Kartellgesetz in der Praxis 2006, pp. 209-225.

1041. ICO, *Intention to fine British Airways £183.39m under GDPR for data breach.*

sonnelles traitées étaient les siennes. Cela renvoie encore une fois à un comportement prudent, diligent, « en bon père de famille ». Il s'agit du comportement attendu d'un individu de référence dans une situation donnée. « Ce comportement sert de norme générale pour mesurer l'adéquation de la conduite d'un individu concret placé dans la même situation afin de déterminer l'existence d'une éventuelle faute [1042] ». L'autorité britannique réactualise cette notion inspirée du standard « of due care ».

1301 Si le responsable du traitement s'écarte de cette norme de référence en ne protégeant pas les traitements de données par des mesures techniques et organisationnelles adaptées au niveau de risque, il y a faute ou négligence du responsable du traitement ou du sous-traitant. Cette faute peut être simple ou lourde selon la gravité du comportement et l'écart par rapport au niveau de risque. Cependant, la faute la plus légère impliquera la responsabilité civile de son auteur si elle a causé un dommage.

1302 L'obligation est faite au responsable du traitement et au sous-traitant de prendre « toutes les mesures appropriées pour s'assurer que le traitement est effectué conformément au Règlement » (art. 24 RGPD). Cette responsabilité est extrêmement large et s'apparente à une responsabilité objective, car le responsable du traitement et le sous-traitant répondent de tout risque de violation du Règlement. C'est au responsable du traitement et au sous-traitant de faire tout ce qui est nécessaire pour protéger les traitements de données personnelles de tout dommage. Cet article 24 RGPD oblige pratiquement à établir qu'il n'y a pas de faute ou de négligence, ce qui apparaît difficile de facto, même si ça ne peut pas être exclu. Le responsable du traitement ou le sous-traitement peuvent tenter de démontrer l'absence de négligence ou de faute. Il peut en effet être exonéré de se responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable. Cette possibilité laissée au responsable du traitement ou au sous-traitant fait obstacle à la qualification du régime de responsabilité du Règlement en un régime de responsabilité sans faute, pour risque (voir paragraphe 1294).

1303 L'article 32 du Règlement est encore plus exigeant concernant l'obligation faite au responsable du traitement de prendre des mesures techniques et organisationnelles appropriées au niveau de risque

1042. Wikipedia, *Bon père de famille*, p. « https://fr.wikipedia.org/wiki/Bon_père_de_famille » (20/07/2019).

du traitement. Il doit « garantir un niveau de sécurité adapté au risque » à travers des mesures techniques et organisationnelles appropriées. La question se pose de savoir si le responsable du traitement fait face à une obligation de moyen ou de résultat. L'exigence imposée au responsable du traitement et au sous-traitant de connaître le niveau de risque de chaque traitement et d'y affecter des mesures de protection appropriées constitue, selon nous, une obligation de résultat.

1304 Afin de démontrer le respect de cette obligation, le législateur donne la possibilité au responsable du traitement et au sous-traitant (art. 32, al. 3 RGPD) de rédiger des codes de conduite (art. 40 RGPD) ou d'obtenir une certification (art. 42 RGPD) pour « démontrer » leur comportement diligent et responsable, ainsi que le caractère approprié des mesures prises (voir paragraphe 941).

1305 Ces articles intègrent ainsi la protection des données dans le domaine de la responsabilité sociale des entreprises. Gestion optimale des risques juridiques ou prise de conscience profonde de l'importance du caractère approprié des mesures de sécurité pour protéger les traitements de données personnelles, quelle que soit la motivation véritable des acteurs économiques, il est fortement recommandé de rédiger un code de bonne conduite, approuvé par l'autorité de contrôle, dans le domaine de la sécurité informatique ou d'obtenir une certification.

1306 La diversité des risques informatiques auxquels les organisations sont confrontées et leur caractère évolutif rendent difficile en pratique, voire illusoire, la création d'un système « immunitaire » dans le domaine de la sécurité informatique, qui exempte les organisations de tout risque.

1307 Il apparaît dès lors essentiel de saisir l'opportunité offerte par le législateur dans l'art. 32, al. 3 RGPD. Le risque d'une telle approche réside dans l'encouragement d'un formalisme juridique déconnecté de la réalité opérationnelle. Les tribunaux jugeront dans quelle mesure l'art. 32, al. 3 RGPD exempte effectivement les responsables du traitement et les sous-traitants de leur responsabilité juridique effective ou considèrent l'existence de codes de conduite comme un élément limitant le montant de la sanction éventuelle sans pour autant remettre en cause la responsabilité du responsable du trai-

tement ou du sous-traitant (art. 83 RGPD).

1308 Il nous apparaîtrait raisonnable de limiter le montant des sanctions pécuniaires en cas d'effort démontré de la part du responsable du traitement et du sous-traitant pour gérer les risques de sécurité de manière prudente et diligente sans pour autant supprimer la responsabilité les concernant.

1309 Cette analyse est partagée par la doctrine. Kühling considère également qu'une certification de conformité éventuelle au Règlement européen n'immunise pas l'organisation d'une mise en cause de sa responsabilité délictueuse [1043]. Il est également d'avis qu'aucune exclusion de responsabilité ne peut être prévue par contrat, conception que nous partageons aussi [1044].

1310 Compte tenu du niveau élevé des sanctions financières (art. 83 RGPD) imposé par le Règlement, il est recommandé au responsable du traitement, en cas de doute concernant une violation de sécurité éventuelle, qu'il demande à l'autorité de contrôle si, compte tenu des éléments de faits en sa possession, une obligation de notification est requise [1045].

C. Le droit à réparation et à la responsabilité du responsable du traitement et du sous-traitant

1311 Le Règlement pose la principe du droit pour « toute personne ayant subi un dommage matériel ou moral du fait d'une violation du Règlement d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi » (art. 82 RGPD). La personne doit démontrer l'existence d'un dommage ou d'un tort moral et établir le caractère illicite du traitement de données personnelles.

1312 Pour comprendre le bien-fondé de ce droit, il faut se reporter à l'article 24 RGPD pré-cité qui précise le contenu et l'étendue de la responsabilité du responsable du traitement ou du sous-traitant. Ainsi ceux-ci devront apporter des éléments matériels attestant qu'ils se sont comportés de manière responsable.

1313 L'article 82 du Règlement pose ainsi le principe du « droit à répara-

1043. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 1117.
1044. *Idem*, p. 1119.
1045. Wybitul / Bausewein, *EU-Datenschutz-Grundverordnung*, p. 514.

tion » (dans l'UE ou dans un pays tiers) [1046] et de la mise en cause de la responsabilité délictueuse dans le domaine de la protection des données [1047].

Afin de renforcer la protection des personnes concernées et les obligations des entreprises traitant des données personnelles, le Règlement introduit un principe de responsabilité conjointe entre les responsables du traitement et les sous-traitants [1048]. Cela signifie que « chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective ». Il s'agit de la reconnaissance de la jurisprudence de la CJUE [1049]. 1314

Le législateur manifeste ainsi sa volonté d'offrir des garanties d'indemnisation optimales aux personnes concernées par le traitement de leurs données personnelles. 1315

Cependant, le responsable du traitement comme le sous-traitant peuvent faire face à une demande en réparation pour la totalité du dommage [1050]. 1316

Cette solution offre des garanties pour les personnes concernées et constitue une solution satisfaisante pour limiter le risque de confusion des rôles et des responsabilités soulevées par la doctrine. Une claire démarcation dans les rôles de chacun n'est pas toujours aisée, sans contrat écrit qui détermine les rôles et responsabilités de chacun [1051]. 1317

La jurisprudence de la CJUE précise cependant qu'il existe aussi un « responsable du traitement à titre principal » : « Il y a lieu de préciser [...] que l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impli- 1318

1046. Cf. aussi le consid. 108 RGPD.
1047. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 1106.
1048. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 1119.
1049. Arrêt CJUE du 5 juin 2018, *Wirtschaftsakademie*, C-210/16, ECLI :EU :C :2018 :388, consid. 34.
1050. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 1109 et Document 9083/15, 2 du Conseil de l'Europe.
1051. Blume Peter, *An alternative model for data protection law : changing the roles of controller and processor*, in : International Data Privacy Law 2015 5/4, pp. 292-297.

qués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce [1052]».

1319 Dans l'hypothèse où deux acteurs économiques déterminent les finalités et les moyens d'un traitement de données à caractère personnel (co-responsables du traitement), un cadre contractuel s'impose. Celui-ci clarifiera les degrés de contrôle de chaque acteur et déterminera le degré de responsabilité de chacun. Les obligations respectives des parties seront définies en toute transparence, afin de remplir les obligations du RGPD et de limiter les risques pour chaque co-responsable (art. 26 RGPD).

1320 Les co-responsables du traitement formaliseront leurs obligations par écrit sous la forme d'un contrat ou de conditions générales. En l'absence d'un tel cadre contractuel, chaque co-responsable pourra être tenu responsable solidairement pour les actes qui sont sous le contrôle de l'autre responsable du traitement.

1321 Les sanctions applicables sont celles définies à l'art. 83, al. 4 RGPD (amende administrative et mesures correctrices). Si les droits des personnes ne sont pas respectés (ex. : absence d'information des personnes concernées avant le traitement de leurs données personnelles), l'autorité de contrôle pourra ordonner de stopper le traitement et le doublement des amendes (art. 83, al. 5 RGPD). Une action en responsabilité pourra également être intentée pour obtenir la réparation du dommage et le versement de dommages et intérêts [1053].

1322 La CJUE a retenu que Facebook et l'administrateur d'une page hébergée sur le réseau social pouvaient être qualifiés de responsables conjoints du traitement de données personnel des visiteurs de la page [1054].

1323 Toute personne physique ou morale qui a une page Facebook est co-responsable du traitement des données liées à sa page avec l'entreprise Facebook. Nous partageons la conception de M. Veale : « cette expansion de la responsabilité de la personne concernée est problématique et risque de limiter le développement des technologies protectrices de la vie privée, de même que les écosystèmes décen-

1052. Arrêt CJUE du 5 juin 2018, *Wirtschaftsakademie*, C-210/16, consid. 43.
1053. Métille / di Tria, *Protection des données*, pp. 308-309.
1054. *Idem*, p. 308 ; Arrêt CJUE du 5 juin 2018, C-210/16, consid. 39.

tralisés de données [1055]».

L'action en responsabilité est ouverte aux personnes physiques concernées par un traitement de données personnelles [1056]. L'auteur de la plainte est fondé à saisir le tribunal de son lieu de domicile [1057]. 1324

Le droit à réparation concerne tant un dommage matériel qu'immatériel (voir paragraphe 1316). Les dommages et intérêts « doivent pour assurer leur efficacité et leur effet dissuasif » être adéquats par rapport aux préjudices subis [1058]. 1325

S'inspirant de la pratique des Treble Damages en droit américain, qui autorise les tribunaux à tripler le montant des dommages-intérêts, la Cour introduit dans cette affaire, l'idée qu'il faut être généreux dans l'évaluation du dommage subi. 1326

À titre d'exemple, une action de groupe pourrait être ouverte sur la base du Règlement par les utilisateurs de l'application FaceApp, sur le fondement du défaut de validité du consentement et du défaut de transparence, concernant les utilisations dérivées des photos collectées. 1327

D. Les sanctions

Le Règlement donne le pouvoir aux autorités administratives de prononcer des amendes administratives (art. 83 RGPD). Celles-ci doivent être « effectives, proportionnées et dissuasives » (art. 83 RGPD). 1328

Les amendes peuvent s'élever « jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu » (art. 83, al. 4 RGPD), en cas de violations des obligations générales du Règlement mentionnées aux articles 11, 25 à 39, 42 et 43 RGPD. Il s'agit notamment de la tenue d'un registre des activités 1329

1055. Arrêt CJUE du 29 juillet 2019, *Fashion ID GmbH & Co. KG contre Verbraucherzentrale NRW eV*, C-40/17, ECLI :EU :C :2019 :629 ; Edwards Lilian, *Data subjects as data controllers : a Fashion (able) concept ?*, in : Internet Policy Review (https ://policyreview.info/), Berlin 2019, p. « https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400 » (12/12/2019).

1056. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 1106 ss.

1057. *Idem*, p. 1121.

1058. Arrêt CJUE du 10 avril 1984, *Sabine Von Colson, Elisabeth Kamann, Land Nordrhein-Westfalen*, ECLI :EU :C :1984 :153, consid. 23.

de traitement, de la sécurité des traitements, de la mise en œuvre des mesures de privacy-by-design et privacy-by-default, de la nomination d'un délégué à la protection des données et de la conduite d'analyses d'impact.

1330 Les amendes pourront atteindre 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83, al. 5 et al. 6 RGPD), en cas de non-respect d'une injonction, en cas de violation des principes de l'art. 5 RGPD, et en cas de non-respect des obligations relatives au consentement (art. 5, 6, 7 et 9 RGPD). Il en va de même en cas de violation des droits des personnes concernées (art. 12 à 22 RGPD) et des dispositions du Règlement dans le cas des transferts transfrontaliers.

1331 Ces amendes seront prononcées à la suite d'une réclamation de la personne concernée auprès de l'autorité de contrôle (art. 77 RGPD) ou lors d'un recours juridictionnel effectif contre une autorité de contrôle (art. 78 RGPD). Des amendes pourront ainsi potentiellement être infligées à des autorités publiques ou de contrôle (art. 83, al. 7 RGPD).

1332 Si la juridiction ne prévoit pas d'amende administrative, l'art. 83 demeure applicable et l'amende par exemple de nature pénale peut être « déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales » (art. 83, al. 9 RGPD). « Les voies de droit doivent être effectives et avoir un effet équivalent aux amendes administratives imposées par les autorités de contrôle ».

1333 En parallèle des amendes, le versement de dommages-intérêts pourra être exigé lors d'une action en responsabilité à l'encontre du responsable du traitement ou du sous-traitant, ouverte par la personne lésée.

1334 L'ampleur des sanctions potentielles, tant en matière financière qu'en matière de réputation, impose une gestion des risques pour les responsables du traitement et le sous-traitant. Cette gestion des risques aboutit à la mise en œuvre d'une politique de conformité dans le domaine de la protection des données qui s'inspire de la conformité dans le domaine bancaire et financier.

1335 Le Règlement s'apparente ainsi au « droit de la compliance » qui

est de nature prudentielle.

Pour M.A Frison-Roche, la méthode utilisée est l'innovation majeure du Règlement : « le contrôle déclaratif ex-ante auprès d'une autorité publique de contrôle a été supprimé et le but de protection des personnes, maintenu et articulé avec le principe de libre circulation des données, a été internalisé dans les entreprises utilisant à des fins commerciales les données à caractère personnel ». Les entreprises ont désormais l'obligation de protéger les personnes, de les informer de leurs droits, l'autorité de contrôle intervenant uniquement a posteriori, pour les activités de contrôle et de sanctions [1059]. 1336

Cela s'explique par le fait que les acteurs économiques sont dans une position privilégiée du fait de leur accès à l'information et de leur interaction avec les personnes concernées. Ils ont le pouvoir d'agir et de protéger les personnes concernées. Ils sont assujettis au droit de la protection des données, indépendamment de l'existence d'un fait reprochable. 1337

Il s'agit de la reconnaissance de l'obligation pour les acteurs économiques de se comporter « en bon père de famille » pour les données personnelles traitées, sous le contrôle a posteriori des autorités de régulation et du juge. Cette obligation n'est pas limitée au responsable du traitement, mais s'adresse également au sous-traitant. 1338

VIII. Les nouvelles obligations du sous-traitant

Le Règlement pose de nouvelles obligations pour le sous-traitant telles que : 1339

- La responsabilité directe du sous-traitant auprès des personnes concernées ;
- Les obligations en matière de traitement de données de santé ;
- La désignation d'un DPO à la protection des données en cas de traitement présentant des risques spécifiques ; et
- L'obligation de tenir un registre dans certaines circonstances ; Ce registre doit contenir le nom et les coordonnées du traitement pour le compte duquel il agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable

1059. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement*, p. 62.

du traitement ou du sous-traitant et du DPO à la protection des données. Les catégories de traitement effectué pour le compte de chaque responsable du traitement. Une description générale des mesures de sécurité techniques et organisationnelles [1060].

1340 L'obligation de tenir un registre ne concerne cependant que les entreprises de plus de 250 salariés (art. 35 al. 1 RGPD). Cette exception ne s'applique pas, si les traitements concernent :

- Les infractions, condamnations, et mesures de sûreté.
- Les catégories particulières d'informations.
- Des opérations présentant des risques pour les droits et libertés des personnes.

IX. La désignation d'un délégué à la protection des données (ci-après « DPO »)

1341 La désignation d'un DPO est rendue obligatoire par le Règlement, sous certaines conditions [1061]. Cette désignation constitue un élément fondamental du Règlement et une condition essentielle à l'effectivité de la protection des données dans l'Union européenne [1062]. Il est de la responsabilité du responsable du traitement de désigner un DPO à la protection des données [1063].

1342 La désignation obligatoire d'un DPO a été la source de nombreuses tensions politiques entre la Commission, le Parlement et le Conseil durant le processus de négociation du Règlement européen [1064].

1343 La directive 95/46/CE (article 18 al. 2) recommandait la désignation d'un DPO à la protection des données, sans la rendre obligatoire. La France et l'Allemagne [1065] ont transposé cette disposition en droit national. La Suisse a également intégré cette possibilité dans la loi

1060. art. 32, al. 1 RGPD.
1061. art. 37 RGPD.
1062. Ehmann Eugen / Selmayr Martin (édit.), *Datenschutz - Grundverordnung*, 2e éd., Wien 2018, p. 657.
1063. *Ibidem.*
1064. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 716.
1065. art. 28, al. 1 Bundesdatenschutzgesetz allemande du 27 janvier 1977 ; Cf. Également Simitis / Hornung / Döhmann, *Datenschutzrecht : DSGVO mit BDSG*, al. 4 Rn. 1 f.

du 19 Juin 1992 sur la protection des données [1066].

Le Règlement 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et les organes communautaires et à la libre circulation de ces données, imposait déjà la désignation d'un DPO pour chaque institution et organe communautaire [1067]. La désignation d'un DPO à la protection des données dans l'Union n'était donc pas totalement inconnue [1068]. 1344

Le Règlement rend obligatoire pour le responsable du traitement ou le sous-traitant, la nomination d'un DPO [1069], dans les trois cas suivants : 1345

1. « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement, qui du fait de leur nature, de leur portée et/ou de leur finalité, exigent un suivi régulier, et systématique à grande échelle, des personnes concernées ».
2. « les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».
3. « le traitement est effectué par une autorité publique, ou un organisme public, à l'exception des juridictions exerçant dans l'exercice de leurs fonctions juridictionnelles ». Le considérant 97 précise qu'il peut s'agir de « juridictions indépendantes et d'autorités judiciaires indépendantes ». Ces deux notions ne sont pas définies dans le Règlement. Par conséquent, cette formulation ouvre la voie à une interprétation de la part des personnes concernées par l'exception. Poten-

1066. art. 11 a), 5, e) de la loi révisée sur la protection des données du 19 juin 1992 (LPD RS 235.1).

1067. Parlement européen et Conseil de l'UE, *Règlement (CE) 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2001, p. « http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF » (25/10/2017), p. 1 ss, et art. 24, al. 1 RGPD.

1068. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 657.

1069. art. 37 à 39 RGPD.

tiellement, toutes les personnes qui exercent la fonction de juge pourraient être concernées.

1346 Les notions d'autorité publique et d'organisme public ne sont pas non plus définies dans le Règlement. Le groupe de travail de l'Article 29 de la Commission européenne précise dans ses lignes directrices [1070] qu'il incombe aux États membres de l'UE de définir ces deux notions et que celles-ci peuvent être les autorités ou organisations publiques au niveau national, régional ou local.

1347 Les articles 37, 38 et 39 du Règlement encadrent le rôle et les missions du DPO. Ces dispositions sont complétées par les lignes directrices du 13 décembre 2016, concernant la fonction du DPO. Elles visent à clarifier le rôle du délégué, en application du Règlement.

1348 Elles encouragent la désignation d'un délégué, sur une base volontaire, c'est-à-dire même lorsque les conditions imposant la désignation d'un DPO ne sont pas remplies [1071]. Le DPO constitue pour le groupe de travail de l'Article 29 un avantage concurrentiel pour le secteur privé, en ce qu'il favorise la mise en conformité de l'organisation au titre de la protection des données [1072].

1349 Le responsable du traitement et le sous-traitant sont les seuls responsables en cas de manquement à la protection des données. Ils doivent démontrer qu'ils ont pris des mesures pour assurer la conformité de l'organisation aux dispositions du Règlement [1073]. Ils doivent également mettre à disposition du DPO des ressources (financières, humaines, organisationnelles, formations) pour faciliter la mise en œuvre du Règlement par le DPO [1074]. Le groupe de travail de l'Article 29 de la Commission européenne préconise également d'assu-

1070. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs') - Adopted on 13 December 2016, Last Revised and Adopted on 5 April 2017 (WP 243 rev.01)*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 » (30/03/2020), p. 7, consid. 2.1.1.

1071. *Idem*, p. 5.

1072. Article 29 Data Protection Working Party, *Appendix : Core Topics in the View of Trilogue*, in : European Commission (https ://ec.europa.eu/), Brussels 2015, p. « https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf » (25/10/2017).

1073. *Ibidem* et art. 24, al. 1 RGPD.

1074. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 5.

rer une communication des missions du DPO en interne, aux employés ou intervenants concernés par les questions de protection des données [1075].

Le DPO remplit un rôle de conseiller, mais n'est pas responsable à titre personnel de la non-conformité de l'organisation au Règlement [1076]. 1350

Les activités de traitement concernées sont les « activités de base [1077] » du responsable du traitement ou du sous-traitant. 1351

Le groupe de travail de l'Article 29 de la Commission européenne clarifie la notion « d'activité de base ». Il s'agit de toute activité de traitement de données qui forme une part « inextricable [1078] » de l'activité du responsable du traitement ou du sous-traitant. Par exemple, dans le domaine de la santé, le service de soins fourni par un hôpital ne peut pas être séparé du traitement de données. 1352

Le considérant 97 précise qu'il s'agit des activités « principales » du responsable du traitement ou du sous-traitement et non pas du « traitement des données à caractère personnel en tant qu'activité auxiliaire ». « Ainsi lorsque les traitements ne sont effectués qu'au soutien d'une activité auxiliaire du responsable du traitement [1079] », la désignation d'un DPO n'est pas obligatoire. 1353

Les entreprises privées devront désigner un DPO lorsque les activités de base du responsable du traitement ou du sous-traitant consistent : 1354

— « en des opérations de traitement, qui du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou consiste,

— en un traitement à grande échelle de données sensibles ou judiciaires ».

1075. *Idem*, p. 17.
1076. *Idem*, p. 4.
1077. Consid. 97 RGPD.
1078. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 20.
1079. *Idem*, p. 8.

A. La notion de traitement à grande échelle

1355 Le Règlement ne définit pas ce qu'est une activité à grande échelle. Il n'y a pas de limite fixe qui permette de déterminer si un traitement doit être qualifié de traitement à grande échelle ou non.

1356 Le considérant 91, précise, que « dans le cadre d'une analyse de risque, la notion de traitement à grande échelle vise à traiter un nombre « considérable » de données à caractère personnel au niveau régional, national ou international. La doctrine ajoute que ce traitement doit être effectué selon une technique méthodique [1080] ».

1357 Les lignes directrice du groupe de travail de l'Article 29 posent certains critères pour déterminer si le traitement peut être qualifié ou non de traitement à grande échelle. Il retient en particulier les éléments suivants :

- Le nombre de personnes concernées (nombre spécifique ou proportion par rapport à une population) ;
- Le volume de données ou un échantillon de données différentes qui est traité ;
- La durée de traitement ou encore son caractère permanent ou non ; et
- L'étendue territoriale de l'activité de traitement.

1358 D'autres critères comme la durée de l'observation du comportement ainsi que la durée de conservation des données traitées doivent également être prises en compte pour la doctrine [1081]. Il importe également de souligner, que la combinaison de plusieurs des critères précités, permet également de qualifier un traitement de traitement à grande échelle [1082].

1359 En pratique, l'automatisation du traitement et le recours au profilage pour évaluer les préférences, les comportements et des aspects personnels, caractérisent le traitement à grande échelle [1083]. C'est

1080. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 669 (« mit einem methodischen Technikeinsatz ») ; Gola Peter, *EU-DS-GVO EU-Datenschutz-Grundverordnung*, 1e éd., München 2016, p. 315 ; Bittner Timo, *Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf*, in : RDV 2014, p. 183.
1081. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 663.
1082. *Ibidem.*
1083. *Ibidem.*

précisément le cas lors de l'analyse de Big Data [1084]. Dans cette hypothèse, une analyse d'impact sera requise [1085]. Le groupe de travail de l'Article 29 recommande de rechercher les conseils du DPO lors de la conduite d'une analyse d'impact dès la phase initiale [1086].

Sont expressément qualifiés de traitements à grande échelle par le groupe de travail de l'Article 29 de la Commission européenne : 1360

- les traitements de données de passagers utilisant un service de transport public (profilage par le biais d'une carte de voyage) [1087].
- le traitement des données clients d'une entreprise d'assurance, ou d'une banque [1088].
- la géolocalisation en temps réel d'employés dans une chaîne internationale de « restauration rapide » pour un objectif statistique par un sous-traitant spécialisé dans ces activités [1089].
- le traitement de données à caractère personnel à des fins de publicités comportementales par un moteur de recherche [1090].
- le traitement de données (contenu, trafic, localisation) par téléphone ou par le biais de fournisseurs de services internet [1091]

Ne doivent toutefois pas être considérés comme des traitements à grande échelle les traitements qui concernent les données à caractère personnel de patients ou de clients collectées par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre in- 1361

1084. *Ibidem*; Müller Gerhard F., *Der Datenschutzbeauftragte.*, München 1981, p. 235.
1085. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 669 et art. 35, al. 3, a) RGPD. « Il s'agira d'une évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ».
1086. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 13.
1087. *Idem*, p. 10 et 25, (Ex. : équivalent du Swiss Pass).
1088. *Idem*, p. 10 et 25.
1089. *Idem*, p. 10.
1090. *Idem*, p. 10 et 25, "behavioral advertising" by a search engine.
1091. *Idem*, p. 10 et 25.

dividuel [1092].

1362 En cas de doute, la désignation systématique d'un DPO est recommandée puisque toute entreprise ou administration doit être capable, à tout moment, de rendre compte à l'autorité de contrôle de l'État de ses traitements de données à caractère personnel. La notion de traitement à grande échelle relevant d'une appréciation au cas par cas, il convient pour le responsable du traitement ou le sous-traitant de documenter une réflexion à cet égard lorsqu'un responsable du traitement considère qu'il n'entre pas dans son obligation de désigner un DPO eu égard au fait qu'il estime ne pas traiter de données à grande échelle [1093].

B. La notion de « suivi régulier et systématique »

1363 Le Règlement ne définit pas non plus cette notion.

1364 Le groupe de travail de l'Article 29 de la Commission européenne confirme dans les lignes directrices du 13 décembre 2016 [1094], que la notion de suivi régulier et systématique implique les activités de tracking ou de profilage sur internet. Cette notion de « suivi régulier et systématique » ne se limite cependant pas à ces activités et ne se restreint pas à l'environnement numérique [1095].

1365 Pour le groupe de travail de l'Article 29 de la Commission européenne, peut être qualifié de « suivi régulier », un suivi qui :

- intervient à des intervalles particuliers sur une période donnée ;
- est réalisé de façon récurrente et répétitive à certains moments ; ou
- est effectué de façon constante ou de façon périodique.

1366 Pour le groupe de travail de l'Article 29 de la Commission européenne, la notion de « suivi systématique » sera retenue lorsque :

1092. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 25 ; Conseil national des barreaux (France), *Guide pratique : les avocats et le règlement général sur la protection des données (RGPD)*, 1e éd., Issy-les-Moulineaux 2018, p. XXV.
1093. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 5.
1094. *Idem*, p. 8.
1095. *Idem*, p. 8.

— Le traitement intervient en exécution d'un système, ou de façon préétablie, organisée ou méthodique ;

— Il prend place dans une planification générale de la collecte d'information ; ou

— Il s'inscrit dans une stratégie [1096].

Le groupe de travail de l'Article 29 de la Commission européenne cite notamment les exemples suivants : 1367

— la géolocalisation systématique,

— la gestion d'un réseau de télécommunication,

— Le profilage à des fins de publicité comportementale ou d'évaluation des risques (assurances, détection du blanchiment d'argent),

— la surveillance qui implique une collecte régulière d'informations (suivi de la santé par des terminaux mobiles), et

— les prestations de services reposant sur des systèmes automatisés connectés [1097].

L'article 37, al. 4 RGPD. donne aux États membres de l'Union la possibilité d'imposer la désignation d'un DPO dans d'autres situations. 1368

En droit suisse, la LPD prévoit la possibilité de désigner un conseiller à la protection des données [1098], pour assurer l'application interne des dispositions relatives à la protection des données et tenir un inventaire des fichiers. 1369

Le groupe de travail de l'Article 29 de la Commission européenne considère que la désignation d'un DPO constituerait une bonne pratique tant pour les entreprises privées accomplissant des tâches publiques ou exerçant une autorité publique, que pour les sous-traitants lorsque la désignation d'un DPO est obligatoire pour le responsable du traitement [1099]. 1370

Lorsqu'un sous-traitant est désigné par un responsable du traitement, le groupe de travail de l'Article 29 de la Commission eu- 1371

1096. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 11.
1097. *Ibidem.*
1098. art. 11a, al. 5, e) LPD.
1099. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 6 et p. 9.

ropéenne recommande que le DPO désigné par le responsable du traitement supervise aussi le traitement des données effectué par le sous-traitant en sa qualité de responsable du traitement [1100].

1372 Le groupe de travail de l'Article 29 de la Commission européenne considère en outre que, si une organisation désigne un DPO sans avoir d'obligation légale de le faire, alors le statut de DPO avec les obligations et les protections y associées s'appliqueront à l'instar d'un DPO qui a été désigné en vertu de la législation [1101].

1373 Un seul DPO à la protection des données peut également être désigné pour plusieurs entités, dans le secteur privé ou public [1102]. Cette solution pourra être valablement retenue pour un groupe d'entreprises ayant un lien entre elles [1103], à condition que le DPO soit facilement joignable à partir de chaque lieu d'établissement.

1374 Le groupe de travail de l'Article 29 de la Commission européenne offre une interprétation large de la notion de DPO, puisqu'il offre la possibilité à une personne morale de remplir ce rôle. Des sociétés de services comme par exemple des sociétés d'audit pourront être désignées en tant que DPO. Se pose dans ce cas de figure la question de l'indépendance du DPO à la protection des données qui dans cette hypothèse, aura à négocier entre la nécessité de satisfaire son client pour voir son mandat prolongé et celui de remplir son rôle en toute impartialité. L'affaire Enron a servi de précédent et a montré les limites d'un tel modèle ou de telles missions d'audit et de conseil étaient réunies au sein d'un seul cabinet [1104].

1375 L'article 3 du Règlement dispose que le Règlement s'applique au traitement des données à caractère personnel relatif à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

— « à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes, ou

1100. *Idem*, p. 10.
1101. *Idem*, p. 5.
1102. art. 37, al. 3 RGPD.
1103. art. 37, al. 2 RGPD.
1104. Ferrandon Benoît, *Les leçons de l'affaire Enron*, in : Les cahiers français 2002/309, p. 69.

— au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'union ».

Ainsi des responsables du traitement ou sous-traitants établis hors du territoire de l'Union peuvent être amenés à désigner un DPO auquel s'appliqueront les dispositions du Règlement. La Suisse avait déjà prévu la désignation d'un conseiller indépendant à la protection des données, dans sa législation nationale [1105]. 1376

Le responsable du traitement ou le sous-traitant devra choisir un représentant. Celui-ci sera le point de contact des autorités de contrôle et des personnes concernées. Il devra répondre vis-à-vis d'eux du respect des obligations du responsable du traitement ou du sous-traitant qui l'aura désigné par écrit en cette qualité [1106]. Même si le pays bénéficie d'une décision d'adéquation de la Commission européenne, comme la Suisse, un représentant devra être désigné [1107]. 1377

Comme le DPO à la protection des données communique avec les autorités de contrôle, il n'est pas exclu qu'une forme de concurrence entre le représentant et le DPO apparaisse sur ce point [1108]. Le Règlement, quant à lui, n'oblige pas le représentant à désigner un délégué [1109]. 1378

Les entreprises multinationales, pourront choisir avec cohérence la désignation d'un représentant implanté sur le territoire de l'Union pour les représenter auprès des autorités de contrôle et des personnes concernées. La désignation d'un DPO local à la protection des données, au sein des entreprises multinationales présenterait l'avantage de soutenir la mise en œuvre effective d'une gouvernance des données au niveau opérationnelle et organisationnelle. Les deux semblent donc complémentaires. 1379

C. Le profil requis

La Commission et le Parlement européen avaient prévu dans leur proposition que les compétences du DPO devaient être fonction du type de traitement et devaient garantir la protection des données 1380

1105. art. 11 de la Loi fédérale du 19 juin 1992 sur la protection des données, (RS 235.1), Cf. aussi l'Ordonnance du 14 juin 1993 relative à la protection des données (RS 235.11).
1106. art. 27, al. 3 RGPD.
1107. Discussion du 8 février 2017 avec Monsieur Jean-Pierre Walter, Préposé fédéral suppléant à la protection des données, Berne.
1108. Docquir, *Vers un droit européen de la protection des données ?*, p. 135 ss.
1109. *Idem*, p. 135.

traitées [1110]. Si la Commission souhaitait fixer des exigences pour les qualifications du DPO (art. 35, al. 11 Projet de la Commission).

1381 L'article 37, al. 5 du Règlement indique que « le DPO à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 ».

1382 Il s'agira donc d'un spécialiste de la protection des données, idéalement juriste avec une bonne compréhension du fonctionnement des systèmes informatiques et des problématiques de sécurité informatique [1111]. Ses compétences doivent exister au jour de la désignation du DPO [1112]. Il doit avoir des connaissances en droit national et en droit européen en particulier du Règlement général en matière de protection des données [1113].

1383 Celui-ci doit en effet connaître la législation pour en contrôler sa mise en œuvre au sein de l'organisation qui l'a nommé. Il aura également un rôle de conseil en gestion des risques. Il n'a pas de fonction décisionnelle quant à la mise en œuvre ou non d'un traitement [1114].

1384 Le niveau d'expertise requis dépendra également du caractère sensible, de la complexité et du volume de données traitées par l'organisation [1115].

1385 Il faudra également tenir compte de la fréquence des transferts. Si l'organisation transfert des données à caractère personnel de façon systématique à l'extérieure de l'Union européenne ou si ces transferts sont occasionnels, le DPO n'aura pas la même responsabilité.

1386 Le groupe de travail de l'Article 29 de la Commission européenne précise dans ses lignes directrices que sa capacité à exercer la fonction doit s'apprécier au regard de son intégrité et sens de l'éthique

1110. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 717.
1111. Docquir, *Vers un droit européen de la protection des données ?*, p. 135 ss.
1112. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 605.
1113. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 11.
1114. Docquir, *Vers un droit européen de la protection des données ?*, p. 135 ss.
1115. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 11.

ainsi qu'au regard de sa position dans l'organisation [1116].

Les missions du DPO sont présentées à l'article 39 du Règlement. 1387

Le Règlement européen place le DPO à la protection des données au cœur de la gouvernance des données des organisations. Il devra accompagner l'entreprise ou l'institution qui l'a désigné pour vérifier l'application des nouveaux principes, droits et obligations du responsable du traitement. 1388

Les missions du DPO sont avant tout de conseiller et de former les collaborateurs et les membres de la direction [1117]. 1389

En tant que spécialiste en droit de la protection des données, il informe la direction de ses obligations légale et propose à la direction une stratégie. La modification des contrats ne rentre pas dans le champ d'application des missions du DPO, car cette tâche dépasse le rôle de surveillance et de conseil attendu du DPO [1118]. 1390

Le DPO a un rôle de conseil et de contrôle. Il doit augmenter la prise de conscience des collaborateurs aux enjeux de la protection des données. Le contrôle diligenté par le DPO s'exprime par la réalisation d'audits internes pour identifier les risques et les flux de données en interne et en externe. La mission de surveillance des traitements de données par le DPO inclut une vérification concrète de la mise en œuvre des mesures de sécurité [1119]. 1391

Il doit également préparer et mettre à jour certains documents comme le registre des activités de traitement visé à l'article 30 du Règlement. Il conseillera les collaborateurs pour la réalisation des analyses d'impact. 1392

Il a également l'obligation de coopérer avec l'autorité de régulation en tant que première personne de contact (art. 39 d et e RGPD) [1120]. 1393

Il traite les demandes des tiers (personnes concernées et autorités de contrôle) et les plaintes éventuelles. En pratique, il doit s'entourer d'une équipe interdisciplinaire afin notamment de développer 1394

1116. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 11.
1117. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 757.
1118. *Ibidem.*
1119. *Idem*, p. 758.
1120. *Idem*, p. 759.

des processus automatisés (ex. : traitement des demandes d'accès).

1395 Pour cela, « le DPO devra s'appuyer sur le département informatique, chargé de définir et de s'assurer de la mise en œuvre de la politique de sécurité. Celui-ci sera particulièrement sollicité pour documenter les démarches de conformité, afin d'assurer un suivi de la traçabilité des données personnelles et une véritable transparence vis-à-vis de la réglementation [1121] ».

1396 Compte tenu du caractère stratégique et sensible du traitement des données personnelles, le DPO et la direction des systèmes d'information constituent un maillon essentiel du dispositif de gouvernance. Elles doivent donc pouvoir rendre compte directement au comité exécutif, afin de raccourcir la chaîne de décision. C'est une demande de l'article 38, al. 3 RGPD.

1397 « Le DPO à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant [1122] ».

1398 Le Règlement n'aborde pas la question de la responsabilité du DPO à la protection des données. Le groupe de travail de l'Article 29 de la Commission européenne insiste quant à lui dans ses lignes directrices sur la seule responsabilité du responsable du traitement ou du sous-traitant en cas de manquement en matière de protection des données [1123]. En cas de non-conformité, le responsable du traitement demeure responsable des manquements et ne peut pas déléguer sa responsabilité au DPO à la protection des données [1124].

1399 Le DPO ne peut pas recevoir d'instruction et ne dispose d'aucun pouvoir décisionnel. Il ne peut pas être tenu responsable pour des manquements réglementaires [1125]. Ses avis et recommandations n'ont aucune force obligatoire, ni contraignante [1126]. Le responsable du traitement peut décider de ne pas suivre l'avis du DPO, en veillant

1121. Consid. 39 RGPD.
1122. art. 38, al. 3 RGPD
1123. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 4.
1124. *Ibidem.*
1125. Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 761.
1126. Docquir, *Vers un droit européen de la protection des données ?*, p. 165.

à documenter les raisons pour lesquelles cet avis n'est pas suivi [1127].

En cas d'erreurs ou de défaillances graves dans l'exercice de la mission du délégué, et qui devraient être sanctionnées, le Règlement et les lignes directrices du groupe de travail de l'Article 29 de la Commission européenne ne permettent pas de tirer des conclusions claires, d'autant que le DPO ne peut pas être sanctionné pour un motif lié à l'exercice de sa fonction et doit pouvoir faire des constats qui dérangent ou donner des conseils qui n'arrangent pas le responsable du traitement ou le sous-traitant [1128]. 1400

D. La nécessaire absence de conflit d'intérêts

Le Règlement impose que les missions et les tâches du DPO soient exemptes de tout conflit d'intérêts [1129]. Dans le même temps, cet article précise que le DPO peut exercer d'autres fonctions. Il est donc crucial que le responsable du traitement ou le sous-traitant veille à préserver le DPO de tout conflit d'intérêts lors du choix de ses missions [1130]. 1401

Par exemple, un directeur des ressources humaines ou un directeur de l'informatique ne pourra pas dans le même temps être désigné en tant que DPO à la protection des données [1131]. 1402

Sur ce point, le groupe de travail de l'Article 29 de la Commission européenne précise dans ses lignes directrices du 13 décembre 2016 que la fonction de DPO ne pourrait pas être assumée par des personnes qui seront amenées à déterminer les finalités et moyens de traitement des données traitées dans l'organisation [1132]. 1403

Est-ce à dire que tout DPO qui détient un pouvoir de décision dans l'exercice de ses missions ou d'une activité complémentaire dans l'organisation pourrait se trouver dans une situation de conflit d'intérêts ? Peut-il par exemple valider des projets en lien avec la protection des données et effectuer des audits ? 1404

Si le DPO n'est pas salarié de l'organisation, mais bénéficie d'un 1405

1127. Docquir, *Vers un droit européen de la protection des données ?*, p. 13.
1128. *Idem*, p. 157.
1129. art. 38, al. 6 RGPD.
1130. Docquir, *Vers un droit européen de la protection des données ?*, p. 155.
1131. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 695.
1132. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 15.

contrat de service, la question de l'existence de conflits d'intérêts se pose également.

1406 Le conflit d'intérêts pourra surgir du fait des missions confiées au DPO (par exemple mission d'audit du DPO et mission de conseil concernant l'organisation du même client), ou encore du fait de l'existence de plusieurs clients, aux intérêts potentiellement opposés. Le DPO ne pourra pas non plus par exemple être membre d'une autorité de contrôle [1133].

E. Le statut de DPO

1407 Le DPO peut bénéficier du statut de salarié ou d'indépendant [1134], mais « doit offrir des garanties d'indépendance dans l'exercice de ses missions [1135] ».

1408 Le responsable du traitement et le sous-traitant veillent à ce que le DPO ne reçoive aucune instruction [1136].

1409 Dans le cadre de l'exercice d'un contrat de travail, qui repose sur un lien de subordination, cette garantie d'indépendance paraît difficile à mettre en pratique et à démontrer.

1410 Le groupe de travail de l'Article 29 de la Commission européenne précise dans ses lignes directrices [1137], que le DPO devrait consulter librement l'autorité de contrôle sur une question. Par cette garantie d'indépendance, le DPO peut identifier des risques pour l'organisation que le responsable du traitement ou le sous-traitant préférerait ignorer.

1411 Le groupe de travail de l'Article 29 de la Commission européenne indique que le DPO devra bénéficier du soutien du haut management. Le Règlement précise encore, que le DPO fait directement rapport au niveau le plus élevé de la direction du responsable du

1133. Docquir, *Vers un droit européen de la protection des données ?*, p. 155.
1134. art. 37, al. 6 RGPD.
1135. Consid. 97 RGPD.
1136. La question se pose de savoir s'il peut en revanche donner des instructions en ce qui concerne l'exercice de ses missions, sans pour autant déterminer les finalités et les moyens du traitement ?
Et aussi art. 38, al. 3 RGPD.
1137. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, n° 2.3, p. 10.

traitement ou du sous-traitant [1138].

Ce même article établit une protection du DPO. Celui-ci « ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant du fait de l'exercice de ses missions ». 1412

Le groupe de travail de l'Article 29 de la Commission européenne relève que les pénalités sont à interpréter de manière large comme toute conséquence ou menace de conséquence négative sur l'évolution de la carrière, la rémunération, le renouvellement d'un contrat qui interviendrait pour un motif lié à l'exercice des missions du délégué. Le DPO pourra voir ses missions retirées tout en le conservant au service de la même organisation pour d'autres fonctions. 1413

Pour le groupe de travail de l'Article 29 de la Commission européenne, seules des circonstances étrangères à l'exercice des missions (vol, harcèlement sexuel ou moral), pourraient justifier un licenciement. Cela pose la question de gestion des relations de travail avec un DPO non diligent. 1414

Enfin, le Règlement impose au délégué [1139], « de tenir compte dans l'accomplissement de ses missions du risque associé aux opérations de traitement, compte tenu de la nature, de la portée, et des finalités du traitement ». Il devra donc travailler en partenariat avec le département du Risk Management, en gardant à l'esprit que les décisions relatives à des traitements, au regard des risques identifiés, incomberont à une autre personne. Il ne dispose d'aucun pouvoir décisionnel. Le groupe de travail de l'Article 29 de la Commission européenne confirme que le DPO devra adopter une approche orientée sur la gestion des risques [1140]. 1415

F. L'obligation au secret professionnel

L'article 38, al. 5 impose au DPO « une obligation de secret professionnel ou une obligation de confidentialité, en ce qui concerne l'exercice de ses missions ». 1416

Ainsi, chaque État évaluera le besoin d'une loi, qui soumettrait le DPO à une obligation au secret professionnel [1141]. A défaut, le 1417

1138. art. 38, al. 3 RGPD.
1139. art. 39, al. 2 RGPD.
1140. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 17.
1141. Docquir, *Vers un droit européen de la protection des données ?*, p. 161.

contrat de travail réglera cette question.

1418 Cette obligation de secret ou de confidentialité n'empêche cependant pas le DPO de solliciter un conseil ou un avis de l'autorité de contrôle nationale [1142]. Le groupe de travail de l'Article 29 de la Commission européenne ne limite donc pas la collaboration du DPO avec l'autorité de contrôle, à une relation unilatérale, au sens de l'article 31. Si l'autorité de contrôle peut requérir des informations spontanément auprès du DPO, dans l'exercice de ses missions, l'inverse est vrai également [1143]. Le DPO constitue un partenaire central pour l'autorité de contrôle [1144].

G. Les obligations du responsable du traitement ou du sous-traitant envers le DPO

1419 L'article 38, al. 2 RGPD. fixe les obligations du responsable du traitement ou du sous-traitant.

1420 Le responsable du traitement doit également bénéficier des ressources matérielles ou de personnel, de la possibilité de suivre des formations, et lorsqu'il remplit plusieurs fonctions, l'organisation de sa charge de travail doit lui permettre d'accomplir ses fonctions de DPO.

1421 Il devra également bénéficier de l'information nécessaire à l'accomplissement de ses missions et pour cela devra avoir accès aux différents services. Ceux-ci peuvent également le contacter directement : « au sujet de toutes les questions relatives au traitement de leurs données, à caractère personnel et à l'exercice des droits que leur confère le [...] Règlement [1145] ». Le DPO doit pouvoir exercer effectivement les missions qui lui sont dévolues. Le Règlement est en cela assez protecteur puisqu'il impose au responsable du traitement ou du sous-traitant « d'associer [le délégué] d'une manière appropriée et en temps utile, à toutes les questions relatives à la

1142. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 10.
1143. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 706.
1144. Härting, *Datenschutz-Grundverordnung*, Rn. 20 ; Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 707.
1145. art. 38, al. 4 RGPD.

protection des données à caractère personnel [1146]».

Le groupe de travail de l'Article 29 de la Commission européenne recommande l'élaboration de procédures internes pour identifier dans quelle hypothèse il convient de consulter le DPO à la protection des données, de manière préventive [1147] ou réparatrice [1148]. 1422

Son identité et son rôle devront être publiés en interne [1149]. 1423

Toute violation des dispositions précédentes peut être sanctionnée. Par exemple, si le responsable du traitement ou le sous-traitant ne respecte pas les obligations qui lui incombent pour permettre au DPO d'exercer sa mission de manière effective et indépendante. L'autorité de contrôle peut imposer une amende pouvant s'élever à EUR 10'000 ou dans le cas d'une entreprise jusqu'à 2 % du chiffre d'affaire annuel mondial total de l'exercice précédent [1150]. 1424

Le rôle du DPO à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le Règlement, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de contrôle. 1425

§4 Les flux transfrontaliers

Le principe de la libre circulation des données à caractère personnel au sein de l'Union européenne, consacré dans la directive 95/46/CE, est conservé dans le Règlement. Il en va de même pour le principe de prohibition des transferts vers l'étranger de données à caractère personnel de l'Union européenne. 1426

Certains États, comme la Suisse, bénéficient d'une décision d'adéquation de la part de la Commission européenne. Cette décision rend licites les flux transfrontaliers de données à caractère person- 1427

1146. art. 38, al. 1 RGPD.
1147. art. 25 RGPD.
1148. art. 33 RGPD ; Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 13.
1149. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 14.
1150. art. 83, al. 4 RGPD.

nel.

1428 À défaut de décision d'adéquation, les États doivent avoir recours à des clauses contractuelles types avant d'effectuer des transferts de données à caractère personnel vers des pays tiers. La Commission européenne a adopté des modèles de clauses contractuelles qui encadrer les transferts de données personnelles effectués par des responsables de traitement vers des destinataires situés hors de l'Union européenne [1151]. Elles ont pour but de faciliter la tâche des responsables de traitement dans l'élaboration de contrats de transferts. Ces contrats peuvent être conclus entre deux responsables de traitement ou entre un responsable de traitement et son sous-traitant. Il existe donc deux types de clauses afin d'encadrer chacun des transferts. Ces clauses contractuelles rendent licites les transferts de données à caractère personnel vers des pays tiers. La validité des clauses contractuelles était contestée et une interprétation de la CJUE était attendue sur cette question [1152]. Le 19 décembre 2019, la CJUE a confirmé la validité de la décision 2010/87/UE relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers [1153].

I. Principe d'interdiction des flux transfrontaliers de données personnelles

1429 Le Règlement interdit les flux transfrontaliers de données à caractère personnel vers des pays ne disposant pas de décision d'adéquation de la part de la Commission européenne. La décision d'adéquation reconnaît que le pays concerné offre un niveau adéquat de

1151. CNIL, *Clauses Contractuelles Types*, in : CNIL (https://www.cnil.fr/), Paris s.a., p. « https://www.cnil.fr/fr/definition/clauses-contractuelles-types » (17/06/2019).

1152. Arrêt CJUE du 9 Mai 2018, *The High Court Commercial between the Data Protection Commissioner and Facebook Ireland Ltd and Maximillian Schrems*, C-311/18, consid. 1-11, p. « https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62018CN0311:EN:HTML » (08/10/2017).

1153. Saugmandsgaard Henrik, *Conclusions de l'avocat général dans l'affaire C-311/18 Facebook Ireland et Schrems - Communiqué de presse de la CJUE du 19 décembre 2019, No. 165/2019*, in : CJUE (https ://curia.europa.eu/), Luxembourg 2019, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62018CC0311 » (31/03/2020).

protection des données personnelles [1154].

Les transferts vers des pays tiers non adéquats sont interdits, sauf s'ils offrent certaines garanties. Ces garanties peuvent être de plusieurs natures. Il peut s'agir de l'adhésion pour les entreprises américaines au programme américain « Privacy Shield », ou de la conclusion de clauses contractuelles types, ou encore de la mise en place de règles d'entreprises contraignantes. Le Règlement présente également deux autres types de garanties que sont les codes de conduite et les mécanismes de certification. L'objectif de ces garanties est de s'assurer que le niveau de protection des personnes physiques, tel que garanti par le Règlement, ne soit pas compromis [1155]. 1430

A. La notion de transfert

Le Règlement ne définit pas cette notion. Il fait uniquement référence au « transfert de données à caractère personnel vers des pays tiers ou vers des organisations internationales [1156] ». 1431

La Cour de Justice a précisé dans son arrêt Linqvist du 6 novembre 2003 (C-101/01) [1157], que « le seul fait de pouvoir accéder aux données à caractère personnel via une page internet ne suffisait pas pour caractériser un transfert de données, lorsqu'une personne télécharge ces données à partir d'un serveur, à partir de l'Union européenne, et que ces données sont conservées sur le territoire de l'Union européenne [1158] ». La Cour a retenu l'absence de « relation directe entre l'émetteur et le destinataire de la donnée [1159] ». 1432

B. Les sous-traitants

Contrairement à la directive 95/46/CE, le Réglement applique aux sous-traitants les règles relatives aux transferts de données à caractère personnel [1160]. 1433

Il augmente ainsi considérablement le nombre d'obligations direc- 1434

1154. Docquir, *Vers un droit européen de la protection des données ?*, p. 64.
1155. art. 44 RGPD.
1156. Consid. 101 RGPD.
1157. Arrêt CJUE du 6 novembre 2003, *Linqvist*, C-101/01, ECLI :EU :C :2003 :596, consid. 71.
1158. *Ibidem.*
1159. *Ibidem.*
1160. Consid. 109 RGPD.

tement applicables aux sous-traitants [1161].

1435 Les sous-traitants doivent ainsi prévoir des garanties spécifiques pour les transferts de données personnelles vers les pays non adéquats [1162].

C. Les groupes d'entreprises

1436 Le Règlement accorde une attention spécifique aux groupes d'entreprises, à leurs filiales ou succursales. Ces groupes peuvent avoir un intérêt légitime à effectuer des transferts transfrontaliers [1163]. L'existence d'un intérêt légitime rend licites les transferts transfrontaliers intragroupes.

II. La compétence de la Commission européenne pour la décision d'adéquation (art. 45 RGPD)

1437 La Commission européenne détient une compétence exclusive pour prendre une décision d'adéquation en faveur d'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers. L'adoption d'une telle décision offre la confiance que cet État, ce territoire ou ces secteurs déterminés assurent un niveau de protection adéquat du point de vue du droit de la protection des données personnelles [1164]. Par conséquent, aucune autorisation supplémentaire n'est requise pour le pays tiers, car le niveau de sécurité juridique et d'uniformité obtenu dans l'ensemble l'Union est considéré comme étant satisfaisant [1165]. Ainsi, une décision d'adéquation présente l'avantage de faciliter les transferts de données vers des pays tiers. Le pays qui bénéficie d'une décision d'adéquation doit cependant respecter toutes les dispositions du Règlement. Il doit en particulier veiller à la licéité des transferts de données à caractère personnel, mais n'est pas tenu de recourir à des mécanismes de transfert de données, tels que les clauses contractuelles types ou encore les règles d'entreprises contraignantes (en anglais, Binding Corporate Rules), du fait de l'existence d'une décision d'adéquation.

1161. art. 28 et 44 RGPD.
1162. art. 46 RGPD.
1163. Consid. 48 RGPD.
1164. art. 45 RGPD.
1165. Consid. 103 RGPD.

A. Les nouveaux principes applicables aux transferts

(a) La décision d'adéquation

La directive 95/46/CE ne s'appliquait qu'aux pays tiers. Le Règlement [1166] autorise quant à lui la Commission européenne à adopter des décisions d'adéquation non seulement pour un pays tiers, mais également pour un territoire d'un pays tiers, et un ou plusieurs secteurs déterminés dans un pays tiers. Le Règlement élargit donc le champ d'application des décisions d'adéquation. Sur ce fondement (art. 45, al. 3 RGPD), certaines entreprises d'un même secteur d'activité (nouvelles technologies, banque, assurance, télécommunication…) solliciteront peut-être une décision d'adéquation de la part de la Commission européenne. 1438

Si le champ d'application des décisions d'adéquation est élargi, la notion de « secteur déterminé [1167] » n'est en revanche pas définie. Ni les articles, ni les considérants [1168] du Règlement ne définissent cette notion. 1439

La jurisprudence de la CJUE [1169] a précisé que « la décision d'adéquation a pour objet d'autoriser le transfert de données à caractère personnel vers le pays tiers concerné. Cela n'implique pas que les autorités de contrôle ne peuvent plus être saisies par les citoyens de l'Union d'une demande visant à protéger leurs données à caractère personnel ». « Les États membres et les autorités nationales de contrôle ne peuvent être tenus de manière absolue par une décision d'adéquation de la Commission ». Par conséquent, pour assurer une protection appropriée des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, les autorités nationales de contrôle doivent être habilitées, en cas d'allégations faisant état de violations de ces droits, à mener des enquêtes et de suspendre le transfert de données vers le destinataire établi dans ce pays tiers. 1440

1166. art. 45, al. 3 RGPD.

1167. Kühling Jürgen / Buchner Benedikt (édit.), *Datenschutz - Grundverordnung : Kommentar*, 1e éd., München 2017, p. 754.

1168. *Ibidem.*

1169. Arrêt Schrems du 6 octobre 2015, C-362/14, ECLI :EU :C :2015 :650, consid. 57.

(b) Les conditions pour bénéficier d'une décision d'adéquation

1441 La Commission européenne vérifie que les conditions suivantes sont réunies (art. 45 RGPD) :

- « L'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers [1170] ». Ces autorités sont chargées « d'assurer le respect des règles en matière de protection des données, les règles professionnelles et les mesures de sécurité ». Ces autorités détiennent un pouvoir de contrainte et de conseil pour assister les personnes concernées dans l'exercice de leurs droits.
- « L'État de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente tant générale que sectorielle (y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal) [1171] ». L'accès des autorités publiques aux données personnelles, la jurisprudence (recours administratifs et judiciaires) sont également inclus.
- « Les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiques contraignants, ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en ce qui concerne la protection des données à caractère personnel [1172] ».

1442 La Commission publie sa décision d'adéquation dans le journal officiel de l'Union européenne, que celle-ci soit positive ou négative [1173]. « Le site internet de la Commission européenne dresse la liste de ces décisions [1174] ».

1443 La Commission européenne dispose d'un pouvoir d'appréciation étendu [1175]. Dans son arrêt C-362/14, la CJUE vient préciser la notion de niveau de protection adéquat. « Ce terme implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection

1170. art. 45, al. 2, b) RGPD.
1171. art. 45, al. 2, a) RGPD.
1172. art. 45, al. 2, c) RGPD.
1173. art. 45, al. 8 RGPD et op.cit., Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 762.
1174. art. 45, al. 8 RGPD.
1175. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 755.

identique à celui garanti dans l'ordre juridique de l'Union ». Toutefois [...], l'expression « niveau de protection adéquat » doit être comprise comme exigeant que ce pays tiers assure effectivement [...] un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union [1176]. Cette interprétation effectuée dans le cadre de la directive 95/46/CE, sur la base de l'article 25, al. 6, demeure toutefois toujours d'actualité avec le Règlement.

Le caractère effectif du niveau de protection adéquat doit être garanti par « l'ordre juridique du pays tiers visé par la décision de la Commission ». Cela signifie que le pays en question soit recourir à des moyens qui, en pratique, sont « effectifs » afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union [1177]. 1444

(c) La procédure d'adoption d'une décision d'adéquation

Comment est prise une décision d'adéquation ? Une telle décision est prise par les représentants des États membres de l'UE. Ils se regroupent en comité et rendent un avis sur la décision d'adéquation. 1445

Seuls onze pays bénéficient d'une telle décision d'adéquation : Andorre, Argentine, Canada, îles Feroé, Guernsey, Israël, île de Man, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay. L'accord Privacy Shield pourrait être ajouté à cette liste, bien qu'il s'agisse pour les entreprises américaines de décider de s'enregistrer auprès du département du Commerce américain pour bénéficier du programme de Privacy Shield. 1446

Quid des décisions prises par la Commission sur le fondement de la directive 95/46/CE/ Celles-ci restent valables et « applicables, jusqu'à ce que la Commission les modifie, les remplace ou les abroge [1178] ». 1447

En 2019, la Commission européenne a octroyé une décision d'adéquation en faveur du Japon, « donnant naissance au plus grand espace de flux sécurisés de données au monde [1179] ». Elle examine ac- 1448

1176. op.cit., Arrêt C-362/14, consid. 73.
1177. op.cit., Arrêt C-362/14, consid. 74.
1178. art. 45, al. 9 RGPD.
1179. Commission européenne, *La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde - Communiqué de presse du 23 janvier 2019*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2019,

tuellement la possibilité d'adopter des décisions d'adéquation avec la Corée du Sud. Elle entend aussi débuter des discussions avec l'Inde et des pays d'Amérique du Sud. Une liste exhaustive est disponible sur le site internet de la Commission européenne [1180].

1449 Pour la doctrine, l'octroi d'une décision d'adéquation peut être influencé par des obligations internationales [1181]. Ainsi la participation d'un État tiers à la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé de données personnelles, peut-elle favoriser l'obtention d'une telle décision [1182]. Encore faut-il que l'État ratifie cette Convention lors de toute modification ultérieure.

(d) Les garanties fondamentales

1450 Sur la base de la jurisprudence de la CJUE et de la Cour européenne des droits de l'homme, le groupe de travail de l'Article 29 de la Commission européenne, a reconnu quatre garanties fondamentales pour le traitement de données personnelles [1183].

1451 Ces garanties sont les suivantes :

— Le traitement doit être fondé sur des règles claires, précises et accessibles.

— La preuve de la nécessité et de la proportionnalité des objectifs légitimes poursuivis doit être rapportée par l'État demandeur.

---

p. « http://europa.eu/rapid/press-release_IP-19-421_fr.htm » (04/06/2019).

1180. Commission européenne, *Échange et protection des données à caractère personnel à l'ère de la mondialisation - Communication de la Commission au Parlement européen et au Conseil du 10 janvier 2017 (COM(2017) 7 final)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2017, p. « http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017DC0007&from=FR » (29/06/2017), p. 9.

1181. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 758.

1182. Conseil fédéral, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1, RO 2002 2847)*, in : Conseil fédéral (https ://www.admin.ch/), Berne 1981, p. « https://www.admin.ch/opc/fr/classified-compilation/20012356/index.html » (09/10/2017).

1183. Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision - Adopted on 13 April 2016 (WP 238)*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf » (31/03/2020), p. 33.

— Un mécanisme de supervision indépendant doit être mis en place (rôle du juge principalement).

— Des voies de recours effectives doivent exister pour les individus.

Il est d'avis qu'« un accès généralisé des autorités publiques aux communications électroniques des particuliers doit être regardé comme compromettant l'essence même du droit fondamental au respect de la vie privée [1184]». 1452

Le groupe de travail de l'Article 29 de la Commission européenne a adopté une opinion le 13 avril 2016, relative aux interférences avec le droit fondamental à la vie privée et à la protection des données, par le biais de mesures de surveillance. Cet avis cible uniquement le transfert de données à caractère personnel [1185]. Cet avis fait référence à l'arrêt Schrems rendu par la CJUE cité préalablement. Il confirme que la réglementation européenne doit fournir des garanties en cas d'interférence avec les droits fondamentaux des articles 7 et 8 de la Charte, et notamment des règles précises et claires concernant le champ d'application et la mise en œuvre d'une mesure, et des garanties minimales afin que les personnes concernées par le transfert de données bénéficient de garanties suffisantes contre le risque d'abus et contre tout accès illicite et l'utilisation arbitraire des données à caractère personnel [1186]. 1453

Le groupe de travail rappelle que la protection des droits fondamentaux doit être garantie, en cas d'interférence arbitraire, lorsque les données sont transférées vers un pays bénéficiant d'une décision d'adéquation [1187]. 1454

(e) L'examen périodique des décisions d'adéquation

Après avoir rendu une décision d'adéquation, la Commission effectue un suivi périodique pour évaluer si le pays tiers, territoire ou 1455

1184. *Idem*, pp. 1-58.

1185. Article 29 Data Protection Working Party, *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) - Adopted on 13 April 2016 (WP 237)*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf » (31/03/2020).

1186. *Idem*, p. 4.

1187. *Idem*, p. 4 ; Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 758.

secteur, assure un niveau de protection adéquat. Cet examen doit avoir lieu au moins tous les quatre ans [1188].

1456 La ré-évaluation de l'adéquation de la législation suisse au cadre juridique européen en matière de protection des données posera vraisemblablement du fait des différences majeures entre les dispositions du RGPD, de la LPD actuelle et de la lenteur du processus d'adoption de la LPD révisée. En outre, la LPD révisée prévoit des sanctions à hauteur de CHF 250 000 uniquement ce qui est très éloigné des dispositions du RGPD.

1457 Bien que la Commission prenne en compte « toutes les évolutions pertinentes », la Suisse aura des difficultés à expliquer les raisons de la lenteur de l'adoption de la LPD révisée. Une annulation ou une modification par la Commission européenne de la décision d'adéquation suisse durant la phase d'examen périodique serait dommageable pour la licéité des transferts entre l'UE et la Suisse et préjudiciable aux activités économiques. La lenteur de la procédure législative suisse est le reflet d'une prise de conscience tardive des enjeux en lien avec la protection des données à l'ère digitale. Elle est également le miroir d'une politique peu centrée sur une protection juridique effective des personnes concernées, sous l'influence du milieu économique (ex : analyse d'impact de PwC).

1458 « Le Parlement et le Conseil de l'UE, sont consultés durant la procédure d'examen périodique et donnent leur avis » (consid. 106 RGPD). « Le comité européen à la protection des données conseille la Commission pour les pays tiers [1189] ».

1459 Après une analyse détaillée, la Commission peut décider de modifier, de suspendre ou d'abroger une décision d'adéquation en vigueur [1190]. Cette décision n'a pas d'effet rétroactif. En cas de désaccord entre la commission et le pays tiers, des consultations ont lieu afin de trouver un consensus [1191].

1460 En l'absence de consensus, le pays perd le bénéfice de la décision d'adéquation et devra légitimer ses transferts sur la base de méca-

1188. art. 45, al. 3 RGPD.
1189. Consid. 139 RGPD.
1190. art. 45, al. 5 RGPD et consid. 107 RGPD.
1191. art. 45, al. 6 RGPD et consid. 107 RGPD.

nismes de transfert contractuels ou de dérogations.

L'arrêt Schrems rendu par la CJUE a clarifié la compétence exclusive de la CJUE pour invalider une décision d'adéquation. Il a précisé la notion d'adéquation. Une autorité de contrôle des données n'est pas compétente pour invalider une décision d'adéquation. L'autorité de contrôle nationale devra épuiser les voies de voies de recours nationales puis effectuer un renvoi préjudiciel devant la CJUE, qui examinera la validité de la décision d'adéquation et pourra invalider celle-ci [1192]. 1461

La CJUE retient qu'un niveau de protection adéquat ne se confond pas avec un niveau identique de protection tel qu'assuré par la directive et la Charte dans l'UE. 1462

Un niveau de protection adéquat correspond pour la CJUE à d'un niveau de protection qui y est « substantiellement équivalent ». Il convient de prouver que le pays tiers recourt à des moyens effectifs en pratique afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'UE. Il s'agit de s'assurer qu'en pratique l'ordre juridique du pays tiers assure effectivement un tel niveau de protection. 1463

Les décisions d'adéquation rendues par la Commission européenne restent valables jusqu'à leur modification ou leur suspension par la Commission [1193]. 1464

Une décision d'adéquation a été rendue à ce jour pour les pays suivants : 1465

- Andorre
- Argentine
- Australie
- Iles Féroé
- Guernsey
- Ile de Man
- Israël

1192. Arrêt CJUE du 6 octobre 2015, *Maximilian Schrems vs. Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :650, consid. 140.

1193. art. 45, al. 9 RGPD ; Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 762.

— Jersey

— Canada

— New-Zeland

— Suisse [1194]

— Uruguay.

1466 Si une décision d'adéquation venait à être suspendue de la part de la Commission européenne, le transfert de données à caractère personnel vers des États tiers ou vers des organisations internationales resterait toujours valable [1195], dès lors qu'il est fondé sur les articles 46 à 49 RGPD.

III. L'accord Privacy Shield (article 45 RGPD)

1467 L'accord Privacy Shield a été adopté le 12 juillet 2016 [1196], en remplacement de l'accord Safe Harbor, invalidé par la CJUE dans l'arrêt Schrems (voir paragraphe 140).

1468 L'accord Privacy Shield a tout d'abord fait l'objet d'un projet initial, préparé en quatre mois par la Commission européenne et les États-Unis, à la suite de l'invalidation par la CJUE de l'accord Safe Harbor [1197]. Ce projet ayant connu de vives critiques, il a ensuite été modifié, puis approuvé le 12 juillet 2016.

1469 Les principes fondateurs demeurent identiques au Safe Harbor : la co-régulation et la certification volontaire. Toute entreprise américaine, enregistrée auprès du Département du Commerce américain est autorisée à transférer des données à caractère personnel vers les États-Unis. Pour être autorisée à s'enregistrer auprès du Dépar-

1194. Commission européenne, *Décision 2000/518/CE du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse (notifiée sous le numéro C(2000) 2304)*, in : Office des publications de l'Union européenne (https ://op.europa.eu/), Luxembourg 2000, p. « https://op.europa.eu/fr/publication-detail/-/publication/ee76f93d-4545-4878-87cb-7750d7f59987 » (10/10/2017).

1195. art. 45, al. 7 RGPD.

1196. Commission européenne, *La Commission européenne lance le bouclier de protection des données UE-États-Unis : une protection renforcée pour les flux de données transatlantiques - Communiqué de presse du 12 juillet 2016*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2016, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_2461 » (31/03/2020), pp. 1-3.

1197. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 764.

tement du commerce, l'entreprise doit avoir une politique de protection de la vie privée conforme aux principes du Privacy Shield en matière de protection des données [1198].

La Commission européenne considère à ce jour que les garanties offertes par le Privacy Shield sont suffisantes pour autoriser les flux transfrontaliers entre l'UE et les États-Unis, sans mécanisme contractuel complémentaire. 1470

Le groupe de travail de l'Article 29 de la Commission européenne a émis un avis très critique sur le projet initial de Privacy Shield [1199]. Il a souligné la nécessité de tenir compte du contexte international et des besoins accrus de sécurité. Il a en outre insisté sur le fait que la décision d'adéquation Privacy Shield a été adoptée sur la base de la directive 95/46/CE. Par conséquent, une réévaluation de cette décision d'adéquation devait intervenir après l'entrée en vigueur du RGPD compte tenu des différences substantielles le concernant [1200]. 1471

Dans son avis 01/2016, le groupe de travail de l'Article 29 de la Commission européenne a relevé que certains principes clés du droit européen ne figuraient pas dans le projet Privacy Shield. Plus précisément, le Privacy Shield ne « ferait pas mention des décisions individuelles prises sur une base automatisée ou ne mentionnerait pas le principe de conservation des données ». Le groupe de travail de l'Article 29 de la Commission européenne a en outre soulevé « le caractère compliqué et donc ineffectif des voies de recours prévues pour les citoyens européens en cas de transfert de leurs données à caractère personnel aux États-Unis [1201] ». Le Privacy Shield reconnaissait expressément la possibilité pour les États-Unis d'accéder à des données à caractère personnel de citoyens européens dans un objectif de « sécurité nationale » et de « respect des lois ». 1472

Le groupe de travail a rappelé que « la surveillance de masse systématique des individus ne peut jamais être considérée comme respectant le principe de proportionnalité et de stricte nécessité, ap- 1473

1198. European Commission, *Guide : EU-US Privacy Shield*, in : European Commission (https ://ec.europa.eu/), Brussels 2016, p. « https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf » (31/03/2020), p. 7.

1199. Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, pp. 1-58.

1200. *Idem*, p. 3

1201. *Ibidem.*

plicables dans une société démocratique [1202]».

1474 Si le groupe de travail reconnaissait la désignation d'un Médiateur (Ombudsman) comme étant un élément favorable à la protection des droits des individus eu égard au contrôle étendu des services de renseignements américains, il a cependant souligné son défaut d'indépendance, la carence des pouvoirs à sa disposition (pour remplir ses obligations de façon effective) et le fait qu'il ne constituait pas un recours satisfaisant en cas de conflit [1203].

1475 Le groupe de travail de l'Article 29 de la Commission européenne a incité la Commission européenne à re-négocier le contenu du projet Privacy Shield afin d'améliorer la décision d'adéquation entre les États-Unis et l'Union européenne et de s'assurer que la décision offerte par le Privacy Shield offrait des garanties équivalentes à celles de l'Union européenne [1204].

1476 Sur la base de l'avis exprimé par le groupe de travail de l'Article 29, le Parlement européen a demandé à la Commission européenne « de poursuivre ses négociations avec les États-Unis afin de remédier aux « failles » que présente le bouclier « vie privée » concernant les données des citoyens européens transférées aux États-Unis à des fins commerciales [1205]».

1477 Cette procédure donna lieu à une révision du projet Privacy Shield initial au mois de juin 2016. La Commission européenne entérina le second projet Privacy Shield, le 12 juillet 2016 [1206].

1478 La seconde version du Privacy Shield présente des garanties supplémentaires concernant le respect des droits des personnes concernées. Ainsi un droit à la suppression des données fut reconnu dans la seconde version du Privacy Shield. Des garanties d'indépendance concernant le rôle du médiateur (Ombudsman) ont également été

1202. Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p. 4.
1203. *Ibidem.*
1204. *Ibidem.*
1205. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 765 ; Parlement européen, *Bouclier « vie privée » UE-États-Unis : des améliorations à apporter - Communiqué de presse du 26 mai 2016*, in : Parlement européen - Actualité (https ://www.europarl.europa.eu/), Bruxelles 2016, p. « http://www.europarl.europa.eu/news/fr/press-room/20160524IPR28820/bouclier-vie-privee-ue-etats-unis-des-ameliorations-a-apporter » (09/10/2017).
1206. Commission européenne, *Décision d'exécution (UE) 2016/1250*, pp. 1-212.

octroyées [1207].

Le groupe de travail de l'Article 29 de la Commission européenne a publié un avis en date du 22 janvier 2019 [1208], dans lequel il reconnaît les améliorations apportées au Privacy Shield, tout en constatant, entre autres, que les décisions individuelles prises sur une base automatisée ne figuraient pas dans le texte et qu'aucun droit d'opposition n'était reconnu aux individus [1209]. 1479

En application de la seconde version du Privacy Shield, les politiques de confidentialité des entreprises américaines participant au programme Privacy Shield doivent désormais respecter certains principes [1210]. 1480

Transferts ultérieurs : les entreprises doivent encadrer les transferts ultérieurs vers d'autres entreprises par un contrat. Il s'agit notamment des transferts de données à caractère personnel vers des sous-traitants. Ce contrat doit inclure des obligations et restrictions spécifiques. Les obligations et restrictions divergent en fonction de la qualité du destinataire (sous-traitant ou responsable du traitement). 1481

Qualité des données et finalité de traitement : seules les données « adéquates, pertinentes et non excessives pour la finalité du traitement », doivent être traitées par les entreprises ayant adhéré au programme du Privacy Shield. Le traitement ne doit pas excéder la durée nécessaire à la réalisation des finalités pour lesquelles les données sont collectées et traitées. 1482

Droits des citoyens européens renforcés : les citoyens européens bénéficient d'un droit d'accès aux données les concernant. Ils peuvent également solliciter des informations auprès de l'entreprise, à l'origine d'une décision produisant des effets juridiques et qui a été prise sur le seul fondement d'un traitement automatique de don- 1483

1207. Celui-ci n'étant pas lié aux services de renseignements américains (op.cit., Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 766).
1208. EDPB, *EU - U.S. Privacy Shield : Second Annual Joint Review report - Adopted on 22 January 2019*, in : EDPB (https ://edpb.europa.eu/), Brussels 2019, p. « https : / / edpb . europa . eu / sites / edpb / files / files / file1 / 20190122edpb _ 2ndprivacyshieldreviewreport_final_en.pdf » (31/03/2020).
1209. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 766.
1210. Commission européenne, *Décision d'exécution (UE) 2016/1250*, Annexe II : « Principes du cadre Bouclier de protection des données UE-Etats-Unis ».

nées.

1484 Recours contre les entreprises qui adhèrent au programme Privacy Shield : Les personnes concernées peuvent déposer une plainte auprès de l'entreprise, ou auprès des autorités de contrôle en Europe, qui travailleront en coopération avec les entreprise américaines correspondantes. Une procédure de résolution alternative des conflits est également envisageable.

1485 Lorsqu'une entreprise n'utilise plus l'accord Privacy Shield, les données collectées doivent être supprimées par l'entreprise dans le cadre de son ancienne adhésion ou s'engager auprès du Département du Commerce américain à continuer d'utiliser ces données en conformité avec les principes du Privacy Shield.

1486 L'adhésion doit être renouvelée par l'entreprise chaque année [1211].

1487 Le Judicial Redress Act, promulgué le 24 février 2016 aux États-Unis, permet en outre aux citoyens de l'UE de saisir les tribunaux américains pour faire valoir leurs droits au respect de la vie privée en cas d'utilisation abusive concernant des données transférées vers les USA à des fins d'ordre public. Elle étend également aux citoyens européens les droits dont jouissent les citoyens américains en vertu de la loi de 1974 sur le respect de la vie privée (Privacy Act) [1212].

1488 Depuis le 1er Aout 2016, plus de 2509 entreprises ont adhéré à l'accord Privacy Shield [1213]. Ce programme fait cependant l'objet de deux recours en annulation près la CJUE, de la part de Digital Rights Ireland, et de la part de la Quadrature du Net. Ces recours ont partiellement été examinés en 2017.

1489 La question de fond concernait la licéité des transferts de données personnelles de citoyens européens vers les États-Unis et les garanties octroyées aux personnes concernées. Max Schrems, à l'origine

1211. *Idem*, p. 2.

1212. Avistem Avocats, *Transferts des données à caractère personnel de l'Union européenne vers les USA, État des lieux*, in : Avistem Avocats (http://www.avistem.com/), Paris 2016, p. « http://www.avistem.com/sites/default/files/20160401_Projet%20d%27article%20Transfert%20de%20donn%C3%A9es%20UE-USA_1.pdf » (10/10/2017).

1213. Voir le site officiel de l'accord Privacy Shield et la liste des entreprises ayant adhéré au bouclier de protection des données, p. « https://www.privacyshield.gov/list » (10/10/2017).

de l'invalidation de l'accord Safe Harbor par la CJUE, a saisi le tribunal irlandais sur cette question (voir paragraphe 140).

Dans son jugement du 3 octobre 2017 [1214], le tribunal irlandais indique son intention de saisir la CJUE lorsque les parties auront déterminé quelles questions devront être soumises à la CJUE. Le tribunal souligne le caractère fondamental de la problématique, tant du point de vue des droits fondamentaux que des enjeux économiques et sécuritaires [1215]. 1490

Le tribunal considère en outre que le Privacy Shield et la création d'un Ombudsman [1216] ne permettent pas aux citoyens européens d'obtenir une protection efficace [1217]. 1491

La procédure de Max Schrems donnera lieu à un jugement de la CJUE. Le 9 juillet 2019, la CJUE a auditionné les parties prenantes de l'arrêt Schrems 2.0. Elle a rendu un avis sur la validité de deux mécanismes de transfert transfrontalier de données au mois de décembre 2019 : les clauses standards contractuelles et l'accord EU-US Privacy Shield. 1492

Cet avis rendu par la CJUE représente des enjeux importants. En effet, une invalidation éventuelle des clauses standards contractuelles et de l'accord Privacy Shield ôterait des mécanismes juridiques aux entreprises effectuant des transferts de données personnelles entre l'UE et les États-Unis. Il en résulterait une grande insécurité juridique. Dans le même temps, une invalidation offrirait l'opportunité 1493

1214. Arrêt CJUE du 3 octobre 2017, *Data Protection Commissioner v Facebook Ireland Limited*, n° 2016/480, consid. 335.

1215. "The case raises issues of very major, indeed fundamental, concern to millions of people within the European Union and beyond. Firstly, it is relevant to the data protection rights of millions of residents of the European Union. Secondly, it has implications for billions of euros worth of trade between the EU and the US and, potentially, the EU and other non-EU countries. It also has potentially extremely significant implications for the safety and security of residents within the European Union. There is considerable interest in the outcome of these proceedings by any parties having a very real interest in the issues at stake. [p. 3]".

1216. Pour une définition, voir Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 764.

1217. "In my opinion, despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by its intelligence agencies. On the contrary, the individual remedies are few and far between and certainly not complete or comprehensive. [p. 118]"

de renforcer les garanties octroyées aux personnes concernées par un transfert de données personnelles entre l'UE et les États-Unis.

1494 L'avocat général Saugmandsgaard a rendu son opinion en décembre 2019. Il n'a pas invalidé la décision 2010/87/EU relative aux clauses contractuelles types dans le cadre du transfert de données personnelles vers des responsables du traitement établis dans des pays tiers.

1495 L'avocat général reconnaît « l'existence d'une obligation - imposée aux responsables du traitement des données et, en cas d'inaction de ces derniers, aux autorités de contrôle - de suspendre ou d'interdire un transfert lorsque, en raison d'un conflit entre les obligations découlant des clauses types et celles imposées par le droit du pays tiers de destination, ces clauses ne peuvent être respectées [1218] ».

1496 Il a en revanche émis des doutes sur la validité de l'accord Privacy Shield entre l'Union européenne et les Etats-Unis en se fondant sur les articles 45 RGPD, art. 7, 8 and 47 Charte des droits fondamentaux de l'Union et l'art. 8 CEDH (consid. 308, 342) [1219]. Il a également formulé des réserves sur l'effectivité des voies de recours extrajudiciaires offertes aux personnes dont les données personnelles sont transférées de l'Union vers les États-Unis. Il a constaté l'absence d'une protection juridictionnelle effective du fait des lacunes du système juridique américain dans la protection juridictionnelle des personnes concernées. Celles-ci ne disposeraient pas selon lui de droits pouvant être invoqués en justice. Il s'interroge aussi sur les garanties de procédures effectives offertes aux personnes concernées. Il indique en particulier que « les moyens d'action sont limités et les réclamations introduites seront déclarées irrecevables lorsque les personnes concernées ne peuvent démontrer leur qualité pour agir, ce qui restreint l'accès aux juridictions ordinaires ».

1497 Selon la Cour de justice, « une règlementation qui ne prévoirait aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecterait pas le contenu essentiel du droit fondamental consacré à l'article 47 de la Charte des droits fondamentaux de l'Union ».

1218. Saugmandsgaard, *Conclusions de l'avocat général dans l'affaire C-311/18 Facebook Ireland et Schrems*, pp. 1-3.

1219. Opinion CEDH du 19 décembre 2019, *Facebook Ireland et Schrems*, C-311/18, ECLI :EU :C :2019 :1145.

La personne concernée doit en outre pouvoir obtenir des autorités publiques « la confirmation du fait qu'elles traitent ou non des données à caractère personnel la concernant ».

L'avocat a également retenu que l'accord Privacy-Shield ne mentionne « aucune exigence d'informer les personnes concernées du fait qu'elles ont fait l'objet d'une mesure de surveillance ». Cette absence de notification a pour conséquence d'empêcher l'exercice effectif des voies de recours juridictionnelles. Pour l'avocat général, cette situation est contraire à la jurisprudence de la Cour de justice de l'UE et nous partageons cet avis. 1498

L'avocat général relève également le manque d'indépendance du médiateur imposé qui est « désigné par le secrétaire d'État américain et fait partie intégrante du département d'État des États-Unis ». La condition de l'indépendance du médiateur imposée à l'art. 47 de la Charte des droits fondamentaux de l'UE n'est donc pas remplie. L'avocat général relève avec justesse qu'aucune garanties particulières n'est prévue en cas de révocation du médiateur ou l'annulation de sa nomination et que les décisions du médiateur devraient en outre faire l'objet d'un contrôle juridictionnel indépendant. 1499

Cette opinion de l'avocat général de la Cour de justice tend á concrétiser l'équivalence substantielle entre la protection juridictionnelle offerte dans l'ordre juridique des États-Unis aux personnes dont les données y sont transférées depuis l'Union et celle qui découle du RGPD lu à la lumière de l'article 47 de la Charte et de l'article 8 CEDH. 1500

Cette opinion va dans le sens de celle du groupe de travail du CEPD qui a publié un avis en date du 22 janvier 2019 sur l'accord Privacy Shield [1220]. 1501

Une invalidation de l'accord Privacy Shield entre l'UE et les États-Unis aurait eu pour conséquences une invalidation de l'accord Privacy Shield entre la Suisse et les États-Unis et aurait ouvert une période de nouvelles négociations. La force de l'argumentation de l'avocat général incite à la préparation de nouvelles négociations, en prévisin d'une ouverture prochaine des négotiations. Il n'est en effet désormais pas exclu que l'invalidation de l'accord Privacy Shield soit formellement reconnue par la Cour de Justice dans les 1502

1220. EDPB, *EU - U.S. Privacy Shield : Second Annual Joint Review report*, pp. 1-29.

prochains mois.

IV. Les transferts fondés sur la base de garanties appropriées (art. 46 RGPD)

1503 En l'absence d'une décision d'adéquation, le Règlement autorise le responsable du traitement ou le sous-traitant à transférer des données à caractère personnel, de manière licite, s'il offre des garanties appropriées préalables au transfert de données. La doctrine considère qu'il s'agit d'une nouvelle base légale pour les transferts transfrontaliers [1221].

1504 Deux conditions doivent être remplies :

— des garanties appropriées existent, et

— les personnes concernées disposent de droits opposables et de voies de droit effectives [1222].

1505 Cette dernière condition est au coeur des enjeux de l'arrêt Schrems [1223] qui vise la protection des données personnelles des résidents européens dont les données sont transférées aux États-Unis. Le Règlement pose l'obligation pour les États effectuant des transferts transfrontaliers de mettre en place des voies de recours effectives. Cela signifie que la personne concernée puisse effectivement exercer ses droits et s'opposer au transfert de ses données vers les États-Unis. La personne concernée doit pouvoir faire valoir ses droits devant les tribunaux ou les autorités de contrôle nationales [1224]. En cela, le jugement du tribunal irlandais du 3 octobre 2017 [1225] revêt un caractère essentiel. Ce jugement reconnaît que le droit américain n'offre pas de voie de droit effective à chaque individu dans le cas d'une violation de sa sphère privée par des agences de renseignement américaines, mais au contraire, que ces voies de droit sont peu nombreuses, incomplètes et non exhaustives [1226]. Le tribunal rap-

1221. Sydow Gernot (édit.), *Europäische Datenschutzgrundverordnung : Handkommentar*, 2e éd., Baden-Baden 2018, p. 890.

1222. art. 46, al. 1 RGPD.

1223. Arrêt CJUE du 6 octobre 2015, *Schrems*, C-362/14, op.cit.

1224. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 772.

1225. Arrêt CJUE du 3 octobre 2017, *Data Protection Commissioner v Facebook Ireland Limited*, No. 2016/4809 P., précité.

1226. "In my opinion, despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by its intelligence agencies. On the contrary, the individual remedies are few and far between and certainly not complete or comprehensive. [consid. 234, p. 118]"

pelle que des garanties doivent être offertes en cas de surveillance excessive ou inappropriée (consid. 40 et 227).

Le rapport Gorski indique que chaque communication internationale entre un individu basé aux États-Unis et une personne non américaine peut être soumise à une surveillance potentielle (consid. 18 du rapport Gorski). 1506

En imposant des voies de recours effectives et des droits opposables, le Règlement européen impose un standard de qualité pour les transferts de données à caractère personnel entre l'UE et les États-Unis. L'opinion de l'avocat général du 19 décembre 2019 est déterminante pour les relations économiques et diplomatiques entre l'UE et les États-Unis. S' il n'a pas invalidé l'accord Privacy Shield, il émet de doutes quant à sa validité sur le fondement des art. 45 RGPD, art. 7, 8 and 47 CFREU and art. 8 ECHR (consid. 308, 342) [1227]. 1507

Si le Règlement ne pose aucune exigence quant au contenu des garanties appropriées, à l'article 46, al. 1 du Règlement [1228], la Convention 108 modernisée indique cependant que « ces garanties doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination ». « L'autorité de contrôle peut exiger de la personne qui transfère les données qu'elle démontre l'effectivité des garanties prises ou l'existence d' intérêts légitimes prépondérants ». 1508

Quant au protocole additionnel de la Conv. 108, il considère que « des garanties peuvent résulter de clauses contractuelles ». Il s'agit donc de règles « inter partes [1229]». Elles sont « fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne ». Cela signifie que les autorités compétentes peuvent considérer que ces garanties n'offrent pas une protection adéquate pour les droits et libertés des personnes concernées. 1509

A ce jour, constituent des garanties appropriées, selon le Règlement, les règles d'entreprises contraignantes et les clauses contrac- 1510

1227. Opinion CJUE du 19 décembre 2019, *Facebook Ireland and Schrems*, Aff. C-311/18, ECLI :EU :C :2019 :1145, consid. 74.
1228. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 770.
1229. *Idem*, p. 771.

tuelles [1230].

A. Les règles d'entreprises contraignantes ou Binding Corporate Rules (ci-après « BCR »)

1511 Le Règlement reconnaît expressément la validité des transferts transfrontaliers de données à caractère personnel sur le fondement de règles d'entreprises contraignantes ou BCR [1231].

1512 Les BCR ont été créés par le groupe de travail de l'Article 29 de la Commission européenne le 19 avril 2013 [1232].

1513 Les BCR sont des « règles internes relatives à la protection des données qu'un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique conjointe [1233]». Les BCR ont une valeur contraignante pour toutes les sociétés du groupe [1234]. Les autorités de contrôle assurent la conformité à cet engagement.

1514 Les autorités de contrôle jouent un rôle central, car elles autorisent les BCR. L'approbation des BCR rend ainsi licites les flux transfrontaliers de données personnelles en-dehors de l'UE.

1515 Tant les responsables du traitement que les sous-traitants peuvent bénéficier des BCR. Lorsque des BCR sont spécifiques aux sous-traitants, l'autorité de contrôle doit autoriser les flux transfrontaliers de données à caractère personnel vers le sous-traitant bénéficiaire, préalablement au transfert.

1516 L'autorité de contrôle compétente est celle, sur le territoire duquel

1230. Consid. 108 RGPD.
1231. Docquir, *Vers un droit européen de la protection des données ?*, p. 75 ; et art. 63 RGPD.
1232. Article 29 Data Protection Working Party, *Explanatory Document on the Processor Binding Corporate Rules - Adopted on 19 April 2013 (WP 204)*, in : European Commission (https ://ec.europa.eu/), Brussels 2013, p. « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf » (31/03/2020), pp. 1-20.
1233. art. 4, al. 20 RGPD.
1234. art. 40, al. 3 RGPD.

se situe le siège de la société dans l'Union européenne [1235]. En application du Règlement, les BCR doivent être approuvés par l'autorité de contrôle compétente, en vertu du nouveau mécanisme de contrôle de la cohérence (voir paragraphe 1707), après avis du contrôleur européen de la protection des données.

D'une manière similaire à l'arrêt Schrems, le Règlement soulève la problématique des garanties appropriées offertes aux personnes concernées lors de l'utilisation des BCR. Le considérant 110 dispose en effet qu'un « groupe d'entreprises ou un groupe d'entreprises engagées dans une activité économique conjointe devrait pouvoir recourir à des règles d'entreprises contraignantes approuvées pour ses transferts internationaux, vers des entités du même groupe d'entreprises, si les règles incluent tous les principes essentiels et les droits opposables aux individus pour assurer des garanties appropriées pour les transferts [...] de données à cadre personnel ». 1517

Comme ces règles doivent être approuvés par l'autorité de contrôle compétente, préalablement au transfert de données à caractère personnel hors de l'union européenne, l'autorité de contrôle joue un rôle central dans l'évaluation des garanties offertes aux personnes concernées dans les BCR. La protection des droits et libertés des personnes concernées dépend donc de la qualité de l'évaluation effectuée par l'autorité de contrôle. L'indépendance effective des autorités de contrôle et leurs ressources (humaines et financières) sont des éléments essentiels. 1518

B. Les clauses contractuelles

A la suite de l'invalidation de l'arrêt Safe Harbor par la CJUE [1236], les entreprises américaines traitant et transférant des données à caractère personnel de résidents européens vers des serveurs américains ont eu recours à des clauses contractuelles. Celles-ci rendent licites les transferts de données personnelles de l'UE vers les Etats-Unis. Les clauses types sont devenues un mécanisme de transfert « par 1519

1235. Groupe de Travail de l'Article 29, *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant - Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017 (WP 244 rev.01)*, in : CNIL (https ://www.cnil.fr/), Paris 2016, p. « https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf » (31/03/2020).

1236. op.cit., Arrêt *Schrems*, consid. 106.

défaut » pour légitimer les transferts de données vers les États-Unis. Comme nous l'avons vu précédemment, la validité de ces clauses est la source d'un contentieux dans le cadre de l'affaire Schrems. L'avocat général de la CJUE a reconnu la validité de ces clauses contractuelles types dans une opinion du mois de décembre 2019 (voir paragraphe 1502).

1520 La Commission européenne a reconnu la validité de l'utilisation de ces clauses contractuelles dans trois décisions : 2001/497/CE, 2004/915/CE, 2010/87/UE [1237].

1521 Les clauses contractuelles prévues dans le Règlement peuvent être de plusieurs types :

- les clauses contractuelles types adoptées par la Commission,
- les clauses contractuelles types adoptées par une autorité de contrôle, et approuvées par la Commission, et
- les clauses contractuelles ad hoc.

C. Les clauses types de protection des données adoptées par la Commission.

1522 Le Règlement s'inspire en cela de la directive 95/46/CE [1238].

1523 Les clauses types sont de *trois* sortes :

1237. Commission européenne, *Décision 2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (notifiée sous le numéro C(2001) 1539)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2001, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32001D0497 » (31/03/2020), pp. 19-31 ; Commission européenne, *Décision 2004/915/CE du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers (notifiée sous le numéro C(2004) 5271)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2004, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32004D0915 » (31/03/2020), pp. 74-84 ; Commission européenne, *Décision 2010/87/UE du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (notifiée sous le numéro C(2010) 593)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2010, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32010D0087 » (31/03/2020), pp. 5-18.

1238. Docquir, *Vers un droit européen de la protection des données ?*, p. 78.

— *deux* pour les transferts de responsable du traitement à responsable du traitement.

— *une* pour les transferts de responsable du traitement à sous-traitant.

(a) Les clauses contractuelles types approuvées par la Commission.

Tout comme les décisions d'adéquation, les clauses contractuelles types, adoptées par la Commission, demeurent valables, tant que la Commission européenne ne modifie, ne remplace ou n'abroge pas ces clauses types [1239]. Seule la Commission européenne a compétence pour modifier ces clauses contractuelles. Cela signifie que ni les autorités de contrôle ni les partenaires commerciaux ne peuvent modifier des clauses types. 1524

Le Règlement autorise le transfert de données sur la base des clauses types approuvées par la Commission, sans que l'entreprise n'ait besoin de faire approuver ces clauses par l'autorité de contrôle. Toute obligation d'approbation préalable par une autorité de contrôle nationale est supprimée par le Règlement [1240]. 1525

(b) Les clauses types adoptées par une autorité de contrôle et approuvées par la Commission

Une autorité de contrôle a le pouvoir d'adopter certaines clauses types afin de légitimer un transfert de données vers des pays tiers, après approbation de la Commission européenne [1241]. 1526

Le transfert de données à caractère personnel peut également se fonder sur des clauses ad hoc, qui varient à chaque transfert [1242]. Ces clauses ne sont pas standardisées. Elles sont cependant reconnues par le Règlement et doivent être adoptées par l'autorité de contrôle. Il s'agit d'une innovation du Règlement, car ces clauses ad hoc ne bénéficiaient d'aucune reconnaissance sous la directive 95/46/CE [1243]. 1527

1239. art. 46, al. 5 RGPD.
1240. art. 46, al. 2 RGPD.
1241. art. 46, al. 2, d) RGPD.
1242. art. 46, al. 3, a) RGPD.
1243. Docquir, *Vers un droit européen de la protection des données ?*, p. 79.

D. Les codes de conduite et mécanismes de certification

1528 Les codes de conduite et les mécanismes de certification constituent deux nouveaux modes de légitimation des transferts [1244].

1529 Les codes de conduite sont élaborés par l'industrie, approuvés par l'autorité de contrôle nationale et doivent être reconnus comme valides par la Commission européenne. Les codes de conduite sont assortis de l'engagement contraignant et exécutoire du responsable du traitement ou du sous-traitant d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées. En principe, si le traitement de données a des effets sur plusieurs États membres, une procédure d'approbation préalable est requise de la part de l'autorité de contrôle.

1530 Le mécanisme de certification démontre que des garanties appropriées sont offertes aux personnes concernées dans le cadre de transferts de données à caractère personnel vers des pays non adéquats ou vers une organisation internationale. La certification est délivrée par des organismes de certification ou par une autorité de contrôle, pour une durée de trois ans renouvelables.

1531 En l'absence d'une décision d'adéquation ou de garanties appropriées, les transferts de données vers des pays non adéquats ne sont pas autorisés sauf dans le cas d'une dérogation prévue expressément par le Règlement [1245].

1532 Tiennent lieu de dérogations valables les cas suivants :

- La personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert peut comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées.
- Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée.
- Le transfert est nécessaire pour des motifs importants d'intérêt public.

1244. art. 46, al. 2, e) et f) RGPD.
1245. art. 49, al. 1 RGPD.

- Le transfert est important à la constatation, à l'exercice ou à la défense de droits en justice.
- Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne, lorsque la personne se trouve dans l'incapacité de donner son consentement.
- Le transfert a lieu au départ d'un registre, qui conformément au droit de l'UE ou au droit d'un État membre, est destiné à fournir des informations au public, et est ouvert à la consultation du public, en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues par la consultation, dans le droit de l'UE ou le droit de l'État membre, sont remplies dans le cas d'espèce.
- Le responsable du traitement poursuit des intérêts légitimes impérieux.

En l'absence de décision d'adéquation, en l'absence de garantie appropriée et de consentement explicite de la personne concernée, les entreprises doivent démontrer l'existence d'intérêts légitimes impérieux justifiant le transfert de données vers des pays tiers non adéquats. Cette notion n'étant pas définie dans le Règlement, une clarification de la part des autorités de contrôle et de la jurisprudence renforcerait la sécurité juridique des entreprises sur ce thème. 1533

Chapitre 3: Le rôle accru des autorités de contrôle

En comparaison internationale, le droit européen offre un cadre juridique très protecteur dans le domaine de la protection des données. 1534

Tant l'article 16 du Traité sur le fonctionnement de l'UE (ci-après « TFUE »), que l'article 8 de la Charte des droits fondamentaux de l'UE reconnaîssent que « toute personne a droit à la protection des données le concernant ». 1535

En application du protocole additionnel de la Convention 108 relatif aux autorités de contrôle et aux flux transfrontaliers de données, les États parties doivent instaurer des autorités de contrôle, qui exercent leurs fonctions en toute indépendance [1246]. Lors de l'évaluation de la mise en oeuvre des accords Schengen, le Conseil de l'UE a relevé des manquements concernant l'indépendance des autorités de contrôle en Suisse [1247]. Ces autorités s'assurent de l'application effective de la Convention 108 et du protocole additionnel (art. 1, al. 1 Protocole) [1248]. 1536

Il est de la responsabilité de chaque État membre de l'UE ou partie à la Convention 108 de s'assurer qu'une autorité de contrôle indépendante veille à l'application des règles de droit en matière de protection des données sur son territoire national. 1537

En tant que garantes du respect effectif du droit fondamental à la protection des données personnelles, ces autorités doivent bénéficier des pouvoirs et des ressources nécessaires à la mise en œuvre effective de leur mandat. La doctrine souligne en particulier l'im- 1538

1246. art. 1, al. 3 Protocole additionnel et Epiney Astrid / Hänni Julia / Brülisauer Flavia (édit.), *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, Zürich 2012, p. 71.

1247. Conseil de l'UE, *Recommandations sur la protection des données du 8 mars 2019*, in : Dossier interinstitutionnel : 2019/0024(NLE) - SCH-EVAL 50, DATAPROTECT 84, COMIX 148, Bruxelles 2019, p. 4.

1248. Applicables à la Suisse du fait de l'Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, du 26 octobre 2004, RS 0.362.31.

portance pour ces autorités de disposer du « droit de mener des enquêtes, du droit de lancer des poursuites, du droit d'intervenir, et du pouvoir de porter toute violation à la connaissance de l'autorité judiciaire [1249] ».

1539 Si le Règlement européen uniformise le droit de la protection des données personnelles, il supprime la déclaration préalable de l'autorité de contrôle, au profit d'un contrôle *a posteriori*. En cas d'investigation, l'autorité de contrôle analysera la documentation du responsable du traitement, en particulier l'analyse d'impact. Le Règlement européen consacre ainsi une logique du contrôle *a posteriori* de la conformité du responsable du traitement dans le domaine de la protection des données, d'une manière analogue au domaine bancaire. Le législateur européen a cependant renoncé à attribuer aux autorités de contrôle le pouvoir d'autoriser ou d'interdire les traitements de données personnelles préalablement aux traitements. Cette décision trouve son fondement dans une logique de rationalité économique et de responsabilisation des acteurs, sur le modèle anglo-saxon. Selon nous, il faut comprendre qu'avec le Règlement, le mécanisme de contrôle *a posteriori* par les autorités de contrôle joue un rôle accru. Le Règlement souligne également l'importance de la notion de Private Enforcement qui est à disposition dans l'action en responsabilité du responsable du traitement ou du sous-traitant, et requiert la mise en oœuvre d'un recours juridictionnel effectif.

1540 Christina Koumpli soutient que cette nouvelle perspective crée un risque de pré-légitimation des traitements qui peut-être favorable au responsable du traitement [1250]. Relevons que cette remarque part de l'idée que le contrôle *a posteriori* n'est fait que par les autorités de contrôle, sans considération de l'action civile. Cette approche démontre combien l'action civile effective en responsabilité est nécessaire, afin de rétablir un équilibre dans les rapports de force entre

1249. Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, p. 15.

1250. Koumpli Christina, *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données personnelles - Etude comparée : Union Européenne, Allemagne, France, Grèce, Royaume-Uni*, thèse, Paris 2019, pp. 1-645.

les acteurs économiques et les personnes concernées.

Dans sa thèse, Christina Koumpli questionne la conformité d'une telle perspective avec le droit fondamental à la protection des données personnelles. « La conception préventive fait partie de l'histoire de la protection européenne des données et peut donner un sens à la protection et à son seul bénéficiaire, l'individu. Un tel sens serait d'ailleurs conforme aux Constitutions nationales qui offrent des garanties à l'individu [1251]». Elle oublie l'importance du Private Enforcement Selon nous, elle oublie l'importance du principe de Private Enforcement et notamment de la *class action* et du renversement de la charge de la preuve dans le mécanisme de protection des personnes physiques mis en place par le Règlement. En effet, la mise en oœuvre du droit de la protection des données dépend en partie de l'action en responsabilité contre le responsable du traitement et le sous-traitant en vertu du Règlement, qui exige que les États mettent à la disposition des personnes physiques un recours juridictionnel effectif et un mécanisme de *class action*. 1541

Cependant, ce principe de pré-légitimation des traitements est-il compatible avec l'art. 8 de la Charte des droits fondamentaux de l'UE ? Celui-ci stipule que « ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ». 1542

Cet article impose ainsi au responsable du traitement une obligation de loyauté, dont le respect est vérifié par l'autorité indépendante. 1543

La reconnaissance du principe de pré-légitimation des traitements de données personnelles peut s'expliquer par l'obligation pour le responsable du traitement de respecter certains principes fondamentaux comme le principe de loyauté, de limitation des finalités et de licéité. 1544

Dans le domaine de la recherche, la loyauté du chercheur est vérifiée eu égard au respect de « règles déontologiques et sa pratique est interrogée par des questions éthiques (responsabilité, confiance) [1252]. 1545

1251. Koumpli, *Les données personnelles sensibles*, p. 2.

1252. Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*,

Il a une obligation de moyens et sa responsabilité est engagée quant à l'efficacité de son travail, sa pertinence, qualité, validité ou au moins l'honnêteté, la loyauté, des résultats qu'il publie, et encore sa capacité à rendre compte de leur utilité [1253]».

1546 Il en est a fortiori de même pour le responsable du traitement professionnel qui est soumis à une obligation de diligence (duty of care). L'autorité de contrôle remplit ainsi le rôle de protecteur du droit fondamental à la protection des données, même si en dernier ressort, il revient à la CJUE de dégager le contenu essentiel de ce droit.

1547 Si les autorités de contrôle de l'UE doivent veiller à la mise en œuvre effective de l'art. 8 Charte des droits fondamentaux de l'UE, elles doivent également s'assurer du respect des libertés et droits fondamentaux spécifiés à l'article 7 de la Charte des droits fondamentaux, ainsi que le droit à la liberté d'expression ou le droit à la protection de la propriété [1254].

1548 Compte tenu du caractère essentiel de ces droits pour le respect des principes et valeurs démocratiques, il est pertinent d'examiner le mandat et les prérogatives des autorités de contrôle dans l'UE en application du Règlement européen.

§1 Le mandat des autorités de contrôle

1549 Si la directive 95/45/CE accordait déjà une place aux autorités de contrôle [1255], celle-ci était très limitée. Un unique article composé de 7 alinéas résumait le mandat de ces autorités. Le Règlement européen consacre quant à lui deux sections et huit articles aux autorités de contrôle, à leurs prérogatives, à leur indépendance et aux mécanismes de coopération entre autorités.

1550 La place prépondérante accordée aux autorités de contrôle dans le Règlement reflète la volonté politique de la Commission euro-

pp. 1-29.

1253. Besse / Castets-Renard / Garivier, *Loyauté des Décisions Algorithmiques*, p. 7.

1254. Simitis Spiros (édit.), *Bundesdatenschutzgesetz : Kommentar*, 8e éd., Baden-Baden 2014, p. 5, art. 1, al. 3. RGPD.

1255. art. 28 de la directive 95/46/CE.

péenne de renforcer le rôle des autorités de contrôle dans l'UE [1256].

Cette volonté politique de la Commission européenne présente un caractère novateur. Contrairement au Règlement européen, la Conv. 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel ne prévoit pas d'obligation de créer une autorité indépendante. Une telle obligation figure uniquement dans le protocole additionnel à la Conv. 108. L'article 12bis de la version consolidée de la Conv. 108 modernisée exige des États parties à la Convention de créer une autorité indépendante pour surveiller la mise en œuvre effective des principes qu'elle édicte. La volonté politique de tous les États européens se manifeste en faveur d'un contrôle accru du respect des normes en matière de protection des données. 1551

§2 Les missions des autorités de contrôle

Les missions des autorités de contrôle sont présentées essentiellement à l'article 51, al. 1 du Règlement européen [1257]. Les articles 52 et 54 et les considérants 117 à 119 du Règlement complètent cet article [1258]. 1552

Ainsi « chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application [du Règlement], afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement automatisé et de faciliter le libre flux des données à caractère personnel au sein de l'Union » (art. 51 RGPD). 1553

L'autorité de contrôle a donc la double mission de protéger les libertés et les droits fondamentaux des personnes privées et de faciliter la libre circulation des données à caractère personnel au sein de l'Union [1259]. 1554

L'autorité de contrôle doit effectuer une pesée des intérêts en présence entre les intérêts de la personne privée et ceux du responsable 1555

1256. Commission européenne, *« Une approche globale de la protection des données à caractère personnel dans l'UE »*.
1257. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 827.
1258. *Idem*, p. 828.
1259. *Idem*, p. 830.

du traitement [1260].

1556 Afin que cette pesée des intérêts en présence soit empreinte de neutralité, il est essentiel que la procédure de nomination ou d'élection de l'autorité de contrôle limite la politisation de la fonction [1261]. Pour Jean-Philippe Walter, membre du Conseil de l'Europe et ancien Préposé suppléant à la protection des données, une nomination par le gouvernement avec confirmation par le pouvoir législatif apparaît opportune, de même qu'une durée de 4 ans renouvelables.

1557 Chaque État adapte le nombre de ses autorités de contrôle, en fonction de la structure de son État. Un État fédéral comme l'Allemagne désigne des autorités de contrôle aux compétences territoriales ou matérielles distinctes [1262]. En plus de l'autorité de contrôle fédérale, plusieurs autorités de contrôle ont été créées dans chaque canton. En-dehors de l'UE, la Suisse a adopté un modèle similaire.

1558 Il est essentiel de noter que chaque autorité de contrôle a vocation à appliquer le Règlement « dans l'ensemble de l'Union ». Ainsi elles échangent des informations entre elles et avec la Commission européenne (art. 51 al. 2 RGPD.).

1559 L'obligation faite aux autorités de contrôle de « contribuer à l'application cohérente du Règlement [1263]», donne la mission aux autorités de contrôle d'harmoniser l'application du Règlement européen. La coopération entre autorités de contrôle s'inscrit dans cet objectif et prend dès lors tout son sens.

1560 Cet effort de convergence dans l'application effective du Règlement est également soutenu par le Comité européen de la protection des données et la conférence annuelle des commissaires à la protection

1260. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 830.
1261. Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, p. 73.
1262. art. 51, al. 1 RGPD : « une ou plusieurs autorités ».
1263. art. 51, al. 2 RGPD.

des données et à la vie privée [1264].

Reconnaissant le rôle fondamental des réunions informelles du groupe de travail de l'article 29 [1265], le Règlement européen formalise cette coopération par le biais d'une procédure obligatoire et de mesures communes aux autorités de contrôle de l'UE [1266]. Cette coopération étroite se traduit pour la doctrine par une obligation de coopération et d'assistance mutuelle [1267]. 1561

Le Règlement introduit une coopération institutionnalisée, qui se justifie par le caractère international des traitements de données personnelles [1268] et par le besoin d'échanger des informations et des expériences entre autorités afin de faciliter l'harmonisation de la protection des données dans l'union. L'article 51, al. 4 pose les bases de cette coopération puisque chaque État doit « notifier à la Commission les dispositions légales qu'il adopte en vertu du présent chapitre, au plus tard, le 25 mai 2018 et, sans tarder, toute modification ultérieure les affectant ». 1562

La coopération entre autorités de contrôle peut prendre plusieurs formes : « One-Stop-Shop » (art. 60 du Règlement), entraide administrative (art. 61 du Règlement), mesures communes des autorités de contrôle (art. 62 du Règlement) ou encore le mécanisme de contrôle de la cohérence (art. 63 du Règlement). Le considérant 119 précise que « des garanties d'efficacité de la coopération entre autorités de contrôle et du mécanisme de la cohérence doivent être apportées. Ceci est primordial pour la procédure de coopération entre autorités » (« One-Stop-Shop »). 1563

1264. 40TH International Conference of Data Protection and Privacy Commissioners (ICDPPC), *Debating Ethics : dignity and respect in data-driven life*, in : ICDPPC (https://www.privacyconference2018.org), Brussels 2018, p. « https://www.privacyconference2018.org » (27/05/2019).

1265. Désigné comme le Comité européen à la protection des données depuis le 25 mai 2018.

1266. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 831.

1267. *Idem*, p. 614.

1268. Docquir Benjamin, *Droit du numérique : contrats, innovation, données et sécurité*, 1e éd., Bruxelles 2018, p. 23.

I. L'indépendance des autorités de contrôle

A. La jurisprudence du Tribunal fédéral

1564 Le Tribunal fédéral s'est prononcé en 2013, sur la notion d'indépendance du Préposé en analysant spécifiquement le budget alloué à ce dernier.

1565 Dans le cas d'espèce, le Grand Conseil du canton de Genève avait réduit de CHF 300 000 le budget alloué en 2012 au Préposé cantonal à la protection des données et à la transparence, ce qui a donné lieu à la suppression de deux postes de collaborateurs [1269].

1566 La Chambre administrative de la Cour de justice a été saisie d'un recours pour déni de justice par la Préposée et a déclaré le recours irrecevable.

1567 Le Tribunal fédéral a rejeté le recours en matière de droit public interjeté par la Préposée. Le Tribunal fédéral a confirmé que le budget n'était pas un acte susceptible de recours.

1568 La doctrine a soutenu avec raison que si les bases légales imposant l'indépendance du Préposé existent, une mesure budgétaire peut les vider de leur substance [1270]. Bertil Cottier a souligné avec justesse que l'absence d'une pleine autonomie budgétaire constituait un obstacle à une indépendance réelle de l'autorité de contrôle [1271].

1569 En outre, Alexandre Flückiger note que lorsque le Tribunal fédéral juge qu'une réduction budgétaire n'est en rien comparable avec une modification législative, il faut comprendre qu'une réduction de budget devient comparable à une modification législative si elle devait remettre en cause l'existence même du Préposé ou restreindre ses compétences d'une manière qui apparaîtrait contraire au droit

1269. Tribunal fédéral, Arrêt 1C_359/2013 du 14 novembre 2013 ; Flückiger Alexandre, *Jurisprudence actuelle en matière de protection des données*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015, p. 158.

1270. Flückiger, *Jurisprudence actuelle en matière de protection des données*, p. 158.

1271. Arrêt CourEDH du 30 novembre 2004, *oneryildiz c. Turquie*, requête n° 48939/99, par. 90 et 104 ss, CE :ECHR :2004 :1130JUD004893999 ; Arrêt CEDH du 10 janvier 2012, *Di Sarno et autres c. Italie*, requête n° 30765/08, par. 110 ss, CE :ECHR :2012 :0110JUD003076508 ; Arrêt CourEDH du 27 janvier 2009, *Tatar c. Roumanie*, requête n° 67021/01, par. 88 et 97ss, CE :ECHR :2009 :0127JUD006702101.

supérieur [1272].

Cette jurisprudence apparaît en contradiction avec le contenu du rapport explicatif du Protocole additionnel à la Convention 108 qui exige d'instaurer des autorités de contrôle qui « exercent leurs fonctions en toute indépendance » (art. 1, al. 3). Selon ce rapport, « l'octroi à l'autorité de ressources suffisantes » fait partie d'un faisceau d'indices qui contribue au respect de cette indépendance [1273]. 1570

Cette jurisprudence apparaît aussi en contradiction avec la jurisprudence de la CourEDH qui exige en outre que les obligations positives sont des obligations de mise en œuvre (duty to fulfil) et ne se limitent pas à l'obligation de protéger [1274]. Des mesures de mise en œuvre efficaces doivent être prises par les États [1275]. Par conséquent, le refus de mettre en œuvre le financement adéquat pourrait constituer une inexécution d'une obligation positive. 1571

En matière budgétaire, le Règlement européen prévoit que l'autorité dispose d'un « budget annuel public propre » même si le budget peut faire partie « du budget global national ou d'une entité fédérée [1276]». L'autorité peut donc planifier, allouer et gérer ses dépenses en toute indépendance [1277]. Le Règlement européen impose aux États membres de « veiller à ce que chaque autorité de contrôle soit soumise à un contrôle financier ». 1572

L'évaluation des politiques publiques constitue également un moyen non juridictionnel de demander d'allouer des ressources financières au futur Préposé cantonal à la protection des données et à la transparence [1278]. 1573

1272. Flückiger, *Jurisprudence actuelle en matière de protection des données*, p. 161.
1273. Conseil fédéral, *Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données - Conclu à Strasbourg le 8 novembre 2001 (RS 0.235.11, RO 2008 731)*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2001, p. « https://www.admin.ch/opc/fr/classified-compilation/20022762/index.html » (01/04/2020), art. 1, al. 3.
1274. Flückiger, *Jurisprudence actuelle en matière de protection des données*, p. 160.
1275. Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, p. 44.
1276. art. 52, al. 6 RGPD.
1277. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 877.
1278. Flückiger, *Jurisprudence actuelle en matière de protection des données*,

B. La jurisprudence de la CJUE

1574 La CJUE est venue préciser la notion et les critères d'indépendance des autorités de contrôle à travers plusieurs décisions de principe [1279]. Ainsi, dans son arrêt Commission c. Allemagne [1280], la Cour, a été saisie d'un recours contre l'Allemagne par la Commission européenne, au motif que les autorités de contrôles allemandes ne remplissaient pas la condition de complète indépendance du fait de la tutelle de l'État, pour les activités de contrôle dans les secteurs non publics [1281].

1575 La CJUE jugea que le terme « indépendance » désigne normalement pour les autorités publiques, un statut qui assure à l'organe concerné la possibilité d'agir « en toute liberté » « à l'abri de toute instruction et de toute pression [1282] ». Elle retient que l'adjectif « toute » vient « renforcer la notion d'indépendance et implique un pouvoir décisionnel, soustrait à toute influence extérieure à l'autorité de contrôle », qu'elle soit « directe ou indirecte [1283] ». « La Cour ajouta que la directive 95/46/CE prévoyait que les autorités de contrôle étaient un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel [1284] et qu'elles sont les gardiennes des droits de l'homme et libertés fondamentales [1285]. La Cour conclut que l'article 28, al.1 de la directive devrait être interprété en ce sens que « les autorités doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure. Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés mais aussi toute injonction et toute autre influence extérieur, que cette dernière soit directe ou

p. 162 ; Republique et Canton de Genève, *Le principe de transparence dans l'administration : Évaluation des dispositions légales concernant l'accès aux documents et l'information du public (LIPAD)*, in : Cour des Comptes (http ://www.cdc-ge.ch/), Genève 2009, p. « http : / / www . cdc - ge . ch / fr / Publications/Archives-CEPP/Liste-des-rapports-d-evaluation/Principe-de-transparence - dans - l - administration - LIPAD . html » (01/04/2020), Recommandation R16, consid. 72.

1279. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 837 ; Docquir, *Vers un droit européen de la protection des données ?*, pp. 26-28 ; et voir aussi Arrêt CJUE du 8 avril 2014, *Commission contre Hongrie*, C—288/12, consid. 59.

1280. Arrêt CJUE du 9 mars 2010, C—518/07, consid. 8.

1281. Docquir, *Vers un droit européen de la protection des données ?*, p. 24.

1282. Arrêt CJUE du 9 mars 2010, *Commission européenne c. République fédérale d'Allemagne*, C—518/07, Rec. 2010 p. I-01885, consid. 18.

1283. Arrêt C-518/07, consid. 19 et op.cit., Docquir, p. 25.

1284. Consid. 62 de la directive 95/46/CE.

1285. Arrêt C-518/07, consid. 23.

indirecte, qui pourraient remettre en cause l'accomplissement par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel [1286]».

« Le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci [1287]». Est-ce à dire que la compétence du conseil fédéral pour déterminer le budget du Préposé fédéral en lien et place du Parlement constitue un risque d'une influence politique sur les décisions de cette autorité de contrôle ? 1576

Afin de limiter l'influence extérieure, la qualification professionnelle des membres de l'autorité de contrôle doit être à la fois juridique et technique dans le domaine de la protection des données, des technologies et des systèmes d'information et de communication afin d'assurer l'expertise nécessaire à l'accomplissement de leurs tâches de conseil et de surveillance [1288]. De ce niveau d'expertise découlera l'indépendance effective, le respect, et la crédibilité de l'activité de l'autorité de protection des données [1289]. 1577

La CJUE a précisé dans un second arrêt condamnant l'Autriche [1290], qu'une indépendance fonctionnelle des autorités de contrôle en vertu de laquelle ses membres étaient indépendants et n'étaient liés par aucune instruction dans l'exercice de leurs fonctions« ne suffisait pas à elle seule, à préserver ladite autorité de toute influence externe [1291]». La Cour a conclu à une violation de l'article 28, al. 1, de la directive 95/46/CE, dès lors que la législation de la République d'Autriche prévoyait que « *(i)* le membre administrateur de l'autorité est un fonctionnaire fédéral assujetti à une tutelle de service, *(ii)* le bureau de l'autorité de contrôle est intégré aux services de 1578

1286. Docquir, *Vers un droit européen de la protection des données ?*, p. 25.
1287. Arrêt CJUE du 9 mars 2010, *Commission contre Allemagne*, C—518/07, ECLI :EU :C :2010 :125, consid. 36.
1288. Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, p. 75.
1289. *Ibidem.*
1290. Arrêt CJUE du 16 octobre 2012, *Commission européenne c. République d'Autriche*, C—614/10, ECLI :EU :C :2012 :631, in : JOUE, C-379/6, 8 décembre 2012.
1291. Arrêt C-614/10, consid. 42.

la Chancellerie fédérale, et que *(iii)* le Chancelier fédéral dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de l'autorité de contrôle [1292]».

1579 Pour que l'autorité de contrôle accomplisse ses missions « en toute indépendance », il ne doit exister « aucun soupçon sur son impartialité [1293]».

1580 La troisième jurisprudence concerne l'arrêt Commission c. Hongrie du 8 avril 2014 [1294]. Par sa requête du 24 mai 2012, la Commission européenne a demandé à la CJUE de constater que la Hongrie, en mettant fin de manière anticipée au mandat d'autorité de contrôle de la protection des données, a manqué aux obligations qui lui incombent en vertu de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. À cet égard, la Commission reproche à la Hongrie une violation de l'indépendance de l'autorité de contrôle de la protection des données prescrite par l'article 28, paragraphe 1, second alinéa, de la directive [1295]. La CJUE retient que le manquement serait constitué par la cessation anticipée du mandat du commissaire de l'autorité de contrôle (M. Jóri) et persisterait du fait que M. Jóri n'aurait pas été rétabli dans ses fonctions à l'expiration de ce délai.

1581 La CJUE confirme les deux arrêts précédents et précise « le caractère incontestable du lien intrinsèque entre l'inamovibilité du commissaire jusqu'à l'échéance du mandat et l'exigence de 'toute indépendance ».

1582 La CJUE reconnaît que les États membres disposent d'une marge d'appréciation quant à la structure institutionnelle de l'autorité prescrite par l'article 28, paragraphe 1, second alinéa, de la directive. Cependant, elle vient ajouter qu'il est « incontestable que l'exigence

1292. Arrêt C-614/10, consid. 66 et Docquir, *Vers un droit européen de la protection des données ?*, p. 25.

1293. Arrêt CJUE du 16 octobre 2012, *Commission contre Autriche*, C—614/10, ECLI :EU :C :2012 :631, consid. 61.

1294. Arrêt CJUE du 8 avril 2014, *Commission c. Hongrie*, ECLI :EU :C :2014 :237, in : Recueil de la jurisprudence, 8 avril 2014. p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0288&from=FR » (12/10/2017). Cf également Kühling / Buchner, *Datenschutz - Grundverordnung*, pp. 838-840.

1295. Kuühling / Buchner, *Datenschutz - Grundverordnung*, p. 1 « Introduction ».

de « toute indépendance » imposée par le droit de l'Union postule l'existence et le respect de règles spécifiques et détaillées, qui, en matière de nomination, de durée des fonctions ainsi que de possibles causes de révocation ou de destitution de cette autorité, permettent d'écarter tout doute légitime sur l'imperméabilité de ladite autorité à l'égard de toute influence extérieure, qu'elle soit directe ou indirecte, susceptible d'orienter ses décisions ».

II. Le Règlement et la notion d'indépendance

Le Règlement reprend toutes les garanties d'indépendance telles que précisées par la CJUE dans la jurisprudence évoquée précédemment [1296]. L'article 52 indique que le ou les membres de chaque autorité ne reçoivent ou ne sollicitent aucune instruction et « demeurent libres de toute influence extérieure ». Cette obligation se retrouve dans l'art. 12 bis de la Convention 108 révisée qui précise que les autorités de contrôle ne doivent pas être l'objet ou solliciter d'instructions que ce soit des autorités de nomination ou de toute autre entité. Un membre d'une autorité de contrôle a également l'interdiction d'exercer toute fonction incompatible avec son mandat [1297]. 1583

Il revient aux États membres de préciser les fonctions et les avantages incompatibles avec la nomination en tant que membre d'une autorité de contrôle [1298], afin d'éviter tout conflit d'intérêt pouvant émerger du fait de l'exercice d'une fonction au sein d'une autorité de contrôle. 1584

En application du Règlement européen, le secret professionnel constitue une obligation légale pour les membres de l'autorité de contrôle, et ses agents [1299]. 1585

Il est en outre prévu que « chaque autorité reçoive des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaire à l'exercice effectif de ses missions et de ses pouvoirs [1300] ». Cette disposition démontre la volonté du législateur européen de renforcer le rôle des autorités de contrôle, leur indé- 1586

1296. Docquir, *Vers un droit européen de la protection des données ?*, p. 29.
1297. art. 52, al. 3 RGPD.
1298. art. 54, al. 1, f) RGPD.
1299. art. 54, al. 2 RGPD.
1300. art.52, al. 4 RGPD.

pendance et l'effectivité de leurs missions.

1587 « Chaque autorité doit disposer de ses propres agents [1301]», qui doivent agir « avec intégrité, s'abstenir de tout acte incompatible avec leurs fonctions et n'exercer, pendant la durée de leur mandat, aucune activité professionnelle incompatible, rémunérée ou non [1302]».

1588 La nomination du ou des membres des autorités de contrôle est soumise à des conditions spécifiques [1303] les membres pourront être nommés « soit par le parlement, le gouvernement, le chef d'État ou un organisme indépendant ». Le Règlement prévoit que chaque membre aura les « qualifications, l'expérience, et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de ses fonctions et de ses pouvoirs [1304]». Le choix des agents embauchés par l'autorité de contrôle fait désormais partie intégrante de l'indépendance de l'autorité de contrôle [1305]. Une loi devrait être prise par chaque État membre et garantir une procédure transparente pour la nomination des agents de l'autorité de contrôle [1306].

1589 Ces conditions de nomination ne figurent pas dans la directive 95 /46/CE [1307].

1590 Le Règlement prévoit enfin que « la fonction ne peut prendre fin qu'à l'échéance du mandat prévu [1308]», ce qui est conforme à la jurisprudence de la Cour de Justice de l'UE dans son arrêt Commission c. Hongrie précité. Enfin, une possibilité de révocation de mandat est prévue au cas où un membre commettrait une faute grave ou ne remplirait plus les critères nécessaires à l'exercice de ses fonctions [1309].

1591 « Les États membres doivent établir par une loi le statut des au-

1301. art. 52, al. 5 RGPD.
1302. Consid. 121 RGPD.
1303. art. 53 RGPD ; Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 843.
1304. art. 53, al. 2 RGPD ; Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 844.
1305. Ehmann / Selmayr, *Datenschutz - Grundverordnung*, p. 876.
1306. Consid. 121 RGPD.
1307. Kühling / Buchner, *Datenschutz - Grundverordnung*, p. 843.
1308. art. 53, al. 3 RGPD.
1309. art. 53, al. 4 RGPD.

torités de contrôle [1310]». Il en va de même « des qualifications et conditions d'éligibilité ainsi que des règles et procédures pour être nommé membre de chaque autorité de contrôle, ou encore de la durée du mandat et son caractère ou non renouvelable ».

III. Les pouvoirs de l'autorité de contrôle

Les pouvoirs de l'autorité de contrôle sont mentionnés à l'article 57 du Règlement [1311]. Ils sont constitués d'activités de « contrôle du respect du Règlement », « d'activités de sensibilisation du public » (et notamment concernant les activités destinées spécifiquement aux enfants), « d'activités de conseil auprès des législateurs nationaux et des autres institutions publiques [1312]». L'autorité de contrôle dispose en outre de « pouvoirs d'enquête sur l'application du Règlement [1313]». 1592

Ces attributions sont conformes à l'article 12 bis de la Convention 108 révisée qui reprend l'art. 1 du protocole additionnel. La mission de sensibilisation au droit à la protection des données des enfants et autres personnes vulnérables est particulièrement soulignée. 1593

L'autorité de contrôle doit en outre coopérer avec les autres autorités de contrôle [1314] et contribuer aux activités du Comité européen de la protection des données [1315]. 1594

Dans un État fédéral comme Allemagne ou la Suisse, une collaboration entre les autorités cantonales et fédérales dans le respect de leurs compétences respectives et une uniformisation des tâches et des compétences, apparaissent nécessaires pour rendre la protection des données effective et offrir des garanties d'indépendance [1316]. 1595

L'autorité de contrôle doit également participer à l'élaboration et à l'approbation de codes de conduite [1317], à l'approbation de clauses 1596

1310. art. 54 RGPD.
1311. art. 57 RGPD.
1312. art. 57, al. 1 RGPD.
1313. art. 57, al. 1, h) RGPD.
1314. art. 57, al. 1, g) RGPD.
1315. art. 57, al. 1, f) RGPD.
1316. Epiney / Hänni / Brülisauer, *Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts = L' indépendence des autorités de surveillance et autres questions actuelles en droit de la protection des données*, p. 75.
1317. art. 57, al. 1, m) RGPD.

contractuelles [1318], ainsi que de critères de certification, qui sont des compétences nouvelles.

1597 Les services rendus par l'autorité de contrôle « seront gratuits pour la personne concernée et [...] pour le délégué à la protection des données [1319] ».

1598 Les États membres prévoient que l'autorité de contrôle puisse demander une contribution financière pour l'accomplissement de ses missions, aux responsables du traitement ou aux sous-traitants, qui ne disposent pas d'un délégué à la protection de données. Cet aspect financier vise à résoudre le problème des ressources financières de l'autorité de contrôle et incite les organismes à nommer un délégué à la protection des données même si elles n'ont pas l'obligation de le faire [1320]. Le Règlement prévoit déjà la possibilité de demander le paiement de frais raisonnables sur la base de ses coûts administratifs ou de refuser de donner suite à une demande lorsque celle-ci est manifestement infondée ou excessive [1321].

1599 Les pouvoirs de l'autorité de contrôle sont harmonisés par le Règlement européen [1322].

1600 Le Règlement prévoit trois catégories de pouvoirs [1323] :

- les pouvoirs d'enquête ;
- les pouvoirs correcteurs ;
- les pouvoirs consultatifs et d'autorisation.

1601 Les pouvoirs d'enquête donnent le droit à l'autorité de contrôle d'exiger des informations et de conduire une évaluation de la politique de la protection des données de l'organisation [1324]. Si celle-ci a obtenu une certification, l'autorité de contrôle peut vérifier la validité de cette dernière [1325]. L'autorité doit avoir accès à toutes les informations et données nécessaires pour conduire son évalua-

1318. art. 57, al. 1, j) RGPD.
1319. art. 57, al.3 RGPD.
1320. art. 37 RGPD.
1321. art. 57, al. 4 RGPD.
1322. Consid. 100 RGPD.
1323. art. 58 RGPD.
1324. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 719 ss.
1325. *Idem*, 3.11, p. 270.

tion [1326].

Dans le cadre de ses pouvoirs d'enquête, l'autorité de contrôle est habilitée à conduire des audits, à demander des informations voire à accéder aux locaux du responsable du traitement. Il s'agit de pouvoirs d'investigations nécessaires pour instruire les dossiers, et constater d'éventuelles infractions au Règlement [1327]. Ces pouvoirs d'enquête permettent une coopération entre autorités compétentes dans le cadre des mécanismes mis en place par le Règlement [1328]. 1602

Le Règlement attribue également des pouvoirs correcteurs à l'autorité de contrôle. Celle-ci est en droit de prendre des mesures effectives pour assurer la conformité de l'organisation au Règlement européen. L'autorité de contrôle peut donner des instructions concernant le respect des droits des personnes concernées et des obligations du responsable du traitement. Elle peut interdire certains traitements ou les limiter, voire retirer un certificat de conformité au Règlement [1329]. Elle détient des prérogatives d'admonestation, de suspension ou d'interdiction du traitement à l'autorité de contrôle. Celle-ci est également habilitée à ordonner des amendes administratives [1330]. 1603

Si le responsable du traitement ou le sous-traitant ne respecte pas une injonction, prononcée par l'autorité de contrôle, une sanction administrative pourra être prononcée [1331]. Le montant de cette sanction pouvant s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu [1332]. Si le système juridique d'un État membre ne prévoit pas d'amende administrative, l'amende sera imposée par une juridiction nationale compétente avec effet équivalent aux amendes administratives prononcées par une autorité de contrôle [1333]. 1604

Dans les autres cas [1334], le montant de l'amende administrative pourra 1605

1326. *Idem*, 5, p. 721.
1327. Docquir, *Droit du numérique*, p. 30.
1328. *Ibidem.*
1329. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 722 ss.
1330. art. 83 RGPD.
1331. art. 83 RGPD.
1332. art. 83, al. 6 RGPD.
1333. art. 83, al. 9 RGPD.
1334. En cas de violation des dispositions spécifiques mentionnées aux articles 83,

s'élever jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires dans les cas les plus graves [1335].

1606 Chaque État membre décidera, si de telles amendes administratives sont susceptibles d'être prononcées à l'encontre des autorités et organismes publics établis sur son territoire [1336].

1607 La CNIL a prononcé une astreinte quotidienne en plus d'une amende administrative en matière de vidéosurveillance excessive. Ce pouvoir d'astreinte peut atteindre 100'000 euros maximum par jour [1337]. Un risque nouveau à prendre en considération.

1608 Ces pouvoirs doivent respecter le cadre juridique applicable, comme par exemple les garanties procédurales : le droit de la défense, le respect du droit à un recours juridictionnel ou le principe d'impartialité [1338].

1609 Chaque autorité de contrôle de l'UE a le pouvoir d'ester en justice en vue de faire appliquer le Règlement ou encore de porter toute violation à l'attention des autorités judiciaires [1339].

1610 Une action judiciaire peut donc être intentée contre le responsable du traitement devant les tribunaux civils ordinaires [1340].

1611 En outre, les tribunaux compétents en matière pénale pourront éga-

al. 4 et 5 RGPD.

1335. art. 83, al. 5 du Règlement qui vise la violation « des principes de bases », des droits des personnes et des règles en matière de transferts hors de l'Union.

1336. art. 58, al. 5 RGPD.

1337. CNIL, Délibération de la formation restreinte n° SAN-2019-006 du 13 juin 2019 prononçant une sanction à l'encontre de la société Uniontrad Company, consid. 4.

1338. art. 58, al. 4 RGPD. Les États membres doivent également veiller à l'application de l'article 6 de la convention européenne de sauvegarde des droits de l'homme ou de la Charte européenne des droits fondamentaux qui s'applique aux États membres dans l'application du droit de l'union (art. 51, al. 1).

1339. Parallèle avec l'art. 79 du Règlement qui prévoit le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant.

1340. art. 79 RGPD.

lement être saisis d'une violation du Règlement [1341].

Le Règlement octroie enfin à l'autorité de contrôle un pouvoir consultatif et d'autorisation. Elle peut rendre des avis au législateur national s'il est saisi par celui-ci dans le cadre d'une consultation préalable [1342]. Du fait de son expertise dans le domaine de la protection des données, l'autorité de contrôle est compétente pour identifier les risques d'un projet législatif ou administratif et pour proposer au législateur des améliorations au texte afin de garantir un traitement des données conforme aux législations (européenne ou nationales) pertinentes. Gage de transparence, la publication des avis de l'autorité de contrôle et celle de son rapport annuel sont des sources précieuses d'informations. Ils témoignent à la fois de l'activité de l'autorité de contrôle et de son interprétation des dispositions relatives à la protection des données. 1612

Pour certaines juridictions, le rôle dévolu à l'autorité de contrôle en matière de protection des données est profondément transformé [1343]. 1613

Cette transformation se manifeste également concernant les transferts transfrontaliers. Le Règlement européen formalise dans ce domaine la jurisprudence de la CJUE [1344]. Cet arrêt de principe stipule que « l'existence d'une décision d'adéquation adoptée par la Commission européenne n'a pas pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat aux données à caractère personnel transférées et, le cas échéant, de suspendre le transfert de ces données ». « Ainsi cette jurisprudence rappelle non seulement que le « caractère adéquat du niveau de protection offert par un pays tiers peut évoluer avec le temps en fonction du chan- 1614

1341. Dès lors que l'article 84 dispose que les États membres peuvent prévoir d'autres sanctions applicables en cas de violation du Règlement, « en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83 ».

1342. art. 67, al. 1, c) RGPD et 58, al. 3, b) ou encore 36, al.4 RGPD.

1343. Agence des droits fondamentaux de l'Union européenne, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données - Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, in : FRA (https ://fra.europa.eu/), Vienne 2010, p. « https : / / fra . europa . eu / fr / publication / 2012 / la - protection - des - donnees - caractere - personnel - dans - lunion - europeenne - le - role - des?lang%5B0%5D=fr » (01/04/2020).

1344. Arrêt M. Schrems du 06 octobre 2015, C-362/14, ECLI :EU :C :2015 :650, consid. 99 ss. ; Kühling / Buchner, *Datenschutz - Grundverordnung / BDSG*, p. 913.

gement des circonstances à la fois factuelles et juridiques qui ont fondé ladite décision » (point 1626) mais donne mandate à l'autorité de contrôle d'enquêter sur une plainte relative aux transferts transfrontaliers voire de suspendre ce transfert ».

1615 Les pouvoirs octroyés à l'autorité de contrôle dans le Règlement visent à protéger les intérêts des tiers. Il s'agit de tous les administrés qui ne veulent pas ou ne peuvent pas faire respecter leurs droits à la protection des données. L'autorité de contrôle doit veiller à une pondération équilibrée des intérêts privés et publics en présence.

IV. Les mécanismes de coopération : l'autorité-chef de file et le mécanisme de guichet unique

1616 L'introduction du mécanisme de coopération et la désignation d'une autorité-chef de file constituent une innovation du Règlement.

1617 L'article 28, par. 1, al. 2 de la directive 95/46/CE, disposait que « les autorités de contrôle [...] exercent en toute indépendance les missions dont elles sont investies ». Cela signifiait que les autorités exerçaient leur mandat en étant indépendantes les unes des autres. Il n'existait « aucun critère de priorité » régissant l'intervention des autorités de contrôle les unes par rapport aux autres ni ne prescrivant l'obligation pour une autorité de contrôle d'un État membre de se conformer à la position exprimée, le cas échéant, par l'autorité de contrôle d'un autre État membre [1345]».

V. La mise en œuvre du droit applicable

1618 Pour les traitements internes à l'UE, la question de la mise en œuvre du droit applicable ne devrait plus se poser, car le Règlement a vocation à s'appliquer sur le territoire de l'Union de manière homogène.

1619 Le Règlement apporte ici une solution à un problème qui était récurrent à l'époque de l'application de la directive 95/46/CE (art.

1345. Arrêt CJUE du 5 juin 2018, *Wirtschaftsakademie*, C—210/16, consid. 69.

4) [1346].

En revanche, la question de la mise en œuvre du droit applicable garde toute sa pertinence pour les traitements transfrontaliers de données. 1620

Afin de résoudre cette difficulté, le Règlement institue une autorité « chef de file ». En principe, seule cette autorité est compétente pour adopter des mesures à l'égard du responsable du traitement, lorsque ce dernier a son établissement principal sur le territoire de l'autorité de contrôle. Désormais, le responsable du traitement et le sous-traitant doivent contacter en priorité cette autorité pour toute question relative à la protection des données [1347]. 1621

La compétence juridictionnelle de chaque autorité de contrôle s'exerce sur le territoire de l'État membre dont elle relève [1348]. « L'autorité de contrôle est compétente pour connaître du traitement de données effectué par des autorités publiques ou des autorités privées situées dans l'État de l'autorité de contrôle et agissant dans l'intérêt du public. Le lieu du traitement importe peu. Si le traitement s'inscrit dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant qui est établi sur le territoire de l'Union, alors le Règlement européen s'applique indifféremment du fait que le traitement a lieu ou non dans l'Union. La structure juridique de l'établissement n'est pas déterminante. Cependant, pour déterminer si l'entreprise est bien établie dans l'UE, il sera vérifié qu'elle exerce effectivement et réellement son activité au moyen d'un dispositif stable [1349] ». 1622

Lorsque plusieurs autorités de contrôle sont compétentes pour exercer concurremment leur pouvoir de contrôle sur un même traitement [1350], les décisions rendues par les autorités de contrôle doivent être harmonisées et cohérentes, afin de contenir le risque d'insécurité juridique dans l'UE, qui découlerait de décisions divergentes. 1623

1346. Commission européenne, *Premier rapport sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE) - (COM(2003) 265/F1)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2003, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52003DC0265 » (01/04/2020) ; idem, *« Une approche globale de la protection des données à caractère personnel dans l'UE »*.
1347. art. 56, al. 6 RGPD.
1348. art. 55 RGPD.
1349. Consid. 22 RGPD.
1350. art. 55 RGPD.

Dans le cas des traitements transfrontaliers, le Règlement européen prévoit des dispositions spécifiques pour désigner l'autorité compétente.

§3 L'autorité-chef de file

1624 Dans le cas d'une concurrence juridictionnelle entre plusieurs autorités et de traitements transfrontaliers, le Règlement prévoit la possibilité de désigner une autorité chef de file [1351].

1625 L'autorité-chef de file est la seule autorité habilitée à prendre des mesures à l'encontre du responsable du traitement, dans le cadre d'un processus coopératif avec les autres « autorités concernées [1352] » lors du processus décisionnel du « mécanisme de coopération ». Elle est l'interlocutrice unique du responsable du traitement ou du sous-traitant [1353].

§4 Le mécanisme de guichet unique

I. Le principe

1626 Le Règlement introduit un nouveau mécanisme de coopération entre autorités de contrôle, dit « mécanisme de guichet unique ». Ce mécanisme concerne uniquement les transferts transfrontaliers. Il vise à faciliter la prise de décision appropriée au cas d'espèce.

1627 La procédure dite du « mécanisme de guichet unique » (ou de « one-stop shop » en anglais) débute par une phase de concertation entre autorités compétentes pour identifier l'autorité de contrôle ayant compétence pour contacter le responsable du traitement ou le sous-traitant [1354]. Cette coopération s'effectue avec le soutien de l'autorité-chef de file qui a l'obligation de coordonner les travaux [1355].

1628 La procédure se poursuivit par des mesures spécifiques : l'autorité peut diligenter l'ouverture d'une enquête ou demander le prononcé d'une sanction. Une procédure de contrôle du traitement transfron-

1351. art. 56 RGPD.
1352. art. 4, al. 22 RGPD.
1353. art. 57, al. 6 RGPD.
1354. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 698.
1355. *Idem*, p. 733.

talier pourra également être ouverte [1356]. Dans cette situation, l'autorité « chef de file » conduira la procédure de coopération de l'article 60 du Règlement [1357].

En principe, l'autorité-chef de file sera chargée d'adopter les mesures concernant un traitement dont le responsable a son établissement unique ou son établissement principal sur le territoire de l'autorité-chef de file [1358]. 1629

Avec le mécanisme de guichet unique, l'autorité « chef de file » coordonne les relations avec les autres autorités. Elle peut rendre une décision et adopter des mesures à l'égard d'un traitement transfrontalier, dans un esprit de coopération et de consensus avec les autres autorités. Dans le cadre de cette coopération avec les autres autorités concernées, elles échangent toutes les informations utiles et s'efforcent de parvenir à un consensus [1359]. 1630

Avant toute décision, l'autorité-chef de file pourra procéder à des enquêtes, à une collecte d'information ou à d'autres actions préalables qui échappent à sa compétence territoriale. Elle pourra également demander à une autre autorité de se prêter mutuellement assistance [1360] ou de mener des opérations conjointes [1361]. 1631

L'autorité « chef de file » communique sans tarder aux autres autorités les informations utiles sur la question traitée et leur soumet également sans tarder un projet de décision en vue d'obtenir leur avis [1362]. 1632

Si des divergences persistent après la communication du projet de décision aux autorités concernées, celles-ci disposent de quatre semaines pour présenter une « objection pertinente et motivée [1363] ». 1633

Préalablement à la communication du projet de décision, à partir duquel court le délai de 4 semaines, les autorités de contrôle pourront échanger des informations dans le cadre de discussions informelles pour sonder leurs positions respectives afin d'arriver à un 1634

1356. art. 56, al. 1 RGPD.
1357. art. 56 RGPD.
1358. art. 56, al. 1 RGPD.
1359. art. 60, al. 1 RGPD.
1360. art. 61 RGPD.
1361. art. 62 RGPD.
1362. art. 60, al. 4 RGPD.
1363. art. 4, 24 RGPD.

consensus préalable.

1635 Si une ou plusieurs autorités font part d'une « objection pertinente et motivée », après la communication de la décision, l'autorité « chef de file » a l'option de suivre ou non l'objection formulée.

1636 Dans le *premier* cas, l'autorité-chef de file soumet la question au Comité ce qui enclenche « le mécanisme de contrôle de la cohérence [1364]».

1637 Dans le *second* cas, l'autorité « chef de file » soumet aux autres autorités un projet de décision amendé, pour avis [1365].

1638 À l'issue de deux semaines de consultation, si une autorité formule encore une objection pertinente et motivée, l'autorité-chef de file soumet la question au Comité dans le cadre du mécanisme de « contrôle de la cohérence ».

1639 A défaut, la décision est adoptée et obtient valeur contraignante à l'égard des autres autorités [1366].

1640 L'autorité-chef de file notifie cette décision au responsable du traitement ou au sous-traitant au lieu de leur établissement. Les autres autorités concernées ainsi que le Comité seront informés de la décision ainsi que des « faits et motifs pertinents ».

1641 Le Règlement prévoit que les communications entre autorités, dans le cadre du mécanisme de la cohérence, s'effectuent par voie électronique, au moyen d'un formulaire type [1367]. Les délais qui s'imposent aux autorités sont courts, ce qui justifie le recours à ce mode de communication.

1642 Le Règlement prévoit qu'en cas de réclamation, dans le cadre du mécanisme de guichet unique, l'autorité de contrôle ayant reçu la réclamation doit informer son auteur de la décision prise [1368].

1643 Dans le cas du rejet d'une réclamation, l'autorité de contrôle ayant

1364. art. 65 RGPD.
1365. art. 60, al. 5 RGPD.
1366. art. 60, al. 7 RGPD.
1367. art. 60, al. 12 RGPD.
1368. art. 77, al. 2 RGPD.

reçu la plainte adoptera la décision et la notifiera à son auteur [1369].

Dans le cas d'un rejet partiel d'une réclamation, deux décisions distinctes peuvent être prises : l'une concernant les obligations du responsable du traitement [1370] et adoptée par l'autorité-chef de file et l'autre concernant le refus ou le rejet de la réclamation et adopté par l'autorité ayant reçu ladite plainte. La première décision est notifiée au responsable du traitement ou au sous-traitant, et l'auteur de la plainte en sera informé. La seconde décision est notifiée à l'auteur de la plainte et les responsables du traitement ou le sous-traitant en seront informés. 1644

Cette procédure offre la garantie d'un recours juridictionnel effectif pour la personnes ayant introduit une réclamation auprès de son autorité de contrôle à l'encontre d'une décision qui ne lui donne pas satisfaction. Le droit à un recours effectif est reconnu par la Charte des droits fondamentaux de l'Union européenne [1371], par l'art. 13 CEDH et par le Règlement qui prévoit l'introduction d'un recours contre une autorité de contrôle [1372]. 1645

Le recours juridictionnel effectif implique en premier lieu l'obligation pour les Etats membres d'ouvrir aux titulaires de droits des procédures de recours susceptibles d'être mises en œuvre en cas de violation alléguée de ces droits [1373]. Ces procédures doivent respecter l'indépendance et l'impartialité du tribunal, et le caractère équitable de la procédure, garanti par le respect des droits de la défense [1374]. 1646

La décision qui résulte d'une plainte est systématiquement notifiée à son auteur [1375]. Un recours contre cette décision peut être porté 1647

1369. art. 60, al. 8 RGPD.
1370. Ou du sous-traitant, même si ce dernier n'est pas mentionné dans l'art. 60, al. 9 du Règlement.
1371. art. 47 de la Charte des droits fondamentaux de l'Union européenne.
1372. art. 78 RGPD.
1373. Arrêt CJUE du 14 mars 2018, *Astellas Pharma*, C—557/16, ECLI :EU :C :2018 :181, consid. 41 ; Arrêt CJUE du 13 décembre 2017, *Soufiane El Hassani contre Minister Spraw Zagranicznych*, C—403/16, ECLI :EU :C :2017 :960, consid. 42 ; Arrêt CJUE du 27 février 2018, *Associaçao Sindical dos Juizes, Porugueses*, C-64/16, ECLI :EU :C :2018 :117, consid. 34.
1374. Arrêt CJUE du 27 février 2018, *Associaçao Sindical dos Juizes*, C—64/16, ECLI :EU :C :2018 :117, consid.16 ; Arrêt CJUE du 13 septembre 2018, *UBS Europe SE et Alain Hondequin et consorts contre DV e.a.*, C—358/16, ECLI :EU :C :2018 :715, consid. 59-61.
1375. art. 60 RGPD.

devant les tribunaux de l'autorité ayant reçu la plainte.

1648 Si le responsable du traitement ou le sous-traitant prend des mesures spécifiques pour assurer le respect de la décision, après sa notification, concernant les activités de traitement menées dans tous les établissements dans l'UE, celles-ci doivent être documentées et notifiées à l'autorité-chef de file qui en informe les autres autorités concernées [1376].

II. Les exceptions au mécanisme de guichet unique

1649 Le principe du mécanisme de guichet unique connaît quelques exceptions (art. 6, 1, c) RGPD).

1650 La première exception concerne les traitements effectués par des autorités publiques ou des organismes privés en exécution d'une obligation légale ou d'une mission d'intérêt public dont est investi le responsable du traitement [1377].

1651 Le mécanisme de guichet unique ne s'applique pas dans cette hypothèse [1378] et l'autorité publique de contrôle de cet État membre est compétente pour superviser les activités de cet organisme public.

1652 Par exemple, la CNIL est responsable du contrôle des transferts transfrontaliers en matière d'échanges d'informations en matière fiscale par la Direction Générale des Finances Publiques en France.

1653 Il en est de même lorsque des organismes privés sont investis d'une mission d'intérêt public ou effectuent un traitement requis par la loi.

1654 La seconde exception concerne le cas d'une réclamation déposée auprès d'une autorité non « chef de file », concernant un traitement transfrontalier. L'autorité sera compétente pour traiter cette plainte, si l'objet de la plainte concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement

1376. art. 60, al. 10 RGPD.
1377. Traitements effectués en application de l'art. 6, 1, c) RGPD.
1378. art. 56 RGPD.

des personnes concernées dans cet État membre uniquement [1379].

L'autorité recevant la réclamation doit notifier l'autorité « chef de file ». Cette dernière dispose de trois semaines pour décider d'appliquer ou non la procédure du mécanisme du guichet unique [1380]. 1655

Si l'autorité-chef de file décide de ne pas traiter le cas, l'autorité ayant reçu la plainte conserve la possibilité de demander l'assistance mutuelle d'autres autorités ou de mettre en place des opérations conjointes en vertu des articles 61 et 62 du Règlement [1381]. 1656

Si l'autorité-chef de file décide de traiter le cas, elle le fera conformément au mécanisme du guichet unique. Cependant l'autorité saisie de la plainte pourra soumettre un projet de décision à l'autorité-chef de file qui en prendra le plus grand compte en élaborant le projet de décision visé à l'article 60 du Règlement [1382]. 1657

L'autorité ayant reçu la plainte bénéficie d'un rôle central, car les autres autorités ne sont pas appelées à proposer un projet de décision. 1658

Le Règlement prévoit enfin une procédure d'urgence, durant laquelle le mécanisme du guichet unique ne s'applique pas [1383]. Lorsqu'il est nécessaire d'intervenir en urgence pour protéger les droits de l'homme et les libertés fondamentales des personnes concernées [1384], une autorité de contrôle qui n'est pas chef de file peut adopter des mesures provisoires dûment justifiées et d'une durée de validité déterminée qui n'excède pas trois mois [1385]. 1659

L'urgence est présumée lorsqu'une autorité ne répond pas à une demande d'assistance mutuelle ou ne respecte pas les obligations prévues en cas d'opération conjointe. L'autorité ayant adopté une mesure urgente en vertu de l'article 66, et qui estime que des mesures définitives doivent être adoptées d'urgence, demande un avis urgent ou une décision urgente au comité dans le cadre du mécanisme de contrôle de la cohérence. Toute autre autorité pourra également également saisir le Comité si elle estime qu'une autre auto- 1660

1379. art. 56, al. 2 RGPD.
1380. art. 56, al. 3 RGPD.
1381. art. 56, al. 5 RGPD.
1382. art. 56, al. 4 RGPD.
1383. art. 60, al. 10 RGPD.
1384. Consid. 137 RGPD.
1385. art. 66, al. 1 RGPD.

rité n'a pas pris les mesures urgentes qui s'imposaient [1386]. Dans ces hypothèses, les délais ordinaires pour adopter une mesure urgente sont réduits [1387].

1661 Le législateur européen a conçu le mécanisme du guichet unique « pour renforcer l'efficacité de la communication avec le responsable du traitement ou le sous-traitant tout en favorisant la concertation entre plusieurs autorités de contrôle, préalablement à l'adoption d'une mesure destinée à produire des effets juridiques en ce qui concerne des opérations de traitement qui affectent sensiblement un nombre important de personnes concernées dans plusieurs États membres [1388] ».

1662 La définition de la notion de traitement transfrontalier est essentielle pour déterminer dans quels cas l'article 56, et le mécanisme de guichet unique de l'article 60, seront applicables.

1663 Le Règlement définit ainsi la notion de traitement transfrontalier. Il s'agit

- « d'un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable de traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou
- d'un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres [1389] ».

1664 La qualification de traitement transfrontalier n'est pas retenue si le responsable du traitement est uniquement établi dans un État membre et si le traitement n'affecte que les individus établis dans ce même État membre. Il s'agit dans ce cas d'un traitement « local [1390] »

1386. art. 66, al. 3 RGPD.
1387. art. 66, al. 4 RGPD.
1388. Consid. 135 RGPD.
1389. art. 4, al. 23 RGPD.
1390. Groupe de Travail de l'Article 29, *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant*, p. 9.

et la procédure du guichet unique ne s'applique pas.

Dans les autres hypothèses, la qualification de traitement transfrontalier est retenue. Le responsable du traitement ou le sous-traitant doivent bénéficier d'au moins un établissement dans l'Union. D'où l'importance de la définition de la notion d'établissement. 1665

L'autorité-chef de file sera celle située dans l'État membre dans lequel se trouve *(i)* l'établissement principal du responsable du traitement, *(ii)* son seul établissement, s'il n'en a qu'un et que le traitement affecte sensiblement d'autres individus dans plus d'un État membre [1391]. 1666

Le Règlement qualifie d'« établissement principal» [1392] : 1667

- « en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement ait le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal » ;
- « en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent Règlement ».

Le siège du responsable du traitement est considéré comme l'établissement principal (présomption du Règlement), même si le groupe possède des succursales, filiales ou bureaux de représentation à l'étranger [1393]. Cette présomption sera renversée lorsque les décisions sur le traitement et le pouvoir de les mettre en œuvre se prennent dans un autre établissement du responsable du traitement 1668

1391. art. 56, al. 1 RGPD.
1392. art. 4 et 56 RGPD.
1393. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 698.

dans un autre État membre [1394]. Ainsi, l'établissement principal suppose l'exercice effectif et réel d'activités de gestion déterminant les décisions principales relatives au traitement, sans pour autant que le traitement ait lieu à cet endroit. Le Règlement respecte en cela la jurisprudence de la CJCE.

1669 Le Règlement s'applique lorsque le responsable du traitement est établi hors de l'Union mais dirige ses activités de traitement vers des individus situés dans l'Union [1395]. Il s'agit du « principe du marché » (« Marktoprinzip aussi appelé ciblage ») [1396].

1670 Dans ses lignes directrices, le Comité européen sur la protection des données considère que « le nombre de personnes affectées dans un autre État membre n'est pas déterminant pour conclure que les personnes sont affectées par un traitement, au contraire de la nature de l'impact qui est centrale ». Les critères à prendre en considération sont les suivants :

- le contexte du traitement,
- les types de données,
- l'objectif du traitement, et
- le fait que le traitement entraîne ou est susceptible d'entraîner un préjudice, une perte ou un désagrément, que le traitement affecte ou est susceptible d'affecter le statut financier ou économique des individus, ou encore le nombre de données en cause [1397].

1671 Le Comité européen reconnaît la possibilité de désigner plusieurs autorités de contrôle pour un seul responsable du traitement, selon les traitements concernés [1398]. Il s'agit des cas où le responsable du traitement opère plusieurs traitements transfrontaliers sous des modalités différentes [1399].

1672 Lorsque le responsable du traitement n'a pas d'administration centrale dans l'UE, ni d'établissement dans l'UE prenant des décisions

1394. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 699.
1395. art. 3, al. 2 RGPD.
1396. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 699.
1397. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 4.
1398. *Idem*, p. 5.
1399. *Idem*, p. 5.

en lien avec le traitement de données personnelles, il désigne l'établissement qui agit comme « établissement principal [1400] ».

Cette solution permet de pallier l'absence de guichet unique pour les multinationales qui ne sont pas établies dans l'Union mais qui sont soumises au Règlement. Celles-ci doivent par ailleurs désigner un représentant établi dans l'UE [1401]. 1673

Quant aux sous-traitants, « s'ils n'ont pas d'administration centrale dans l'Union, leur établissement principal est l'établissement dans lequel se déroule l'essentiel des activités de traitement dans l'Union [1402] ». 1674

Le considérant 36 du Règlement précise que « lorsque le responsable du traitement et le sous-traitant sont tous deux concernés, l'autorité de contrôle de l'État membre dans lequel le responsable du traitement a son établissement principal devrait rester l'autorité de contrôle chef de file compétente, mais l'autorité de contrôle du sous-traitant devrait être considérée comme étant une autorité de contrôle concernée et cette autorité de contrôle devrait participer à la procédure de coopération prévue par le présent Règlement ». Lorsque le sous-traitant est choisi par le responsable du traitement, deux autorités chef de file peuvent être compétentes, chacune séparément pour ces deux acteurs ». 1675

Les autres autorités de contrôle qui ne sont pas désignées comme autorité « chef de file » jouent cependant un rôle dans la procédure de coopération (mécanisme de guichet unique) [1403]. 1676

Elles sont consultées par l'autorité-chef de file, avant l'adoption d'une mesure [1404]. Le Règlement les qualifie « d'autorités de contrôle concernées ». 1677

Les autorités sont qualifiées d'« autorités de contrôle concernées » dans des cas précis : 1678

— « le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de

1400. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, p. 7.
1401. art. 27 RGPD.
1402. art. 4, al. 16 et consid. 36 RGPD.
1403. art. 60 à 62 RGPD.
1404. art. 60 RGPD.

contrôle relève ;

— des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ; ou

— une réclamation a été introduite auprès de cette autorité de contrôle [1405] ».

1679 Si les autorités compétentes sont en désaccord concernant la désignation de l'autorité-chef de file, alors le Comité européen pour la protection des données est compétent pour trancher cette question [1406].

§5 L'assistance mutuelle et les opérations conjointes

1680 La coopération entre autorités de contrôle constitue une nouvelle obligation formelle du Règlement, en cas de transferts transfrontaliers [1407] dans le cadre du mécanisme de guichet unique, l'autorité-chef de file coopère avec les autres autorités qui apportent leurs contributions, à l'occasion d'une demande d'information, d'une enquête, de mesures de contrôle. Il s'agit d'une nouveauté majeure du Règlement, qui soulève de nombreuses questions notamment concernant la planification des ressources [1408].

1681 La coopération entre autorités de contrôle peut également être instaurée en-dehors du mécanisme de guichet unique, et des cas de traitements transfrontaliers. À titre d'exemple peut être citée la coopération intervenue dans le cadre du contentieux de l'arrêt Google Spain.

1682 Le Règlement prévoit deux situations spécifiques :

— l'assistance administrative mutuelle [1409] ; et

— les opérations conjointes des autorités de contrôle [1410].

1405. art. 4, al. 22 RGPD.
1406. art. 65, al. 1, b) RGPD.
1407. art. 60 RGPD ; Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 732.
1408. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 732.
1409. art. 61 RGPD.
1410. art. 62 RGPD.

Le Règlement ne définit pas la notion d'« assistance administrative mutuelle ». Le Règlement indique qu'elle le service offert le sera en principe à titre gratuit [1411]. Le champ d'application de l'assistance administrative mutuelle comprend les demandes d'information et les mesures de contrôle, comme les demandes d'autorisation préalable, les inspections et les enquêtes [1412]. 1683

Pour la doctrine, cette assistance mutuelle s'étend au-delà du soutien et de l'échange de renseignements dans des cas isolés. Les administrations doivent définir un cadre pour traiter de manière efficace et rapide les demandes reçues [1413]. 1684

Les autorités de contrôle doivent répondre à une demande d'assistance mutuelle dans le délai d'un mois [1414]. La demande doit contenir les informations nécessaires, notamment les finalités et les motifs qui la fondent [1415]. 1685

Elles ont cependant l'obligation d'offrir une prestation de soutien, lors d'une enquête sur le traitement de données personnelles d'un cas d'espèce [1416]. 1686

Une autorité de contrôle doit répondre systématiquement aux demandes reçues, sauf si *(i)* elle n'est pas compétente pour traiter l'objet de la demande ou pour prendre les mesures qu'elle est requise d'exécuter, *(ii)* satisfaire à la demande constituerait une violation du Règlement ou du droit de l'Union ou du droit de l'État membre auquel l'autorité de contrôle qui a reçu la demande est soumise [1417]. 1687

L'obligation de coopération, définie de façon aussi précise est une nouveauté du Règlement. Les possibilités de refus d'entrée en matière sont limitées par des conditions strictes [1418]. 1688

Une procédure de coopération extraordinaire existe aussi en cas d'urgence (art. 66, al. 1 RGPD). Elle dure trois mois et permet de 1689

1411. art. 62, al. 5 RGPD.
1412. art. 61 RGPD.
1413. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 739.
1414. art. 61, al. 2 RGPD.
1415. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 739.
1416. *Ibidem.*
1417. art. 62, al. 3 RGPD.
1418. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 740.

contourner le mécanisme de contrôle de la cohérence. Si une autorité ne fournit pas les informations demandées dans le mois, l'autorité de contrôle peut, par dérogation au mécanisme de guichet unique ordinaire, adopter une mesure provisoire, conformément à l'article 66, relatif aux mesures prises, en cas d'urgence, l'urgence étant ici présumée [1419].

1690 Une coopération conjointe est également possible [1420] pour conduire des enquêtes conjointes, et prendre des mesures répressives conjointes, entre plusieurs autorités de contrôle. Cette option apparaît particulièrement pertinente pour les traitements transfrontaliers : le Règlement européen précise en effet que l'autorité de contrôle d'un État membre où se trouve l'un des établissements ou d'un État où se trouve « un nombre important de personnes concernées sont susceptibles d'être sensiblement affectées par des opérations de traitement », a le droit de participer aux opérations conjointes [1421].

1691 Dans la limite du droit applicable, cette dernière autorité de contrôle peut conférer des pouvoirs aux agents de l'autorité de l'autre État (ex. : pouvoirs d'enquête) [1422].

1692 Dans l'éventualité d'un dommage causé lors d'opérations conjointes, les principes de responsabilité applicables de l'autorité de contrôle sont précisés en toute transparence dans le Règlement [1423]. Lorsqu'une autorité de contrôle ne se conforme pas dans le mois à la demande de participer à une opération conjointe ordonnée par l'autorité chef de file, les autres autorités de contrôle peuvent adopter une mesure provisoire sur le territoire de leur État, conformément à l'article 66 applicable aux mesures prises en cas d'urgence, l'urgence étant ici présumée.

1693 Selon le Préposé fédéral à la protection des données, « on peut s'attendre à ce que l'Union européenne souhaite exercer un droit de regard sur la façon dont les États tiers, mettent en application les principes que le Règlement contient. La Suisse sera tout particulièrement l'objet d'une surveillance étroite de l'Union européenne, car en tant que membre associé du dispositif de Schengen et de Du-

1419. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 755.
1420. art. 62 RGPD.
1421. art. 62, al. 2 RGPD.
1422. art. 62, al. 2 RGPD.
1423. art. 62, al. 4 à 6 RGPD.

blin, elle échange de grandes quantités de données administratives sensibles avec l'UE [1424]».

§6 Le Comité européen de la protection des données

Le Comité européen de la protection des données remplace le groupe de travail de l'Article 29 de la Commission européenne, en l'institutionnalisant formellement [1425]. Il vise à l'uniformisation de la doctrine des autorités de contrôle concernant au sein de l'Union européenne [1426]. 1694

Il est constitué des différentes autorités de contrôle nationales, du Contrôleur européen de la protection des données et d'un représentant de la Commission européenne. 1695

Le Comité est un organe indépendant de l'UE [1427], qui détient la personnalité juridique [1428]. 1696

Il joue un rôle central dans le « mécanisme de contrôle de la cohérence » des décisions prises par les autorités de contrôle en application du Règlement. 1697

Le Comité européen est représenté par un président, soutenu de deux vice-présidents nommés à la majorité simple pour un mandat de cinq ans renouvelable une fois [1429]. 1698

Le Président convoque les réunions du Comité, établit l'ordre du jour, notifie les décisions du Comité aux autorités de contrôles, et veille au bon déroulement du mécanisme de contrôle de la cohérence [1430]. Il supervise également le secrétariat du Comité, qui est assuré par le Contrôleur européen de la protection des données. Ce dernier est placé sous l'autorité exclusive du président du Comité [1431]. Le secrétariat du Comité fournira un « soutien analy- 1699

1424. PFPDT, *24ème Rapport d'activités*, p. 8.
1425. art. 139 RGPD.
1426. Banck Aurélie, *RGPD : la protection des données à caractère personnel : 18 fiches pour réussir votre mise en conformité*, 1e éd., Issy-les-Moulineaux 2018, p. 17.
1427. art. 69 RGPD.
1428. art. 68, al. 1 RGPD.
1429. art. 73 RGPD.
1430. art. 74, al. 1 RGPD.
1431. art. 75, al. 2 RGPD.

tique, administratif et logistique au Comité [1432]». Le secrétariat sera chargé de la « communication avec d'autres institutions et le public », de la préparation et du suivi des réunions du Comité, et enfin de la préparation, de la rédaction et la publication d'avis, de décisions et d'autres textes adoptés par le Comité [1433].

1700 Le Comité prend ses décisions à la majorité simple de ses membres [1434], sauf pour l'adoption du Règlement intérieur qui nécessite une majorité de deux tiers [1435] ou pour l'adoption de décisions dans le cadre du mécanisme de contrôle de la cohérence (art. 65, al. 1 RGPD). La Commission peut participer aux réunions du Comité mais n'a pas de droit de vote [1436].

1701 Le contrôleur européen dispose également d'un droit de vote « pour les décisions concernant les principes et règles applicables aux institutions, organes et organismes de l'Union qui correspondent en substance à ceux énoncés dans le Règlement [1437]». Son personnel est indépendant (art. 75 RGPD).

1702 Le Comité définit sa politique en matière de confidentialité des débats, dans son Règlement intérieur [1438]. Les débats sont confidentiels lorsque le Comité le juge nécessaire. Par conséquent, le principe est celui de la publicité des débats ce qui est essentiel dans une logique de transparence. Le public a ainsi connaissance de la position de chaque autorité en cas de vote, d'adoption d'avis et de décisions contraignantes.

I. Les missions du Comité

1703 Le Comité surveille et garantit l'application du mécanisme du contrôle de la cohérence [1439]. Il « favorise la coopération des autorités de contrôle dans l'ensemble de l'Union [1440]».

1704 Il conseille la Commission sur « toute question relative à la protection des données à caractère personnel dans l'Union, y compris sur

1432. art. 75, al. 5 RGPD.
1433. art. 75, al. 6 RGPD.
1434. art. 72, al. 1 RGPD.
1435. art. 72, al. 2 RGPD.
1436. art. 68, al. 4 RGPD.
1437. art. 68, al. 6 RGPD.
1438. art. 76, al. 1 RGPD.
1439. art. 64 et 65 RGPD.
1440. Consid. 139 RGPD.

tout projet de modification du Règlement [1441]».

Il publie un rapport annuel sur la protection des personnes physiques dans l'UE, qui effectue la synthèse des lignes directrices, recommandations ou bonnes pratiques afin de favoriser l'application cohérente du Règlement [1442]. 1705

Le Comité peut émettre des avis sur les décisions d'adéquation rendues par la Commission [1443]. 1706

II. Le mécanisme du contrôle de la cohérence

Une autorité de contrôle doit soumettre un projet de décision pour avis au Comité européen pour la protection des données, chaque fois qu'elle envisage d'adopter l'une des mesures citées à l'article 64, al. 1 du Règlement. 1707

Cela concerne toute mesure qui : 1708

(a) « vise à adopter une liste d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données doit être effectuée en application de l'article 35, al. 4 RGPD ;

(b) concerne la question de savoir, en application de l'article 40, al. 7, si un projet de code de conduite ou une modification ou une prorogation d'un code de conduite respecte le présent Règlement ;

(c) vise à approuver les critères d'agrément d'un organisme en application de l'article 41, al. 3, ou d'un organisme de certification en application de l'article 43, al. 3 ;

(d) vise à fixer des clauses types de protection des données visées à l'article 46, al.2 , d), et à l'article 28, al. 8 ;

(e) vise à autoriser les clauses contractuelles visées à l'article 46, al. 3, pt a) ; ou

(f) vise à approuver des règles d'entreprise contraignantes au sens de l'article 47 ».

L'article 64, al. 1 du Règlement n'est pas exhaustif. D'autres sujets peuvent être relevés pour que le Comité se prononce, ce qui offre la 1709

1441. Banck, *RGPD*, p. 66.
1442. art. 70, al. 1, a), b), e) RGPD.
1443. Mécanisme déjà prévu à l'art. 30, al. 1, b) de la directive 95/46/CE.

garantie au public que toute nouvelle question importante pourra être traitée, selon un mécanisme empreint de souplesse.

1710 L'approbation est présumée si les membres n'ont pas émis d'objection dans le délai fixé par le président, après notification de toutes les informations utiles [1444].

1711 Le Comité peut également être saisi pour avis par la Commission, par toute autorité de contrôle ou par le président du Comité « pour examiner toute question d'intérêt général ou produisant des effets dans plusieurs États membres [1445] ».

1712 Le Comité européen doit émettre son avis dans un délai de huit semaines pour rendre son avis, à la majorité simple de ses membres (avec prolongation possible de six semaines en fonction de la complexité de la question).

1713 Le comité notifie son avis à l'autorité de contrôle nationale et celle-ci dispose de deux semaines pour faire savoir au président du Comité, si elle maintient ou modifie son projet de décision. Elle informe le Comité si elle modifie son projet de décision et lui transmet le cas échéant le projet de décision modifié [1446].

1714 L'autorité de contrôle destinataire de l'avis du Comité « tient le plus grand compte de l'avis du Comité ». Si elle refuse de suivre l'avis du Comité, la procédure de Règlement des litiges de l'article 65 s'applique.

1715 La procédure d'avis est contraignante pour l'autorité de contrôle qui soumet sa mesure à l'avis du comité et limite ainsi son autonomie dans la prise de décision. L'autorité de contrôle doit attendre la fin de la procédure d'avis (maximum 14 semaines) pour adopter cette mesure [1447].

1716 À l'issue de cette procédure, le Comité rend une décision contraignante à l'égard de toutes les autorités concernées et de l'autorité-chef de file [1448].

1444. art.30, al. 3 RGPD.
1445. art. 64, al. 2 RGPD.
1446. art. 63, al. 7 RGPD.
1447. art. 60, al. 6 RGPD.
1448. art. 65, al. 2 RGPD.

III. Les décisions contraignantes du Comité européen

Le Comité adopte une décision contraignante dans des cas spécifiques (art. 60 RGPD) : 1717

(a) si dans le cadre de la procédure de coopération, une autorité-chef de file n'a pas suivi une objection pertinente et motivée émise par une autorité de contrôle concernée ;

(b) en cas de divergence entre autorités de contrôle pour déterminer la localisation de l'établissement principal ;

(c) lorsqu'une autorité de contrôle ne suit pas l'avis du Comité.

Si une autorité-chef de file n'a pas suivi une objection pertinente et motivée émise par une autorité de contrôle concernée, concernant un projet de décision qu'elle lui avait soumis ou a estimé que cette objection n'était pas pertinente ou motivée, un mécanisme de coopération et le cas échéant de règlement des litiges doit être mis en place [1449]. Préalablement à toute décision, l'autorité-chef de file doit envoyer son projet de décision aux autres autorités de contrôle concernées en vue de recueillir leurs observations (art. 60 RGPD). Si l'autorité-chef de file ne suit pas cet avis, ou estime que l'objection n'est pas pertinente ou motivée, elle doit soumettre la question au mécanisme du contrôle de la cohérence ou au Comité. 1718

L'article 66, al. 2 et 3 prévoit une procédure d'urgence, autorisant l'autorité de contrôle à adopter une mesure provisoire valable pour une durée déterminée, qui n'excède pas trois mois. Dans le cadre de cette procédure d'urgence, elle pourra introduire une demande motivée afin d'obtenir un avis urgent ou une décision contraignante urgente du Comité. 1719

La décision contraignante est adoptée à la majorité des deux tiers des membres du Comité dans un délai d'un mois à compter de la transmission de la question au Comité (prolongation possible d'un mois). Si le Comité n'a pas été en mesure d'adopter une décision dans le délai initial, le Comité peut également adopter une décision à la majorité simple, dans le délai de deux semaines, après échéance du premier délai de deux mois. La voix du président est prépondérante en cas d'égalité des voix. 1720

Un mois après la notification de la décision contraignante du Co- 1721

1449. Banck, *RGPD*, p. 67.

mité, l'autorité nationale adopte cette décision et informe le Comité de la date à laquelle sa décision finale sera notifiée au responsable du traitement, au sous-traitant et à la personne concernée. La procédure de notification est présentée à l'article 60, al. 7 à 9 du Règlement. La décision est publiée sur le site internet du Comité.

1722 Du fait du mécanisme du contrôle de la cohérence et donc de la supervision effective des décisions prises par les autorités nationales, le Comité européen peut accroître la conformité des décisions prises dans l'UE et ainsi renforcer la sécurité juridique des acteurs publics et privés. Signe d'une intégration européenne croissante, ce mécanisme est cependant perçu par certaines autorités nationales comme une mise sous tutelle, qui enfreint leur souveraineté.

1723 Certaines questions demeurent ouvertes. Selon Romain Robert, conseiller européen de la protection des données, la question se pose de savoir si, « dans le cas où l'objection concerne le montant de l'amende administrative, le Comité peut déterminer le montant de l'amende ou uniquement interdire à l'autorité-chef de file de retenir le montant proposé en lui proposant une fourchette alternative ».

IV. Les recours juridictionnels

1724 Dans le cadre du contrôle de légalité et en application de l'article 263 TFUE, la Cour de Justice de l'Union européenne peut examiner la légalité des décisions rendues par le Comité. Les recours peuvent être introduits par le responsable du traitement, sous-traitant ou une personne concernée, affectée par la décision du Comité, qui la concerne directement et individuellement, dans les deux mois de la notification qui leur est faite. L'article 263 TFUE dispose en effet que « toute personne physique ou morale peut former, dans les conditions prévues aux premiers et deuxièmes alinéas, un recours contre les actes dont elle est le destinataire ou qui la concernent directement et individuellement ainsi que contre les actes réglementaires qui la concernent directement et qui ne comportent pas de mesures d'exécution ».

1725 Les autorités de contrôle qui veulent contester la décision peuvent introduire un recours contre les décisions du Comité dans les deux

mois de la publication sur le site internet du Comité [1450].

Le Règlement prévoit enfin dans son article 78, al. 1, que toute personne physique ou morale dispose d'un recours juridictionnel effectif, devant la juridiction nationale compétente, contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne. Toute décision de sanctions, mais aussi les mesures d'enquête, les mesures d'autorisation ou les mesures correctrices, le refus ou le rejet de réclamations pourront être concernés. Les juridictions de l'État membre sur le territoire duquel l'autorité est établie seront compétentes pour examiner les recours contre une autorité de contrôle. L'article 77, al. 2, précise que lorsqu'une réclamation a été rejetée ou refusée par une autorité de contrôle, l'auteur de la réclamation peut également intenter une action devant les juridictions de ce même État membre. Il en est de même quand l'autorité de contrôle compétente ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'État d'avancement ou de l'issue de la réclamation qu'elle a introduite [1451]. 1726

L'autorité de contrôle doit transmettre l'avis ou la décision contraignante contestée à la juridiction concernée [1452]. Si la question de la validité de la décision est mise en cause, la juridiction doit soumettre cette question à la Cour de Justice, en application de l'article 267 TFUE, dans le cadre d'un renvoi préjudiciel. Cependant, un justiciable qui avait le droit d'introduire un recours en annulation contre un acte de l'Union devant la Cour de Justice de l'UE et qui ne l'a pas fait dans le délai imparti, ne peut plus se prévaloir de l'illégalité prétendue de cet acte devant le juge national pour demander un renvoi préjudiciel [1453]. Le Règlement garantit l'effectivité des pouvoirs des autorités de contrôle en limitant les conditions d'accès au renvoi préjudiciel [1454]. 1727

Ces outils institutionnels mis en place par le Règlement visent à renforcer l'effectivité du droit européen de la protection des données au sein de l'Union. Toutefois, la question des moyens mis à 1728

1450. Consid. 143 RGPD.
1451. art. 78, al. 2 RGPD.
1452. art. 78, al. 4 RGPD.
1453. Arrêt CJUE du 9 mars 1994, *TWD, Textilwerke Deggendorf*, C-188/92, ECLI :EU :C :1994 :90, consid. 26 ; Arrêt CJUE du 23 Février 2006, *Atzeni e.a.*, C—346/03 et C-529/03, ECLI :EU :C :2006 :130, consid. 93.
1454. Consid. 143 RGPD.

disposition des autorités se pose. Auront-elles les ressources suffisantes pour traiter les plaintes et assurer de facto le traitement effectif des recours des personnes concernées dans un délai raisonnable ? Quelles seront la qualité et l'efficacité de leur coopération ? Sauront-elles préparer des lignes directrices qui assureront une sécurité juridique tout en maintenant la flexibilité nécessaire pour s'adapter aux évolutions technologiques ? Des budgets des autorités de contrôle, de leur indépendance réelle, et de la volonté de coopération des autorités de contrôle dépendra la mise en œuvre cohérente du Règlement au sein de l'Union. Le Comité participera à l'élaboration d'une jurisprudence européenne en matière de protection des données, qui aura valeur contraignante pour toutes les autorités.

1729 Le Règlement met en place un recours *a posteriori* des décisions prises par les autorités nationales. Il s'agit d'une démarche de coopération dont l'efficacité demande à être prouvée. Compte tenu de l'impact des avis et des décisions du Comité européen sur les pays européens, il est essentiel qu'ils reflètent une pesée des intérêts en présence, au sens de la jurisprudence de la Cour de Justice de l'Union européenne.[1455]

1730 Si le Comité européen vise à harmoniser l'interprétation des dispositions du RGPD, en publiant des opinions et des lignes directrices, il n'est pas certain que l'objectif puisse être atteint compte tenu du nombre de publications, de leur longueur et du langage adopté [1456].

1731 Si l'intention d'une unité d'interprétation du RGPD est louable, la doctrine soulève«le risque d'un découragement des autorités nationales de protection, du fait de leur perte de souveraineté et la perte d'une émulation entre les diverses interprétations qui s'est révélée bénéfique dans le passé [1457].

1455. Arrêt CJUE du 24 septembre 2019, *Google L.L.C c. CNIL*, C-507-17, ECLI :EU :C :2019 :772, consid. 60.

1456. Poullet, *La vie privée à l'heure de la société du numérique*, p. 99.

1457. *Idem*, p. 95 ss, voir « Le régime actuel de protection des données et son adéquation aux enjeux du digital ».

Troisième partie

Le développement du droit de la protection des données en Suisse

En Suisse, la protection de la sphère privée est consacrée par l'art. 13 Cst. féd. du 18 avril 1999. Cet article garantit à toute personne le droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications (al. 1). Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent (al. 2). Cet article accorde un droit fondamental à l'auto-détermination informationnelle, soit le droit de ne pas accepter un traitement de données qui ne correspond pas à la volonté exprimée [1458]. 1732

L'art. 36 est dispose que seule une base légale, ou une restriction proportionnée au but visé et justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui justifient la restriction de ce droit fondamental. 1733

En droit privé (art. 28ss CC), toute personne subissant une atteinte illicite à sa personnalité est fondée à agir en justice pour sa protection non seulement contre le responsable, mais également contre toute personne qui y participe. Une atteinte est considérée comme illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public ou par la loi. 1734

Le traitement des données à caractère personnel constitue une atteinte particulière à sa sphère privée. Le droit de la protection des données encadre donc cette activité. 1735

La LPD est entrée en vigueur le 1er juillet 1993. Elle est actuellement en cours de révision afin de consolider les droits des personnes concernées et renforcer la responsabilité de celui qui traite des données personnelles (pour tenir compte du RGPD et de la Convention 108 révisée). Elle se veut technologiquement neutre. 1736

Le champ d'application de la LPD est large puisque cette loi concerne les traitements de données effectués par l'administration fédérale et par les personnes privées. La LPD met en œuvre la protection de la sphère privée reconnue par l'art. 13 Cst féd. pour le secteur public et par l'art. 28ss CC pour le secteur privé. 1737

La Suisse n'a pas adhéré à l'Union européenne (UE) et a privilégié la voie bilatérale pour préserver son indépendance institution- 1738

1458. Métille Sylvain / Arasteh Yasmine, *Le Règlement général sur la protection des données et les assureurs privés suisses*, in : Jahrbuch SGHVR = Annuaire SDRCA 2018, pp. 111-142.

nelle [1459]. La Suisse est liée à l'UE du fait des accords de Schengen et de Dublin [1460] et aux dispositions relatives à la protection des données du droit européen [1461].

1739 Si le Règlement n'est pas d'application directe en Suisse, certaines de ses dispositions sont applicables aux organisations établies en Suisse, dès lors que certaines conditions sont remplies (art. 3, al. 2 RGPD). Afin d'éviter l'application d'une double législation en matière de protection des données, il apparaît cohérent de modifier la LPD et d'intégrer les dispositions du RGPD en droit suisse.

1740 En outre, dans le cadre des accords de Schengen, la Suisse doit transposer la directive de l'UE sur la protection des données, dans sa législation interne [1462]. L'Union européenne a notifié la Suisse de cette obligation de transposition [1463].

1741 Le Conseil fédéral a mis en consultation le projet de révision totale de LPD en date du 21 décembre 2016 [1464]. Il s'inspire de plusieurs sources : Conv. 108 et son protocole additionnel, la directive euro-

1459. Près de vingt accords principaux et une centaine d'accords d'importance secondaire ont été conclus au fil des années.

1460. Conseil fédéral, *Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne (RS 0.362.31)*.

1461. Epiney Astrid / Nüesch Daniela (édit.), *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, 1e éd., Zürich 2016, p. 76.

1462. Parlement européen et Conseil de l'UE, *Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2016, p. « » (01/04/2020), pp. 89-131.

1463. Mission de la Suisse auprès de l'Union européenne, *Echange de notes entre la Suisse et l'Union européenne du 1er septembre 2016 entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (Développement de l'acquis de Schengen)*, in : OFJ (https ://www.bj.admin.ch/), Berne 2016, p. « https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/notenaustausch-f.pdf » (17/10/2019).

1464. Conseil fédéral, *Renforcer le contrôle sur ses propres données et rendre leur traitement plus transparent*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2016, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques / communiques - conseil - federal . msg - id - 65055 . html » (01/11/2019).

péenne 2016/680 (UE) et le Règlement européen.

Jean-Philippe Walter, Préposé suppléant à la protection des données et à la transparence soutient cette évolution : « Nous avons tout intérêt à être proche du règlement européen. L'échange de données entre l'UE et un État tiers ne peut en principe se faire que si ce pays assure un niveau de protection adéquat [1465]». 1742

La Suisse bénéficie d'une décision d'adéquation des législations, octroyée par la Commission européenne. Cette décision garantit la licéité des transferts de données à caractère personnel entre la Suisse et l'Union Européenne. Afin de conserver cette décision d'adéquation, la Suisse doit veiller à intégrer dans son droit interne les législations européennes pertinentes. Le groupe de travail de l'article 29 et la Cour de justice de l'Union européenne sont venus préciser les exigences du maintien d'une décision d'adéquation. Dans l'arrêt Schrems, la Cours indique que le niveau de protection doit être « substantiellement équivalent au niveau de protection des données dans l'Union européenne [1466]». Dans ses lignes directrices, le groupe de travail de l'art. 29 indique qu' il « convient de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données [1467]». Ainsi le contenu des règles et le moyen de garantir leur application effective seront au coeur de l'évaluation de la Commission européenne. L'article 45, al.2 RGPD définit les éléments dont la Commission européenne doit tenir compte lorsqu'elle évalue le caractère adéquat du niveau de protection dans un 1743

1465. Walter Jean-Philippe, *La protection des données n'est pas un frein à l'innovation*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2017, p. « https: / / www . letemps . ch / opinions / protection - donnees - nest - un - frein - linnovation » (01/11/2018).

1466. Arrêt CJUE du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14, ECLI :EU :C :2015 :650, consid. 52.

1467. Groupe de Travail de l'Article 29, *Critères de références pour l'adéquation - Adoptés le 28 novembre 2017, Version révisée et adoptée le 6 février 2018 (WP 254 rev.01)*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 » (01/04/2020), p. 4.

pays tiers ou une organisation internationale [1468].

1744 Il s'agit d'un problème majeur pour la Suisse : adapter à l'avenir sa législation au Règlement, et continuer ainsi à bénéficier de la décision d'adéquation. Selon nous, les deux buts du Règlement ne peuvent être mis au même niveau et poursuivis ensemble que par la mise en place d'un contrôle a posteriori réellement effectif, afin d'assurer une réelle libre circulation des données et la responsabilité des acteurs économiques.

1745 Dans cette partie, il est précisé ce que signifie un recours juridictionnel effectif contre les responsables de traitement. Cette explication est donnée en faisant référence au droit américain et européen de la concurrence, en particulier le concept de private enforcement qui s'est imposé en droit antitrust. Ces explications sont présentées dans la partie consacrée au développement du droit de la protection des données en Suisse, afin d'expliquer que les modifications du droit suisse dans le projet de LPD révisé sont nettement insuffisantes, si l'on prend la mesure de ce que met en place le Règlement. La mise en place d'une véritable class action dans le domaine de l'action civile des personnes physiques contre les responsables de traitement est particulièrement importante, dès que l'on voit l'importance pour les consommateurs et les personnes physiques d'avoir en main un instrument qui ne dépend pas de décisions publiques et donc de considérations politiques, mais seulement des tribunaux civils. Une telle action civile est la clé de voûte qui permet au système de la mise à égalité des deux buts du Règlement d'exister.

1468. *Ibidem.*

Chapitre 1: Le projet de LPD révisée

§1 Historique

La révision de la LPD s'inscrit dans un contexte économique et technologique en pleine mutation, dans lequel les données personnelles sont au cœur des enjeux stratégiques des acteurs publics et privés. 1746

De la modernisation du cadre légal suisse et de sa prise en compte des dispositions du RGPD, dépend la compétitivité des entreprises suisses sur le marché européen. La Suisse n'est plus attractive sur le plan légal car sa législation sur la protection des données date de 1992. Elle ne garantit pas un niveau de protection des données adéquat en comparaison avec la législation européenne. 1747

L'introduction d'une action civile en droit européen contre le responsable du traitement ou le sous-traitant, de manière individuelle ou collective constitue un changement de paradigme. Aménagée de façon à devenir un instrument aussi efficace et facile d'utilisation que possible, notamment par l'introduction de la possibilité de *class action*, il importe d'examiner comment garantir la mise en œuvre effective du droit de la protection des données. Une analyse comparée entre le droit de la concurrence et le droit de la protection des données, en droit américain, droit européen et droit suisse s'avère précieuse. Cette analyse conduira à mieux cerner les notions juridiques de Private Enforcement et du Public Enforcement, issus du droit de la concurrence, et leur application en droit suisse de la protection des données. 1748

I. Les étapes de la révision

Le projet de LPD révisée prévoit une révision totale de la LPD. Il nécessite une révision partielle des lois sectorielles applicables au domaine de la coopération policière et judiciaire instaurée par Schengen ainsi qu'une révision partielle de certaines lois fédérales 1749

induites par la révision de la LPD [1469].

1750 Du point de vue économique, la mise en conformité permet de conserver l'accès au marché européen. Du point de vue politique, elle a pour but de faciliter les négociations entre la Suisse et l'UE. Du point de vue juridique, elle constitue un enjeu stratégique pour le maintien de la décision d'adéquation des législations prise par la Commission européenne. Du contenu de la LPD révisée et de son caractère adéquat avec la législation européenne dépendra le maintien, la modification ou l'abrogation de la décision d'adéquation prise par la Commission européenne à l'égard de la Suisse.

1751 Le Conseil fédéral a présenté le 15 septembre 2017 son projet de révision de la LPD. Au printemps 2019, la Commission européenne a débuté l'évaluation du niveau de protection des données de la Suisse. Cette évaluation fait suite au jugement négatif de la Commission européenne, en mars 2019, concernant la densité des contrôles de la Suisse et sa dotation insuffisante dans le cadre de l'évaluation Schengen [1470].

1752 Comment expliquer cette situation ? Pour la comprendre, il nous faut examiner l'historique du projet de modernisation de la législation suisse de la protection des données.

1753 Le 9 décembre 2011, le Conseil fédéral a approuvé un rapport sur l'évaluation de la LPD et a chargé le Département fédéral de justice et police (DFJP) d'examiner l'opportunité de renforcer la législation en matière de protection des données, en tenant compte des résultats de l'évaluation et des développements en cours au sein de l'UE et du Conseil de l'Europe, et de faire des propositions concernant la marche à suivre avant la fin de 2014 [1471].

1754 Un groupe de travail a été constitué de septembre 2012 à octobre

1469. Epiney / Nüesch, *Die Revision des Datenschutzes in Europa und die Schweiz = La révision de la protection des données en Europe et la Suisse*, p. 148.

1470. PFPDT, *26e rapport d'activités 2018/2019 : La Suisse doit maintenir son niveau de protection des données*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2019, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75448.html » (27/06/2019).

1471. OFJ, *Renforcement de la protection des données*, in : OFJ (https ://www.bj.admin.ch/), Berne s.a., p.« https : / / www . bj . admin . ch / bj / fr / home / staat / gesetzgebung / datenschutzstaerkung . html » (27/06/2019).

2014 pour définir les mesures législatives requises [1472].

Le 1er avril 2015, le Conseil fédéral a pris connaissance du rapport du groupe d'accompagnement et des propositions du DFJP. Il a mandaté le DFJP pour préparer un avant-projet de révision de la LPD avant la fin du mois d'août 2016. La révision devait d'une part renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies et d'autre part tenir compte des réformes du Conseil de l'Europe et de l'Union européenne en la matière [1473]. Ce dernier élément est explicitement demandé par le Conseil fédéral [1474]. 1755

En 2015, l'Office fédéral de la Justice, conjointement avec le Secrétariat d'État à l'économie, a mandaté l'entreprise Pricewaterhause-Cooper (ci-après « PwC ») pour qu'elle procède à une étude d'impact de la nouvelle réglementation européenne, dans le cadre de la révision de la loi fédérale sur la protection des données [1475]. 1756

L'entreprise de conseil PwC a procédé à une enquête en ligne et a analysé les résultats obtenu. 1757

Il importe de relever que ce document n'est plus publié contrairement á ce que relève l'OFJ dans son rapport explicatif [1476]. Cette absence de publication est particulièrement problématique du fait de l'impact de cette étude sur le contenu de l'avant-projet. Cette étude devrait être publiée car elle repose sur une obligation légale de l'art. 170 Cst. et 141, al. 2 de la loi du 13 décembre 2002 sur l'As- 1758

1472. OFJ, *Esquisse d'acte normatif relative à la révision de la loi sur la protection des données : Rapport du groupe d'accompagnement Révision LPD*, in : OFJ (https ://www.bj.admin.ch/), Berne 2014, p. « https://www.bj.admin.ch/content / dam / data / bj / staat / gesetzgebung / datenschutzstaerkung / ber - normkonzept-f.pdf » (27/06/2019).

1473. OFJ, *Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales*, in : OFJ (https ://www.bj.admin.ch/), Berne 2016, p. « https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-f.pdf » (27/06/2019).

1474. Vers un renforcement de la protection des données, Communiqué de presse du 01 avril 2015.

1475. Hofmann Susanne / Meyer Michael Adrian, *Que signifie la révision pour les entreprises ?*, in : La Vie économique 2016/11, pp. 59-61 ; OFJ, *Rapport explicatif du 21 décembre 2016*, p. 23.

1476. OFJ, *Rapport explicatif du 21 décembre 2016*, p. 107.

semblée fédérale (LParl) [1477].

1759 Dans son rapport, PwC a relevé l'importance de la révision de la LPD pour sensibiliser la société suisse et les acteurs économiques à l'importance de la protection des données à caractère personnel. L'entreprise a considéré que cette réforme « allait renforcer l'attractivité de la place économique suisse tout en améliorant la fiabilité, la sécurité juridique et l'égalité dans les traitements de données à caractère personnel ».

1760 Tout en soutenant ce projet de réforme, l'analyse d'impact du cabinet PwC a identifié le risque d'une augmentation des coûts pour la Confédération et les entreprises. Cette augmentation résulte du besoin de mettre en place des processus spécifiques pour les entreprises en lien avec le renforcement des droits des personnes : droit d'accès, droit de rectification auprès des tiers, analyses d'impact, amendement des contrats des sous-traitants. PwC a également anticipé la conversion de certains modèles d'affaires basés sur des services « gratuits » en services payants, du fait de la difficulté croissante de traiter des données personnelles de manière licite pour les acteurs économiques.

1761 Le 16 août 2019, la Commission des institutions politiques du Conseil National a terminé l'examen du projet de LPD. Ce projet a été accepté difficilement grâce à la voix prépondérante du Président (neuf voix contre neuf et sept abstentions) [1478].

1762 Une faible majorité a adhéré au projet du Conseil fédéral et suggère quelques modifications. Un premier groupe minoritaire (Rutz Gregor, Addor, Brand, Buffat, Burgherr, Glarner, Pantani, Reimann Lukas, Steinemann) a refusé le projet du Conseil Fédéral et renvoyé le projet en demandant qu'il soit « épuré autant que possible en accordant notamment un maximum de liberté et de souplesse aux entreprises et aux collectivités qui n'opèrent qu'en Suisse et en allégeant leur cahier des charges. Les prescriptions de l'Union européenne ne doivent être reprises que lorsque cela est indispen-

1477. Loi sur l'Assemblée fédérale (Loi sur le Parlement, LParl) du 13 décembre 2002 (Etat le 2 décembre 2019), RS 171.10, RO 2003 3543.

1478. Parlement suisse, *Réforme de la protection des données : fin de l'examen du projet - Communiqué de presse du 16 août 2019*, in : Parlement suisse (https ://www.parlament.ch/), Berne 2019, p. « https : / / www . parlament . ch / press - releases / Pages / mm - spk - n - 2019 - 08 - 16 - a . aspx ? lang = 1036 » (22/12/2019).

sable [1479]». Cette minorité voulait réduire la protection de la personnalité de manière radicale et donner la priorité aux acteurs économiques et à la libre circulation des données, sans tenir compte de la protection des personnes physiques dont les données personnelles sont traitées. Cette approche visait à faire basculer la Suisse dans une ère «post-privacy».

Un second groupe minoritaire (Wermuth) proposait le renvoi du projet à la commission, avec le mandat « d'élaborer un projet tenant compte au moins des exigences suivantes : 1763

— Compatibilité avec la convention STE n° 108 (Conseil de l'Europe).

— Garantie de la reconnaissance de l'équivalence avec le règlement (UE) 2016/679 — Compatibilité avec les accords de Schengen.

— Garantie d'un niveau de protection au moins égal à celui conféré par la LPD en vigueur ».

Cette recommandation permettrait à la Suisse de mettre sa législation au même niveau que les États voisins et de l'adapter aux évolutions technologiques dans le sens d'une pesée des intérêts en présence de tous les acteurs. 1764

De l'avis du Préposé fédéral à la protection des données, cette dilution de la protection des données décidée par le Conseil national est problématique compte tenu de la nécessaire décision d'adéquation de la Commission européenne. 1765

Durant sa session d'hiver, le Conseil des États (CIP-CE) a examiné les propositions de modification du projet de LPD révisée [1480]. La Commission des institutions politiques du Conseil des Etats (CIP-CE) a achevé l'examen par article du projet de loi sur la protection 1766

1479. Propositions de modifications du projet de LPD révisée sur Parlement suisse, *17.059 : Loi sur la protection des données. Révision totale et modification d'autres lois fédérales - Propositions du Conseil fédéral du 15 septembre 2017, Projet de la Commission des institutions politiques du Conseil national du 16 août 2019*, in : Parlement suisse (https ://www.parlament.ch/), Berne 2017, p. « https://www.parlament.ch/centers/eparl/curia/2017/20170059/N3-1%20F.pdf » (30/08/2019).

1480. Parlement suisse, *Le Conseil des Etats examinera la loi sur la protection des données á la session d'hiver - Communiqué de presse du 20 novembre 2019*, in : Parlement suisse (https ://www.parlament.ch/), Berne 2019, p. « https://www.parlament.ch/press-releases/Pages/mm-spk-s-2019-11-20.aspx » (22/12/2019).

des données (17.059). Au vote sur l'ensemble, elle a adopté le projet à l'unanimité et transmis celui-ci à son Conseil, qui pourra l'examiner lors de la session d'hiver.

1767 Le Conseil des Etats a ainsi achevé la consultation concernant la révision totale de la Loi sur la protection des données (LPD). Il a largement repris les propositions d'amélioration de sa commission face à la version du conseil national.

1768 Le Conseil fédéral voulait un projet économiquement compatible et flexible, un projet qui soit fondé sur le risque, c'est-à-dire qui ne soit pas basé sur la taille de l'entreprise mais sur le type et la nature des données traitées. En effet, une entreprise telle qu'une boucherie ou une menuiserie locale ne dispose pratiquement pas de données sensibles. Un petit cabinet médical, par contre - il n'est pas nécessaire qu'il s'agisse d'un groupe d'entreprises - peut très bien avoir des données sensibles sur ses patients. Il existe également des fournisseurs de services de Cloud, par exemple, qui présentent un risque plus élevé. De cette manière, on peut prendre en considération les entreprises où le traitement des données ne joue qu'un rôle mineur.

1769 Le texte adopté maintient le montant des sanctions à CHF 250 000, en cas de violation des dispositions légales, ce qui justifierait selon nous fait courir un risque de retrait de la décision d'adéquation attribuée par la Commission européenne.

1770 La CIP-CE a décidé de réintroduire les données sur les opinions et activités syndicales dans la liste des données personnelles sensibles, lesquelles bénéficient d'un niveau de protection particulièrement élevé (art. 4, let. c, ch. 1, P-LPD), évitant ainsi de créer une divergence avec la réglementation UE sur ce point.

1771 La CIP-CE a également décidé de supprimer l'exception au devoir d'informer en cas d'efforts disproportionnés, qui avait été introduite par le Conseil national (art. 18, al. 1, let. e, P-LPD).

1772 La CIP-CE a en outre renoncé à introduire un catalogue exhaustif des informations à fournir en cas d'exercice du droit d'accès, comme le souhaitait le Conseil national (art. 23, al. 2, P-LPD).

1773 En ce qui concerne les sanctions pénales, la CIP-CE a proposé de sanctionner le non-respect intentionnel des exigences en matière

de sécurité des données.

Elle a retenu la notion de «profilage à risque élevé» et prévoit une protection renforcée lorsqu'un traitement de données tombe dans cette catégorie. La CIP-CE considère par ailleurs que les droits des personnes faisant l'objet d'une évaluation de leur solvabilité doivent être renforcés : à l'unanimité, elle a notamment limité dans ce contexte la possibilité de traiter des données datant de plus de 5 ans ainsi que des données concernant des mineurs. 1774

Si la version révisée de la LPD reste éloignée des dispositions du RGPD, la signature par la Suisse du Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des données à caractère personnel (Convention 108) [1481] démontre la volonté de la Suisse de participer ou tout au moins de ne pas être exclu de l'effort d'harmonisation du cadre juridique de la protection des données au niveau international. 1775

II. Avant-projet

L'avant-projet de révision a étudié l'impact économique de la révision de la LPD sur la concurrence en Suisse. Il a souligné que « si la Suisse perdait son statut de pays doté d'un niveau adéquat de protection des données, ou si elle adoptait des réglementations qui lui sont propres ou qui sont plus restrictives que le droit de l'Union européen », alors la Suisse serait moins compétitive sur le plan économique [1482]. 1776

L'avant-projet de révision de la LPD a été accueilli favorablement par le Préposé fédéral à la protection des données [1483]. 1777

Conformément au mandat du Conseil fédéral, il a intégré les dispositions de la Conv. 108 [1484], du Règlement général sur la protection des données et de la directive (UE) 2016/680 du 27 avril 2016, sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des 1778

1481. Conseil fédéral, *Le Conseil fédéral signe la nouvelle Convention du Conseil de l'Europe sur la protection des données*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2019, p. « https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76861.html » (22/12/2019).
1482. OFJ, *Rapport explicatif du 21 décembre 2016*, point 1.7.3.
1483. PFPDT, *24ème Rapport d'activités*, p. 15.
1484. Conseil fédéral, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1)*.

fins de détection et de prévention des infractions pénales, d'enquête et de poursuites en la matière [1485].

A. Les définitions

1779 Les définitions de la Conv. 108 et du Règlement européen ont été reprises dans l'avant-projet de révision de la LPD. Ce dernier a en particulier substitué les notions de responsable du traitement au concept de maître du fichier et la notion d'activité de traitement à la notion de fichier.

B. Les principes

1780 Les principes de l'avant-projet de LPD révisée demeurent inchangés. Ils sont très proches de ceux de la Conv. 108 et du Règlement : licéité, proportionnalité, finalité, exactitude des données, notion de consentement demeurent des éléments essentiels.

1781 Cependant, et c'est un point essentiel, l'avant-projet n'a pas repris la notion de responsabilité structurelle des responsables du traitement et des sous-traitants, qui figure dans le Règlement, ce qui limite la portée de cette réforme. Cette carence est source d'insécurité juridique pour les personnes concernées et fait courir un risque politique majeur à la Suisse concernant le maintien de la décision d'adéquation octroyée à la Suisse par la Commission européenne. On a vu en effet à quel point la notion de contrôle *a posteriori* avec les deux mécanismes de Public et de Private Enforcement est essentielle pour remplir les buts du Règlement, que sont la responsabilité des acteurs économiques et la libre circulation des données (voir paragraphe 661).

C. Le responsable du traitement

1782 L'avant-projet renforce les obligations du responsable du traitement, en cohérence avec le Règlement européen et la Convention 108 modernisée.

1783 L'avant-projet crée quatre nouvelles obligations principales : tout d'abord une obligation d'annonce des violations en matière de protection des données (art. 17 LPD), ensuite une obligation de conduire des analyses d'impact (art. 16 AP) pour les traitements présentant

1485. Parlement européen et Conseil de l'UE, *Directive (UE) 2016/680 du 27 avril 2016.*

des risques élevés pour les droits et libertés des personnes concernées, également une obligation de documenter les traitements effectués (registre des activités de traitement, art. 19 AP). Le responsable du traitement devra enfin tenir compte de la protection des données « dès la conception » (Privacy by Design) des systèmes informatiques et « par défaut » (privacy by default) (art. 18 AP).

Tout en renforçant les obligations du responsable du traitement, l'avant-projet conserve les obligations de la LPD (art. 7) actuelles. On peut citer l'obligation de sécuriser les données [1486], en cohérence avec la Conv. 108, le Règlement [1487] et la directive (UE) 2016 / 680 [1488]. Les responsables du traitement et les sous-traitants ont toujours l'obligation de protéger les données personnelles contre tout traitement non autorisé et toute perte, par des mesures organisationnelles et techniques appropriées (Voir paragraphe 941). La notion de perte intègre aussi la destruction des données. Les mesures prises pour sécuriser le traitement de données à caractère personnel sont identiques à celles de la législation européenne. Elles comprennent la pseudonymisation, le chiffrage de données, des garanties pour assurer la confidentialité, l'intégrité et la disponibilité des systèmes et des services de traitement. Elles doivent permettre de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique. L'efficacité des mesures techniques et organisationnelles sera testée, analysée et évaluée régulièrement grâce au développement de procédures spécifiques. 1784

L'avant-projet conserve l'obligation faite au responsable du traitement d'informer (art. 13 AP) la personne concernée de la collecte de ses données à caractère personnel, afin qu'elle puisse faire valoir ses droits [1489] (Voir paragraphe 1075). Cette obligation d'information est étendue aux décisions automatisées (art. 15 AP). Le responsable du traitement et le sous-traitant doivent aussi informer « les destinataires auxquels les données ont été communiquées de toute demande de rectification, effacement, ou destruction des données personnelles, de toute violation de la protection des données ainsi que de toute limitation du traitement (art. 19 AP) ». L'obligation d'informer n'est pas nouvelle. Elle figure également dans la 1785

1486. art. 11 de l'avant-projet.
1487. art. 32 RGPD.
1488. art. 29 de la directive.
1489. art. 13 de l'avant-projet (fusion des arts. 14 et 18a de la LPD).

Conv. 108 [1490], dans le Règlement européen [1491] et la directive (UE) 2016/680 [1492]. La LPD actuelle pose aussi une obligation d'information. Celle-ci est renforcée avec le projet de LPD révisée, car les personnes concernées doivent être informées au moment de la collecte.

1786 Lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement doit informer la personne concernée de l'existence du traitement et des données concernées (ou catégories de données).

1787 Il existe quelques exceptions au devoir d'information du responsable du traitement. La première exception concerne les cas où la personne concernée dispose déjà des informations. La seconde hypothèse concerne les cas où les données personnelles n'ont pas été collectées auprès de la personne concernée. La troisième exception concerne les restrictions au droit d'information, si une loi le prévoit [1493] ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés [1494].

1788 Dans les cas précités, le responsable du traitement peut renoncer à la communication des informations, la restreindre ou la différer. Conformément à la jurisprudence de la CJUE, il doit procéder à une pesée des intérêts en présence, dont les modalités diffèrent selon que ce dernier est un particulier ou un organe fédéral. La liste des cas de limitation est exhaustive et doit être interprétée de manière restrictive.

1789 Les dispositions de l'avant-projet relatives aux décisions individuelles prises sur une base automatisée [1495] remplissent les exigences du protocole additionnel de la Conv. 108 [1496], de la directive (UE) 2016 / 680 [1497]. Le Règlement (UE) 2016/679 contient une disposition similaire [1498] (Voir paragraphe 1124).

1790 En application du droit d'être entendu, le responsable du traitement doit donner la possibilité de faire valoir son point de vue sur la déci-

1490. art. 7 bis de la Convention.
1491. art. 13 RGPD.
1492. art. 13 de la directive.
1493. art. 4, let. a de l'avant-projet ; art. 14, al. 2, let. a de l'avant-projet.
1494. art. 14, al. 2, let. b de l'avant-projet.
1495. art. 15 de l'avant-projet.
1496. art. 8 de l'avant-projet.
1497. art. 3, al. 3 et 11 de l'avant-projet.
1498. art. 4, par. 3 et 22 RGPD.

sion individuelle prise uniquement sur une base automatisée et sur les données traitées. À titre d'exception, l'avant-projet précise que le devoir d'informer et d'entendre la personne concernée ne s'applique pas lorsque la décision individuelle automatisée est prévue par la loi.

Le droit à une intervention humaine dans la prise de décision algorithmique et la possibilité pour la personne concernée d'apporter des compléments lors de la procédure de prise de décision par les algorithmes, constituent des garanties indispensables pour la personne qui supporte les conséquences d'une décision prise sur une base uniquement automatisée. 1791

Lorsque le responsable du traitement ne permet pas à la personne concernée de faire valoir son point de vue, cette dernière peut faire valoir son droit d'opposition et son droit d'accès (art. 20 de l'avant-projet). La loi ne fixe pas le moment auquel l'information et l'audition doivent avoir lieu. En conséquence, la personne concernée peut être informée et entendue avant ou après la prise de décision automatisée. Il est ainsi notamment possible de lui notifier une décision individuelle automatisée — qui sera désignée comme telle — et de l'entendre dans le cadre de l'exercice du droit d'être entendu, ou lors d'une procédure de recours, pour autant qu'il n'en résulte pas de frais supplémentaires (par ex. des frais de procédure) pour elle. 1792

Le droit d'explication prévoit notamment la communication à la personne concernée d'informations utiles concernant la logique sous-jacente de l'algorithme décisionnel. La jurisprudence viendra préciser les éléments indispensables à considérer [1499]. Une formation des juges ou une coopération interdisciplinaire entre les juges et les experts en intelligence artificielle s'avère indispensable pour soutenir les juges dans leur compréhension des recommandations algorithmiques. 1793

D. Le sous-traitant

L'avant-projet de LPD révisée a repris les dispositions du Règlement relatives aux sous-traitants et a renforcé leurs obligations, de manière similaire aux responsable du traitement (voir paragraphe 1794

1499. Goodman / Flaxman, *Right to Explanation*, pp. 50-57.

1020).

1795 En conformité avec le Règlement européen (art. 30 RGPD), l'avant-projet crée l'obligation pour les organes fédéraux de tenir un registre des activités de traitement [1500].

1796 Selon l'avant-projet, le responsable du traitement doit s'assurer que le sous-traitant est en mesure de garantir non seulement la sécurité des données, mais aussi l'exercice effectif des droits de la personne concernée [1501]. Cette extension est exigée par la directive (UE) 2016/680 [1502]. Le Règlement (UE) 2016/679 prévoit les mêmes dispositions [1503].

1797 Dans la lignée du Règlement, l'art. 5, al. 3 du projet de LPD révisée prévoit désormais que le sous-traitant ne peut lui-même sous-traiter un traitement qu'avec l'accord écrit préalable du responsable du traitement. Ceci constitue une innovation.

E. Les personnes décédées

1798 Le champ d'application du Règlement européen exclut toute disposition relative aux personnes décédées. L'avant-projet de LPD révisée introduit quant à lui des dispositions spécifiques sur ce thème.

1799 Il règle notamment le droit d'accès aux données personnelles d'une personne décédée [1504]. Un droit d'accès aux données d'une personne décédée est reconnu dans l'avant-projet en cas d'intérêt légitime, de mariage ou de partenariat enregistré, de concubinage ou en présence d'un exécuteur testamentaire. Cet accès requiert l'absence d'interdiction par le défunt de son vivant, l'absence d'intérêt prépondérant du responsable du traitement ou d'un tiers à la consultation.

F. L'autorité de contrôle

1800 L'avant-projet de LPD révisée améliore les possibilités de coopération avec d'autres autorités de contrôle en Suisse (cantonales) et à

1500. art. 36 de l'avant-projet de LPD.
1501. art. 7, al. 2 de l'avant-projet de LPD.
1502. art. 22, al. 1 de la directive (UE) 2016/680.
1503. art. 28, al. 1 RGPD.
1504. art. 12 de l'avant-projet de LPD et art. 16 P-LPD.

l'étranger (entraide administrative, art. 47 AP).

Le statut et l'indépendance du Préposé fédéral à la protection des données et à la transparence sont renforcés (art. 37 AP). 1801

Pour assurer son rôle de manière effective, le Préposé devrait cependant disposer de ressources et de moyens supplémentaires conséquents en adéquation avec l'ampleur de la transformation digitale en cours. 1802

Le Préposé devrait également disposer d'un budget autonome, à l'image du contrôle fédéral des finances ou de la nouvelle autorité de contrôle sur le service de renseignement de la Confédération. 1803

Ce budget devrait contribuer à éduquer et à sensibiliser la population aux technologies digitales et à leur impact sur la protection des données. 1804

Il soutiendrait les activités du Préposé fédéral à la protection des données dans le cadre de la coopération avec les autorités de contrôle de l'Union européenne. Dans la limite de ses prérogatives, il contribuerait au respect de la loi sur la protection des données. 1805

L'avant-projet renforce les pouvoirs du Préposé et lui octroie la possibilité de prendre des décisions contraignantes à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur demande. 1806

L'avant-projet donne la prérogative au Préposé d'encourager l'élaboration de bonnes pratiques (Best Practices) en coopération avec les milieux intéressés [1505]. Il lui octroie la possibilité d'approuver ou de reconnaître des règles contraignantes d'entreprises (Binding Corporate Rules, BCR) dans le cadre des transferts de données à l'étranger. De même, il lui donne le pouvoir d'édicter, de reconnaître ou d'approuver des clauses contractuelles types. 1807

1505. OFJ, *Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales : Synthèse des résultats de la procédure de consultation (10 août 2017)*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2017, p. « https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Rapport-resultats_fr.pdf » (02/04/2020), p. 4.

G. Les flux transfrontaliers

1808 Dans le cadre des flux transfrontaliers, l'avant-projet reprend en particulier le principe selon lequel des données ne peuvent être transmises à l'étranger, que si un niveau approprié de protection des données est garanti [1506]. En vertu de l'al. 2, des données peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que la législation de l'État concerné assure un niveau de protection adéquat. Cette disposition attribue explicitement la compétence au Conseil fédéral d'examiner l'adéquation de la législation étrangère en matière de protection des données.

1809 En l'absence d'une décision du Conseil fédéral, des données personnelles peuvent être communiquées à l'étranger, si un niveau « approprié » de protection des données personnelles est garanti [1507]. A l'instar du droit de l'Union européenne, l'avant-projet recourt à deux termes différents [1508]. Le terme « adéquat » est réservé pour qualifier la législation de l'État étranger.

1810 Le niveau de protection approprié peut également être assuré par un traité international [1509]. Par « traité international », on entend non seulement une convention internationale en matière de protection des données à laquelle l'État destinataire serait partie, telle que la Conv. 108 et son protocole additionnel, mais aussi tout autre accord international qui prévoit un échange de données entre États parties et qui répond en substance aux exigences de la Conv. 108. Il peut également s'agir d'un traité international conclu par le Conseil fédéral [1510].

1811 Un niveau de protection des données approprié peut également être assuré par des garanties ad hoc et standardisées agrées, établies par des instruments juridiquement contraignants et opposables. Le Règlement (UE) 2016/679 prévoit une réglementation analogue [1511]. Il en va de même pour la directive (UE) 2016/680 [1512].

1812 En l'absence de décision d'adéquation du Conseil Fédéral, des ga-

1506. art. 5, al. 2 de l'avant-projet de révision de la LPD.
1507. art. 5, al. 3, let. a à d de l'avant-projet de LPD.
1508. art. 5, al. 2 et 3 de l'avant-projet de LPD.
1509. art. 5, al. 3 let. a de l'avant-projet de LPD.
1510. art. 56, let. b de l'avant-projet de LPD.
1511. art. 46 RGPD.
1512. art. 37 RGPD.

ranties spécifiques [1513] doivent être fournies par le responsable du traitement. Il incombe au responsable du traitement de démontrer qu'il a pris toutes les mesures requises pour s'assurer d'un niveau de protection approprié et que le destinataire respecte les garanties [1514]. Il reste également responsable du préjudice qui pourrait résulter d'une violation des garanties prévues. Les garanties spécifiques peuvent être, dans le secteur privé, des clauses contractuelles convenues dans le cadre d'un contrat entre le responsable du traitement et le destinataire. Dans le secteur public, l'organe fédéral peut, lorsqu'il accorde sa coopération à un État étranger, lui fixer des conditions à respecter en matière de protection des données [1515].

1813 Des données peuvent également être communiquées à l'étranger moyennant des garanties standardisées. Ces garanties peuvent être élaborées soit par les personnes concernées ou les milieux intéressés, soit établies ou reconnues par le Préposé. Les organes fédéraux peuvent également recourir à ce type de garanties. La notion de « garanties standardisées » peut viser par exemple des clauses contractuelles types insérées dans le contrat conclu entre le responsable et le destinataire. Il peut également s'agir d'un code de conduite élaboré par le secteur privé auxquelles les personnes privées peuvent se soumettre volontairement. Les garanties doivent préalablement avoir été approuvées par le Préposé [1516]. Cette condition constitue un renforcement du droit en vigueur qui prévoit uniquement une obligation d'informer le Préposé [1517]. Elle correspond à l'exigence prévue à l'art. 12bis, al. 2 let. *b* du protocole additionnel à la Conv. 108.

1814 Le responsable du traitement qui décide de communiquer des données à l'étranger moyennant des garanties standardisées au sens de l'art. 5, al. 3, let. c, est présumé avoir pris toutes les mesures nécessaires pour garantir un niveau de protection adéquat. Toutefois, cette présomption ne le libère pas de toute responsabilité pour les préjudices qui pourraient résulter de la violation de ces garanties notamment par le destinataire des données. Il convient de prévoir dans l'ordonnance une obligation pour le Préposé de publier une liste des garanties standardisées établies ou reconnues, comme le

1513. art. 5, al. 3, let. b de l'avant-projet de révision de la LPD.
1514. art. 5, al. 3 let. b de l'avant-projet de LPD.
1515. art. 5, al. 3 let. b de l'avant-projet de LPD.
1516. art. 5, al. 3, let. c, ch. 1 de l'avant-projet.
1517. art. 6, al. 3 LPD.

prévoit du reste le droit en vigueur [1518].

1815 Des données peuvent également être communiquées à l'étranger moyennant des règles d'entreprise contraignantes, approuvées au préalable par le Préposé ou par une autorité chargée de la protection des données à l'étranger [1519]. Cette disposition remplace l'art. 6, al. 2, let. g, LPD. L'art. 5, al. 2, let. d se rapproche du droit de l'Union européenne qui prévoit, à l'art. 47 du Règlement (UE) 2016/679, que des données peuvent être communiquées entre les entités d'un groupe d'entreprises moyennant des règles d'entreprise contraignantes préalablement approuvées par l'autorité de contrôle de protection des données. L'approbation des règles d'entreprises est prévue à l'art. 57, par. 1 let. s du Règlement (UE) 2016/679. Le al. 3, let. d constitue un renforcement du droit en vigueur dans la mesure où les règles d'entreprises contraignantes doivent être approuvées. Le Préposé dispose d'un délai de six mois pour communiquer à la société concernée s'il approuve ou non les règles d'entreprise contraignantes qui lui ont été soumises (al. 5) [1520].

1816 Pendant ce laps de temps, aucune donnée ne peut être transmise à l'étranger. La décision du Préposé est susceptible de recours, mais aucune action en responsabilité ne peut être exercée pour obtenir le versement de dommages-intérêts, contrairement aux dispositions du Règlement.

III. La procédure de consultation

1817 La procédure de consultation a été ouverte le 21 décembre 2016 et s'est clôturée le 4 avril 2017 [1521]. Plus de deux cents commentaires ont été recueillis [1522].

1818 Le Préposé à la protection des données a relevé certaines différences terminologiques et matérielles par rapport au Règlement général sur la protection des données et à la Conv. 108 STE révisée du Conseil de l'Europe. Le Préposé estime que « nombre de ces différences ne sont pas judicieuses, en compliquant inutilement la situation des entreprises suisses et des services de l'administration

1518. art. 6, al. 3, OLPD.
1519. art. 5, al. 3, let. d, de l'avant-projet.
1520. OFJ, *Rapport explicatif du 21 décembre 2016*, p. 48.
1521. OFJ, *Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales*, pp. 1-79.
1522. *Idem*, p. 6.

qui sont directement soumis au Règlement général de l'UE [1523]».

Economie suisse et les associations du secteur informatique (ICTs- 1819
witzerland, SWICO, SwissICT) ont exprimé leur souhait d'une LPD révisée au contenu minimaliste.

Inversement, les associations de consommateurs et la conférence 1820
des Préposés suisses à la protection des données (Privatim) se sont exprimées en faveur du renforcement des droits des personnes concernées, du rapprochement de la LPD suisse avec les dispositions du Règlement (portabilité, charge de la preuve), en particulier concernant les prérogatives et l'indépendance du Préposé fédéral [1524].

Le Parlement est compétent pour définir l'étendue de la surveillance 1821
que la Confédération exercera à l'avenir dans le domaine de la protection des données et le degré d'adaptation au droit de l'UE [1525].

IV. La prise de position du Conseil Fédéral

La procédure de consultation a donné lieu à la rédaction d'un rap- 1822
port du Conseil fédéral et à la publication du message de la loi révisée sur la protection des données, en date du 15 septembre 2017 [1526].

Le projet de loi révisée reprend les exigences de la directive euro- 1823
péenne 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins pénales [1527]. En effet, il importe que la Suisse puisse remplir ses engagements au titre des accords Schengen. Il s'agit en outre d'harmoniser le droit suisse avec le Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Enfin, la révision a permis à la Suisse de signer en novembre 2019 la nouvelle version de la convention du Conseil de l'Europe pour la protection des per-

1523. PFPDT, *Message du 15 septembre 2017 concernant la révision totale de la loi fédérale sur la protection des données : appréciation du PFPDT*, in : Conseil fédéral (https ://www.edoeb.admin.ch/), Berne 2017, p. « https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news/zur-botschaft-ueber-die-totalrevision-des-datenschutzgesetzes-de.html » (02/04/2020).
1524. *Ibidem.*
1525. Conseil fédéral, *Helsana+ : Le jugement entre en force.*
1526. Message du 15 septembre 2017 concernant la révision totale de la loi fédérale sur la protection des données et sur la modifications d'autres lois fédérales (17.059), FF 2017 p. 6565 ss.
1527. *Idem*, p. 6668.

sonnes à l'égard du traitement automatisé des données à caractère personnel [1528].

1824 La réforme de la LPD a été examinée par le Conseil National. Dans un premier temps, le Conseil National a scindé le projet en deux, en date du 12 janvier 2018 [1529]. La priorité a été donnée à la transposition de la directive UE 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes dans le domaine du droit pénal. Le Conseil National a indiqué que la réforme complète de la LPD serait abordée dans un second temps (et « sans contrainte de temps [1530] »).

1825 La directive UE 2016/680 fait partie du développement de l'acquis de Schengen et ont été reprises par la Suisse dans son droit interne. Le champ d'application de cette directive est limité aux personnes publiques. Les traitements effectués par des personnes privées sont exclus. Depuis le 1er mars 2019, toutes les dispositions concernant le traitement des données dans le cadre de la coopération Schengen en matière pénale sont entrées en vigueur [1531].

1826 La Suisse a ainsi rempli ses obligations au titre de l'acquis de Schengen.

1827 En outre, l'UE a également modernisé et renforcé son cadre général de protection des données en mai 2018 avec le RGPD. Celui-ci ne constitue pas un développement de l'acquis de Schengen. Il ne doit donc pas nécessairement être adopté par la Suisse. Un rapprochement du droit suisse de la protection des données avec le RGPD est toutefois nécessaire pour que la Suisse continue d'être reconnue par l'UE comme un pays tiers disposant d'un niveau de protection des données approprié.

1828 Conformément à la législation européenne, les données à caractère personnel ne peuvent être transférées vers d'autres pays sans obs-

1528. Conseil fédéral, *Le Conseil fédéral signe la nouvelle Convention du Conseil de l'Europe sur la protection des données.*

1529. Parlement suisse, *Législation sur la protection des données : Révision en deux étapes - Communiqué de presse du 12 janvier 2018*, in : Parlement suisse (https ://www.parlament.ch/), Berne 2018, p. « https : / / www . parlament . ch / press - releases / Pages / mm - spk - n - 2018 - 01 - 12 . aspx ? lang = 1036 » (01/11/2019).

1530. *Ibidem.*

1531. OFJ, *Renforcement de la protection des données.*

tacles supplémentaires que si ces pays disposent d'un niveau de protection des données équivalent à celui de l'UE.

Cela signifie que seule une décision d'adéquation de l'UE permettra aux entreprises suisses d'être traitées sur un pied d'égalité avec les entreprises établies dans l'UE. Ce n'est qu'à cette condition que les entreprises suisses bénéficieront également d'une libre circulation des données personnelles. 1829

L'UE examine actuellement le niveau de protection des données en Suisse et dans d'autres pays tiers qui ont une décision d'adéquation de l'UE. Cette évaluation devrait être terminée d'ici la fin mai 2020. Une perte ou une suspension de la décision d'adéquation aurait des inconvénients considérables pour l'économie suisse. Dans un tel cas, les entreprises de l'UE ne seraient autorisées à communiquer des données personnelles à leurs partenaires commerciaux suisses que dans des conditions plus difficiles. Si les sociétés suisses fournissent des données, elles devront établir des déclarations de garantie correspondantes si la constatation d'adéquation n'était plus applicable. Cela entraînerait une charge administrative supplémentaire considérable, en particulier pour les PME. Contrairement à ce que l'on pourrait croire à première vue, cela ne désavantagerait pas simplement les groupes actifs au niveau international. 1830

Si la Suisse n'adaptait pas son droit au niveau européen de protection des données, il existerait une inégalité de traitement entre les citoyens suisses et les citoyens européens. La vie privée des citoyens suisses serait moins bien protégée que dans le reste de l'Europe. 1831

Le Conseil de l'Europe a également modernisé sa convention sur la protection des données en 2018. Pour la Suisse, l'acte juridique modernisé du Conseil de l'Europe est très important tant pour la protection de la sphère privée que pour l'accès au marché international. En outre, la convention 108 sur la protection des données joue un rôle important dans l'évaluation de l'adéquation de l'UE. Le Conseil fédéral a donc signé le protocole à la Convention modernisée sur la protection des données le 21 novembre 2019. Lors de sa réunion du 6 décembre, il a également adopté la dépêche sur la convention modernisée afin que le Parlement puisse décider de son approbation dans les meilleurs délais. Ces mesures représentent également un signal positif important en ce qui concerne 1832

l'évaluation de l'adéquation de l'UE.

1833 Ces mesures sont importantes pour que les exigences essentielles de l'UE pour un niveau adéquat de protection des données puissent également être respectées.

1834 La réforme complète de la LPD concerne les traitement de données par des personnes privées.

1835 Le Conseil national a adhéré au projet de LPD révisé le 12 juin 2018. La Commission des institutions politiques du Conseil des États a adhéré à la décision du Conseil national le 22 juin 2018. La second partie du projet n'entrera pas en vigueur avant 2020, compte tenu du calendrier actuel.

1836 Le projet de LPD confirme de manière synthétique :

— le renforcement des droits des personnes concernées par un traitement de données à caractère personnel et le renforcement des obligations des responsables du traitement et des sous-traitants. Les responsables du traitement et les sous-traitants doivent par exemple tenir un registre des activités de traitement (art. 11 P-LPD).

— l'amélioration de la transparence en matière de traitement des données à caractère personnel. Cela se traduit notamment par l'obligation pour les responsables du traitement d'informer les personnes concernées du traitement de leurs données à caractère personnel et de leur droit d'accès, au moment de la collecte, sauf en cas « d'obligation légale de garder le secret » (art. 18 al. 1 let. c P-LPD). Le responsable du traitement a le devoir d'informer la personne concernée lors de décisions individuelles automatisées, ainsi que le droit pour la personne concernée, à certaines conditions, de faire valoir son point de vue et d'exiger une intervention humaine pour revoir une décision prise uniquement sur une base automatisée. Le responsable du traitement doit également fournir des informations plus nombreuses lors de l'exercice de son droit d'accès [1532].

— l'obligation de conduire une analyse d'impact, préalablement au traitement pour les projets du secteur privé ou du secteur public, qui présentent un risque élevé pour les droits fonda-

1532. Message du 15 septembre 2017, p. 6565.

mentaux et la personnalité des personnes concernées (art. 20 P-LPD).

- la prise en considération des enjeux de protection des données dès la mise en place de nouveaux traitements (Privacy-by-Design et Privacy-by-Default) (art. 6 P-LPD).
- la responsabilisation des responsables du traitement et des sous-traitants en encouragement l'auto-réglementation, par le biais de codes de conduite ou de certifications (art. 10 P-LPD).
- la facilitation des flux transfrontaliers (art. 13 P-LPD).
- le renforcement de l'indépendance et des pouvoirs du Préposé fédéral (art. 44 P-LPD). Nommé par l'assemblée fédérale et non par le Conseil fédéral (proposition du CIPN-N). Le Préposé pourra ordonner des mesures provisionnelles et prendre des décisions contraignantes, au terme d'une enquête ouverte d'office ou sur dénonciation (mesures d'instruction) contre un organe fédéral (art. 43 ss P-LPD) ou au titre de mesures administratives (art. 45 P-LPD). Il ne pourra toutefois pas décréter de sanction administrative. Seuls les tribunaux auront cette prérogative [1533]. Le Préposé ne peut que donner des conseils (art. 28 LPD) et émettre des recommandations (art. 29 LPD) avec la LPD actuelle ce qui constitue une transformation du rôle du Préposé La violation d'une décision du Préposé pourra être sanctionnée. Les cantons demeurent compétents pour prononcer des sanctions (art. 59 P-LPD).
- la supervision des entreprises privées suisses et leur soumission aux décisions des autorités de contrôle des États membres de l'UE, pour les traitements de données à caractère personnel, remplissant les conditions de l'art. 3, al. 2 RGPD.
- l'obligation d'annoncer les violations de sécurité des données (art. 22 P-LPD).
- l'obligation pour les entreprises étrangères traitant des données à grande échelle de manière régulière, en rapport avec un suivi de comportement ou l'offre de biens ou de services en Suisse de désigner un représentant en Suisse, si ce traitement présente un risque élevé.

1533. Conseil fédéral, *Une meilleure protection des données et un renforcement de l'économie suisse.*

— l'anonymisation des données dès que la finalité du traitement le permet (art. 27 P-LPD).

— des sanctions financières de nature pénale (500 000 CHF).

— la punissabilité des organes dirigeants à titre personnel (art. 29 CP et art. 6 de loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA) et l'absence de sanction directe des entreprises par le biais de sanctions administratives (sauf si le montant de l'amende prévisible ne dépasse pas 50 000 francs et que l'identification de la personne punissable nécessite des actes d'enquête disproportionnés).

— la suppression du caractère express du consentement en cas de traitement de données sensibles ou de profilage.

— la création d'une présomption d'atteinte en cas de communication de données à des tiers, et sa limitation lorsque la communication porte sur des données sensibles ou à des fins de prospection publicitaire.

— l'extension de la dérogation à la tenue d'un registre pour les entreprises de moins de 500 collaborateurs (au lieu de moins de 50).

— l'obligation pour le Préposé de tenir un registre des traitements pour les responsables du traitement privé et non pas uniquement pour les organes fédéraux.

— L'obligation de disposer d'indices suffisants ou d'éléments probants pour ouvrir une enquête par le Préposé.

— L'introduction d'un délai de 24 mois entre l'expiration du délai référendaire (ou la votation) et son entrée en vigueur.

§2 Analyse comparée du projet de loi et du Règlement

1837 L'analyse qui suit tient compte des modifications apportées par la CIPN-N en août 2019. La modification de la LPD révisée s'inscrit dans la logique du droit européen de la protection des données. En témoigne, l'augmentation des obligations du responsable du traitement et du sous-traitant (art. 5, 6, 7, 8, 11, 17, 19, 20, 21, 22, art. 30 P-LPD) et le renforcement des droits des personnes (art. 23, art. 28

P-LPD).

Le projet de réforme de la LPD renforce les instruments de mise en œuvre de la loi, en renforçant les pouvoirs du Préposé (art. 44 P-LPD : accès, auditions, expertises, mesures provisionnelles). Ces pouvoirs demeurent cependant insatisfaisants au regard de ceux prévus par le Règlement européen. 1838

Le champ d'application matériel du projet de LPD est similaire au Règlement. Le projet de LPD s'applique aux traitements des personnes physiques sans renoncer pour autant à la protection des personnes morales. La législation suisse sur la protection des données s'applique aux mégadonnées, dans les cas où il est possible d'identifier une personne en particulier [1534]. 1839

Comme le Règlement, le champ d'application territorial du projet de loi dispose d'un élément d'extranéité et n'est pas limité au territoire suisse. Le projet s'applique aux entreprises n'ayant pas de siège en Suisse, mais qui traitent des données de personnes domiciliées en Suisse, dans le cadre d'un suivi de comportements ou de l'offre de biens ou de services en Suisse. Ces entreprises sont contraintes d'avoir un représentant en Suisse afin que les personnes concernées puissent exercer plus facilement leurs droits. 1840

Le projet de LPD révisée diffère cependant du Règlement en plusieurs points. 1841

Au niveau des principes, le projet de LPD révisée conserve les principes de l'article 4 LPD : licéité, proportionnalité, information de la personne concernée, finalité du traitement et principe de bonne foi. Les articles 5 à 7 LPD, à savoir le principe d'exactitude (art. 5 al. 1 LPD), le droit de rectification (art. 5 al. 2 LPD) ainsi que le principe de sécurité (art. 7 al. 1 LPD), viennent compléter l'article 4 LPD. Le Règlement pose le principe de loyauté et de transparence des traitements. Il est plus exigeant concernant les finalités du traitement. Il requiert des « finalités déterminées, explicites et légitimes, et que les données ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités » (limitation des finalités). Il introduit un principe de minimisation des données et de limitation de la 1842

1534. Message du 15 septembre 2017, p. 6623.

conservation des données (art. 5 RGPD et voir paragraphe 849).

1843 Si le projet de loi renforce les droits des personnes concernées, il ne reprend pas l'intégralité des dispositions du Règlement. Cela introduit une différence de traitement potentiel entre les personnes domiciliées en Suisse et celles domiciliées dans l'UE. Les personnes concernées bénéficieront de droits limités en Suisse en comparaison européenne : ils bénéficieront d'un droit d'accès, d'un droit à l'effacement des données (« droit à l'oubli »), d'un droit d'opposition et d'un droit à la limitation du traitement en Suisse.

1844 La protection des personnes concernées est moindre que celle octroyée par le Règlement, comme en atteste l'absence de renversement du fardeau de la preuve, lors d'une procédure civile et l'absence d'action civile en réparation du dommage et en responsabilité du tort moral. Seules des actions défensives sont prévues dans la LPD (art. 15 LPD, art. 25 LPD).

1845 Les mineurs ne disposent d'aucune protection spécifique, si ce n'est la présomption de violation lors d'une communication de données personnelles, sauf pour les données sensibles ce qui aurait été particulièrement justifié du fait de leur plus grande vulnérabilité [1535]. Cette distinction majeure par rapport au Règlement (art. 8, al. 1) constitue une spécificité suisse. Le Règlement fixe deux limites d'âge de 13 et 16 ans. Il s'inspire du Children's Online Privacy Protection Act (COPPA) en droit américain. Ce texte a été préparé par le Congrès américain en 1998 et promulgué par la *Federal Trade Commission* en 2000 [1536].

1846 En application des articles 11 et 13 de la Constitution suisse, et compte tenu des innovations digitales dans le domaine de l'éducation en Suisse [1537], une protection spécifique de la sphère privée des mineurs apparaît essentielle. Une pesée des intérêts avec la protection de la liberté économique (art. 27 de la Constitution

1535. Pour une analyse approfondie de cette problématique, voir Fasnacht, *Die Einwilligung im Datenschutzrecht*, p. 247 ss et p. 256.

1536. COPPA, p. « www.coppa.org » (16/10/2017).

1537. Duvillard Laureline, *Une nouvelle application qui aide à apprendre*, in : Actualités EPFL (https://www.epfl.ch/), Lausanne 2018, p. « https://actu.epfl.ch/news/une-nouvelle-application-qui-aide-a-apprendre/ » (18/12/2018) ; Duvillard Laureline, *L'EPFL inaugure un centre dédié aux sciences de l'éducation*, in : Actualités EPFL (https://www.epfl.ch/), Lausanne 2018, p. « https://actu.epfl.ch/news/l-epfl-inaugure-un-centre-dedie-aux-sciences-de-l-/ » (18/12/2019).

suisse) doit cependant être effectuée [1538]. Pour Tobias Fasnacht, le droit de la protection des données en Suisse devrait fixer un âge spécifique pour le recueil du consentement d'un mineur préalablement au traitement de ses données à caractère personnel dans le cadre des « services de la société de l'information ».

Si le projet de LPD révisé rend obligatoire la notification des violations de données au Préposé fédéral (art. 22 P-LPD) et, dans certains cas, à la personne concernée, en cohérence avec le Règlement et la Conv. 108, il est cependant regrettable que l'obligation du devoir d'annonce ne soit pas pénalement réprimée par le projet de LPD. 1847

Si le Projet de LPD révisée exige la réalisation d'une analyse d'impact en cas de traitements présentant un risque élevé, les entreprises dotées d'un conseiller à la protection des données ne sont pas soumises à cette nouvelle obligation, ce qui diffère du Règlement. Aucune sanction n'est prévu en cas de manquement. 1848

Contrairement au Règlement, le Préposé fédéral n'est pas autorisé à imposer des sanctions administratives. La voie pénale doit être choisie pour sanctionner financièrement une violation aux dispositions de la LPD. Le montant des sanctions pénales reste inférieur aux montants du Règlement : 500 000 CHF en cas de violation intentionnelle du devoir d'information (omission ou fourniture d'informations inexactes ou incomplètes), contre EUR 20 Mio en application du Règlement. 1849

Le législateur suisse introduit une sanction pénale en cas de violation du devoir de diligence du responsable du traitement dans le cadre de la sous-traitance (art. 55 P-LPD et art. 29 CP). Cette disposition pénale réprime uniquement les violations intentionnelles du devoir de diligence sous l'angle des articles 7, 8, 13 et 14 P-LPD. En revanche, la violation du devoir d'annonce n'est pas sanctionnée pénalement (art. 22 P-LPD). 1850

Si les pouvoirs du Préposé fédéral sont renforcés (amendes en cas d'insoumission à une décision ou à une décision d'autorité de recours, art. 57 P-LPD), ils demeurent moins étendus que ceux des autorités de contrôle de l'UE. 1851

Si la Suisse adopte l'approche européenne qui encourage le recours 1852

1538. Fasnacht, *Die Einwilligung im Datenschutzrecht*, p. 260.

aux mécanismes de Soft Law, les associations professionnelles et les associations économiques suisses seront seules en charge de la préparation des codes de conduite. Le Préposé ne préparera pas, ni n'approuvera pas les codes de conduite, ce qui diffère du Règlement. En effet, l'approbation d'un code de conduite dans l'UE, crée une présomption de conformité. Cette approche ne garantit pas la conformité réelle, mais valorise la conformité formelle uniquement. En outre, pour la doctrine « la réglementation qui se fonde sur des principes de Soft Law et qui est uniquement mise en œuvre par l'industrie est vouée à l'échec [1539] ». Le législateur devrait s'assurer que les intérêts de toutes les parties prenantes sont représentés lors de l'élaboration des codes de conduite.

1853 Quant á la désignation des conseillers à la protection des données en entreprise, elle n'est pas soumise aux mêmes conditions que celles prévues par le Règlement (art. 9 LPD).

1854 Le Conseil fédéral a renforcé la responsabilité pénale des organes dirigeants par l'application de l'art. 6 DPA en plus de l'art. 29 CP [1540]. Le délai de prescription de l'action pénale est prolongé à cinq ans (art. 60 P-LPD).

1855 Lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement, conformément à l'al. 6, que si elle exprime librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée. Cette formulation légèrement remaniée permet de se rapprocher de la terminologie de la Convention 108 (art. 5, par. 2), afin de satisfaire aux exigences de celle-ci. Pour que le consentement soit valable, il faut toujours que le traitement, en particulier son ampleur et son but, soit suffisamment défini.

1856 Le message de la loi fédérale portant révision de la LPD, du 15 septembre 2017 précise que le consentement doit être clair. l'art. 5 P-

1539. Wright / de Hert, *Enforcing Privacy*, p. 74.

1540. « Lorsque le comportement punissable consiste en la violation d'un devoir qui incombe au responsable du traitement et que celui-ci est une entreprise, l'infraction est imputée aux représentants des organes dirigeants (art. 6 de la loi sur le droit pénal administratif et 29 du Code pénal) ». Les autorités de contrôle peuvent enfin renoncer à poursuivre les personnes physiques responsables et décider de punir l'entreprise directement, lorsque l'amende ne dépasse pas 50 000 CHF. Si l'identification de la personne responsable nécessite des actes d'enquête disproportionnés, le Préposé fédéral peut sanctionner, non pas les entreprises elles-mêmes, mais leurs dirigeants.

LPD précise que « lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement que si elle exprime librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles, ou en cas de profilage, son consentement doit être exprès ». Le message précise que le terme : « exprès » va plus loin que le consentement « clair ». Le Conseil fédéral ne voit cependant pas de raison de s'écarter de la situation juridique actuelle. Pour plus de clarté, le Projet de LPD remplaçait, avant la modification du CIPN-N en août 2019, dans les versions française et italienne du texte, les termes de « explicite » et de « esplicito », s'agissant de la qualité du consentement concernant les données sensibles, par ceux de « exprès » et « espresso », reprenant ainsi la terminologie de l'art. 1 CO. Le texte allemand reste inchangé. « Une déclaration de volonté est « expresse » lorsqu'elle est formulée oralement, par écrit ou par un signe, et qu'elle découle directement des mots employés ou du signe en question [1541]». Le caractère exprès requiert une action par exemple le besoin de cocher une case pour la personne concernée ou d'opter activement pour certains paramètres techniques. Il faut que la déclaration de la personne concernée exprime la volonté de celle-ci sans ambiguïté. Plus les données sont sensibles, plus l'exigence de clarté du consentement est forte. Or, la Commission des institutions politiques du Conseil National a choisi une option très surprenante en renonçant au consentement exprès de la personne concernée pour le traitement des données sensibles. Cette décision risque de faire perdre à la Suisse sa décision d'adéquation tant elle s'éloigne de la protection de la personne physique et de la philosophie du RGPD qui cherche à effectuer une pesée des intérêts en présence. Il y a là une manifestation explicite de la renonciation de la Suisse à la protection de la sphère privée.

Le Règlement prévoit un droit à des recours collectifs (art. 80 RGPD), contrairement au projet de LPD révisée. 1857

Le Conseil fédéral sera désormais compétent pour examiner et constater l'adéquation de la législation étrangère en matière de protection des données (art. 13, al. 1 de la loi fédérale sur la révision de la LPD), concernant les transferts de données à caractère personnel à l'étranger. Cette solution apporte de la sécurité juridique car à ce jour, il incombe aux responsables du traitement de vérifier si la 1858

1541. Message du 15 septembre 2017.

législation de l'État concerné assure un niveau de protection adéquat [1542].

1859 En l'absence d'une décision du Conseil fédéral, « des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti » (art. 13, al. 2 du projet de loi révisée). Ce niveau de protection approprié peut trouver sa source dans la conclusion d'un « traité international » ou « peut être assuré par des garanties ad hoc et standardisées agrées, établies par des instruments juridiquement contraignants et opposables, conclus et mis en œuvre par le personnel impliqué dans le transfert et le traitement ultérieur des données ». Ces dispositions font échos à l'article 46 du Règlement (UE) 2016/679, qui fait aujourd'hui l'objet d'un recours auprès de la CJUE (voir paragraphe 140).

1860 Le projet de loi renforce le système des sanctions pénales, en prévoyant les mesures suivantes :

- l'augmentation du montant maximum des amendes de CHF 10 000 à 500 000.
- l'introduction de nouvelles infractions pénales : violation des devoirs de diligence et insoumission à une décision du Préposé ou d'une autorité de recours (sur le modèle de l'art. 292 du Code pénal).
- l'extension du devoir de discrétion à toutes les données personnelles secrètes.
- l'obligation d'annonce d'une violation de la sécurité des données personnelles (art. 22 P-LPD). Cette obligation s'applique du sous-traitant au responsable du traitement « pour tout cas de violation de sécurité » (art. 22, al. 3 P-PLD) et du responsable du traitement au Préposé (art. 22, al. 1 P-LPD), « en cas de risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée » (art. 22, al. 1 P-LPD). La personne concernée peut être notifiée « lorsque cela est nécessaire à sa protection ou que le Préposé l'exige » (art. 22, al. 4 P-LPD).
- l'introduction de la possibilité, à certaines conditions, de punir directement les entreprises d'une amende de CHF 50 000 maximum.

1542. Message du 15 septembre 2017, p. 6656.

— l'augmentation du délai de prescription de l'action pénale à 5 ans [1543].

Dans le projet de LPD révisée, les sanctions pécuniaires ont un caractère pénal. Ceci implique le respect de certaines garanties de procédure propres à la procédure pénale, que la loi sur la procédure administrative fédérale, applicable aux sanctions administratives, ne prévoit pas [1544]. Le projet de loi révisée ne prévoit pas de sanction administrative, mais uniquement des sanctions pénales. Cette solution s'explique par un manque de volonté politique de conférer au Préposé fédéral, le pouvoir de rendre des sanctions administratives ce qui aurait impliqué une modification de son organisation et des besoins supplémentaires en ressources [1545]. 1861

Afin de conserver la décision d'adéquation rendue par la Commission européenne, il serait souhaitable que la Suisse coopère avec les autres autorités de protection des États membres dans le cadre de la mise en place du mécanisme de contrôle de la cohérence et qu'elle suive les travaux et avis du Conseil Européen à la Protection des données, afin d'appliquer le droit de la protection des données, de façon cohérente en Suisse, bien qu'elle ne soit ni membre de l'Union européenne, ni membre de l'Espace économique européen. 1862

Il serait également souhaitable que le Préposé fédéral à la protection des données soit autorisé à émettre des avis consultatifs, notamment en cas de réclamations introduites par des personnes physiques. 1863

L'ordonnance sur la protection des données (R.S 235.11) du 14 juin 1993 devra également être révisée. Quant à l'accord Privacy-Shield entre la Suisse et les USA, il devrait lui aussi être amendé de manière à refléter le renforcement du cadre juridique en matière de protection des données. Cette modification n'est pas prévue à ce jour [1546]. Quant au calendrier de l'entrée en vigueur de la nouvelle LPD, il dépend d'éléments politiques. 1864

1543. Conseil fédéral, *Dossier de presse de 15 septembre 2017 : Les sanctions dans le projet de révision totale de la loi sur la protection des données*, in : DFJP (https ://www.ejpd.admin.ch/), Berne 2017, p. « https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/rohstoff-f.pdf » (20/10/2017).

1544. Message du 15 septembre 2017, p. 6714.

1545. *Ibidem.*

1546. Communication avec Camille Dubois, Office fédéral de la justice, le 1er novembre 2017.

§3 Les aspects politiques

1865 Le projet de loi portant révision de la LPD et le message de la nouvelle LPD ont été approuvés par le Conseil fédéral le 15 septembre 2017. Le Conseil national a adhéré au projet le 12 juin 2018 et la Commission des institutions politiques du Conseil des États a adhéré à la décision du Conseil national le 22 juin 2018. Le Conseil fédéral a fixé au 1er mars 2019 la date de l'entrée en vigueur des dispositions concernant le traitement des données dans le cadre de la coopération Schengen en matière pénale [1547]. Le 1er mars 2019, les dispositions concernant le traitement des données dans le cadre de la coopération Schengen en matière pénale sont entrées en vigueur. En mars 2019, la Commission européenne à jugé que « la densité des contrôles du Préposé et sa dotation étaient insuffisantes dans le cadre de l'évaluation Schengen [1548] ». Dans son rapport, le Préposé soulignait que la Commission européenne avait entamé son évaluation générale du niveau de protection des données de la Suisse au printemps 2019. Il exhorait le Conseil fédéral à signer la Convention 108, « d'autant plus que la Commission européenne a rappelé à plusieurs reprises que la ratification de cette convention actualisée était déterminante dans sa décision d'adéquation [1549] ». Ce rapport a positivement influencé la Suisse qui a signé la Conventioon 108 en fin d'année 2019.

1866 Des aspects politiques influencent l'adoption de la LPD révisée. La question de l'étendue de la reprise des dispositions du Règlement européen en droit suisse est particulièrement discutée [1550]. Le contexte politique des négociations de l'UE avec la Suisse dans le cadre de la révision de l'accord-cadre a également pesé indirectement sur l'adoption de la LPD révisée. L'accord-cadre vise à régler les questions institutionnelles relatives à l'intégration de la Suisse dans le marché intérieur de l'UE. En revanche, il ne modifie pas directement le périmètre sectoriel d'accès au marché, qui est défini dans des accords séparés. L'accord-cadre ne préconise pas directement la reprise du Règlement par la Suisse. En revanche, une fois que l'accord-cadre sera ratifié, il deviendra possible d'étendre le périmètre de l'intégration sectorielle par la conclusion de nouveaux

1547. OFJ, *Renforcement de la protection des données.*
1548. PFPDT, *26e rapport d'activités 2018/2019.*
1549. *Ibidem.*
1550. Husi-Stämpfli Sandra, *Die DSG-Revision oder : Ein Beziehungsdrama in drei Akten - Gedanken zur komplexen Revision des Datenschutzrechts in der Schweiz*, in : Jusletter 2018/7, p. 1.

accords ou la mise à jour des accords existants. Cela permettrait notamment de reprendre formellement le Règlement. D'ici là, le législateur suisse considère que la Suisse est libre de s'aligner unilatéralement par rapport aux dispositions du Règlement à travers le principe de la reprise autonome de l'acquis, ce qui est préconisé par la révision en cours de la LPD. Il n'en reste pas moins que le ré-examen éventuel de l'adéquation de la législation suisse sur la protection des données au droit européen par la Commission européenne, constitue une pression politique pour la Suisse.

Un des éléments essentiel est de s'assurer que le projet du Conseil fédéral codifie le droit à l'autodétermination informationnelle de l'art. 13, al. 2 Constitution et donne une place centrale à l'action civile en responsabilité du tort moral et en réparation des dommages en cas de violation de la LPD révisée. 1867

§4 Les conséquences pour les cantons

La modification de la LPD et l'entrée en vigueur du Règlement européen ne modifient pas la répartition des compétences législatives entre la Confédération et les cantons qui demeure inchangée. 1868

Cependant, les cantons ont l'obligation de mettre en œuvre la directive (UE) 2016/680. Si la Suisse ratifie la nouvelle Conv. 108 modernisée, les cantons devront également se mettre en conformité avec cette Convention. Le niveau de protection du droit cantonal sera déterminant pour le maintien de la décision d'adéquation de l'UE. 1869

Le projet de révision prévoit l'abrogation de l'art. 37 LPD, qui régit l'exécution de la LPD par les cantons. 1870

§5 L'amélioration relative du cadre législatif suisse

Le Conseil fédéral n'apporte aucun changement radical, mais prévoit une amélioration générale du cadre législatif suisse en droit de la protection des données. Le but de la LPD révisée est de « protéger la personnalité et les droits fondamentaux des personnes physiques dont les données font l'objet d'un traitement ». Il n'est pas fait mention du caractère économique du droit de la protection des données en référence à la libre circulation des données comme dans 1871

le Règlement européen.

1872 Contrairement au Règlement européen, le projet de LPD révisée ne reconnaît pas le rôle central de l'action civile pour garantir l'effectivité de la protection des données et la réparation des dommages en cas de violation des dispositions du droit de la protection des données par le responsable du traitement et le sous-traitant. Il est regrettable que la responsabilité des acteurs économiques ne constitue pas un élément structurel du projet de LPD, dans le contexte d'une économie fondée sur les données. Il importe que la Suisse reprenne cet élément dans son projet de LPD en faveur des personnes physiques. Le corollaire d'une telle responsabilité serait la possibilité d'une action civile et l'existence de sanctions (amendes administratives ou judiciaires dissuasives) équivalentes au droit européen en cohérence avec la décision d'adéquation de la Commission européenne (Voir paragraphe 1075).

1873 Le Conseil fédéral prescrit un renforcement des droits des personnes concernées et augmente les obligations du responsable du traitement. La protection des données des personnes morales est maintenue en droit suisse, ce qui est plus exigeant que le RGPD. Le droit à la portabilité des données a été ajouté de justesse en août 2019 seulement par la Commission des institutions politiques du Conseil National (CIP-CN). Le projet ne prévoit pas de conditions particulières pour les traitements des données des enfants. Les activités syndicales, opinions et les données sur les mesures d'aide sociale sont exclues du champ d'application des données sensibles. Ces derniers point sont particulièrement problématiques concernant les risques d'abus et de discriminations qui risquent d'en résulter.

1874 Le Conseil fédéral renforce les pouvoirs du Préposé, mais sans comparaison avec le mécanisme de Public Enforcement mis en œuvre par le Règlement européen et les pouvoirs octroyés aux autorités de contrôle des États membres de l'Union (art. 58 RGPD).

1875 Le Préposé doit disposer d'un registre pour les responsables du traitement privés et publics. Les pouvoirs d'enquête du Préposé sont limités et soumis à condition. Ils ne sont pas aussi vastes que ceux des autorités de contrôle européennes. Dans le cadre de leurs pouvoirs d'enquête (art 42, al. 7 RGPD et art. 58, al. 1 let. a à f RGPD.), les autorités de contrôle de l'UE ont le pouvoir « d'ordonner la communica-

tion d'informations dont l'autorité de contrôle a besoin pour exercer ses missions, de mener des enquêtes sous forme d'audits, d'examiner les certifications octroyées au responsable du traitement ou sous-traitant1, de notifier au responsable ou au sous-traitant une violation alléguée des prescriptions du RGDP, d'accéder à toutes les données et les informations nécessaires ainsi que d'accéder à tous les locaux, installation et moyen de traitement du responsable ou du sous-traitant dans le respect du droit de l'UE et du droit procédural national [1551]».

1876 Dans le cadre de leurs pouvoirs d'intervention, les autorités de contrôle de l'UE peuvent prendre des mesures correctrices. Quant à lui, le Préposé fédéral sera autorisé à prendre des mesures provisionnelles (art. 44, al. 2 P-LPD), pour la durée de l'enquête et de les faire exécuter, le cas échéant, par une autre autorité fédérale ou par des organes de police cantonaux ou communaux. Ces mesures peuvent viser à prévenir ou à faire cesser le préjudice (art. 262 CPC). De manière similaire au droit de la concurrence, les mesures provisionnelles doivent respecter le principe de proportionnalité [1552]. La mesure doit tenir compte des intérêts de la partie intimée, être nécessaire et supprimer l'atteinte [1553].

1877 Contrairement aux autorités de contrôle européennes, le Préposé fédéral ne sera pas autorisé à sanctionner un comportement illicite par des amendes administratives, en tant que mesure correctrice. Seules les autorités pénales seront autorisées à distribuer de telles amendes. Une plainte est requise pour engager des poursuites pénales. Le montant des amendes pénales (art. 54 ss P-LPD) reste faible, bien que la CIP/CN en ait augmenté le montant (augmentation de 250 000 CHF à 500 000 CHF) et sans comparaison avec les montants du Règlement européen (20 000 000 EUR). Les amendes pourront être prononcées dans des cas limités en cas de violation intentionnelle des obligations d'informer, de renseigner et de collaborer, et lors de la violation intentionnelle de devoirs de diligence (lors de transfert transfrontalier de données personnelles, de recours à un sous-traitant ou de violation des obligations minimales dans le domaine de la sécurité). La Suisse conserve la responsabilité

1551. Métille / Arasteh, *Le Règlement général sur la protection des données et les assureurs privés suisses*, p. 140.
1552. BSK-ZPO-Sprecher, N. 47, art. 262 ZPO.
1553. Handelsgericht SG, *APC Software AG et Sevelen c. Waldmeier AG*, in : DPC 1999/2, p. 324 ss, consid. II/7.

pénale des personnes physiques (20 000 CHF). L'amende est limitée à 50 000 CHF lorsque l'entreprise est sanctionnée.

1878 Il est regrettable que le Conseil fédéral n'ait pas précisé la procédure d'encaissement d'une amende imposée à une organisation suisse, sans établissement ou représentant dans l'UE, par une autorité de contrôle européenne. La question se pose également de la licéité d'une telle amende administrative éventuelle pour les entreprises suisses, puisque le projet de LPD révisée ne retient pas la qualification d'une amende en droit suisse de la protection des données [1554].

1879 Le P-LPD donne compétence au Préposé de prononcer des décisions ordonnant le respect des obligations de la LPD sous menace de sanctions pénales en cas d'insoumission (art. 57 P-LPD) [1555]. Le P-LPD ne prévoit aucune disposition punissant pénalement la négligence. Lorsque l'obligation administrative incombe au responsable du traitement, la violation de la LPD est imputée aux personnes occupant une fonction dirigeante (Cf. art. 29 CP et 6 DPA).

1880 Le volet pénal est particulièrement renforcé dans le projet de LPD révisé. Le Code pénal protège le secret de fonction et le secret professionnel et sanctionne leur violation (art. 320, art, 321 CP). Le Conseil fédéral prescrit dans son projet de LPD révisée l'introduction d'un nouvel article pour sanctionner l'usurpation d'identité (art. 179 decies CP) d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire. Plusieurs articles du code pénal sont applicables à la protection des données : les article 173 à 177 CP. Ils sanctionnent les atteintes à l'honneur (diffamation, calomnie, injure). L'article 179 protège le secret de la correspondance et traite de manière similaire la surveillance du courrier électronique et du courrier postal, en application du principe de neutralité technologique [1556]. La confidentialité des conversations téléphoniques est protégée par l'art. 179bis CP. Ainsi une conversation est enregistrée à l'insu des personnes concernées, sans base légale, constitue

1554. Métille / Arasteh, *Le Règlement général sur la protection des données et les assureurs privés suisses*, p. 141.
1555. Message du 15 septembre 2017, p. 6708.
1556. Métille Sylvain, *Le droit au respect de la vie privée : Les défis digitaux, une perspective de droit comparée (Suisse)*, in : EPRS | Service de recherche du Parlement européen, Bruxelles 2018, pp. 1-44.

un traitement illicite, punissable pénalement [1557].

Afin de répondre aux demandes d'enquêtes d'une autorité de contrôle européenne envers une entreprise suisse, un accord de coopération entre la Suisse et l'UE sera vraisemblablement nécessaire. A défaut, les enquêtes ne pourront pas être conduites sur le territoire helvétique. Anticipant cette difficulté, le législateur européen a imposé la désignation d'un représentant dans l'UE pour toute entreprise établie en-dehors de l'UE [1558]. Les entreprises suisses doivent veiller à désigner un représentant dans l'UE, si leurs activités remplissent les conditions de l'art. 3, al. 2 RGPD. En cas d'enquête, l'autorité de contrôle européenne fera parvenir sa demande ou sa décision au représentant de l'entreprise suisse établis dans l'UE. La question se pose de savoir si des entreprises suisses pourront être doublement sanctionnées pour les mêmes faits dans l'UE et en Suisse. Le principe de l'interdiction des doubles sanctions pourrait cependant trouver application, si des amendes étaient infligées dans l'UE et des sanctions pénales en Suisse [1559]. 1881

Les entreprises suisses établies dans l'UE, dont les traitements de données personnelles sont conformes au droit suisse, pourront être sanctionnées par les autorités de contrôle européennes, si elles ne se sont pas également mises en conformité avec le Règlement européen alors que leurs activités tombent dans le champ d'application de l'art.3, al. 2 RGPD. Dans un objectif de rationalité économique et de sécurité juridique, il ferait sens d'harmoniser les législations sur la protection des données entre la Suisse et l'UE. Plus encore que le Règlement, le droit suisse devrait intégrer les dispositions de la Convention 108 modernisée, dans son droit interne. La signature de cette Convention sera déterminante pour le maintien de la décision d'adéquation de la Suisse. L'article 12bis de la Convention nécessite en particulier de donner des pouvoirs de décision au Préposé fédéral à la protection des données. Il doit être habilité à prononcer des sanctions susceptibles de recours ou à demander aux autorités judiciaires de le faire. Pour pouvoir exercer ces pouvoirs de contrainte, le PFPDT devrait pouvoir demander le soutien des autorités de police. La coopération avec d'autres autorités de contrôle et l'échange d'informations dans le cadre d'investigations 1882

1557. *Ibidem*; ATF 133 IV 249, consid.3.2.2. in : JdT 2009 IV 10, p. 19.
1558. art. 27 RGPD.
1559. Patklom, *Herausforderungen bei der Umsetzung des Datenschutzes*, p. 45.

communes devrait également être abordé.

1883 Le projet de LPD révisé ne prévoit pas l'inversion de la charge de la preuve. Par conséquent, la personne concernée, partie à un procès, doit apporter la preuve des faits allégués. La jurisprudence du Tribunal fédéral pose des exigences élevées dans le domaine de l'allégation et de la preuve du dommage [1560] : pour ne pas voir sa demande qualifiée d'irrecevable ou de non-fondée, la preuve apportée doit être précise et tous les éléments de preuve rapportés. Si la charge de la preuve n'est pas inversée, la personne concernée pourra fonder sa plainte sur la soustraction de données enregistrées ou transmises électroniquement (art. 143 CP) si l'existence d'un dessein d'enrichissement illégitime peut être démontré et sur « l'accès indu à un système informatique spécialement protégé » (art. 143bis CP).

1884 La protection de la sphère privée est assurée par le code pénal. Sont punissables, « l'écoute et l'enregistrement de conversations non publiques entre d'autres personnes, ainsi que l'utilisation ou la conservation de tels enregistrements » (art. 179bis CP), de même que l'enregistrement non autorisé de conversations auxquelles l'auteur prend part (art. 179ter CP). Constitue également une infraction « l'observation avec un appareil ou la prise de photos de faits qui relèvent du domaine secret d'une tierce personne, ainsi que le fait de conserver ces images, d'en tirer profit ou d'en donner connaissance à un tiers » (art. 179 quater CP), sauf dispositions légales autorisant la surveillance (comme en droit du travail par exemple). De même ne sont pas punissables les enregistrements de données en relation avec des services d'assistance, de secours ou de sécurité ou s'inscrivant dans le champ d'application de l'art. 179 quinquies al. 1 CP (ex : dans le domaine bancaire, lors de conversations dans le cadre de relations d'affaires entre le client et le salarié). La personne concernée pourra aussi invoquer l'application de l'art. 35 LPD qui « punit la personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans l'exercice

1560. ATF 127 III 365, c. 2b ; TF, 5A_336/2008, c. 4 ; TF 4C.82/2006, c. 3.4 ; Walter Hans Peter, *Prozessuale Aspekte beim Streit zwischen Kunden und Vermögensverwaltern*, in : Zeitschrift für schweizerisches Recht 2008 127/1, RDS I 2008, p. 112 ss ; Sur la question du *"Substanziierungspflicht"* à la lumière des nouvelles règles du CPC, cf. Fellmann Walter, *Substanziierungspflicht nach der schweizerischen Zivilprozessordnung*, in : Haftpflichtprozess, Zürich 2011, p. 13 ss, particulièrement p. 19 concernant la preuve du dommage.

d'une profession qui requiert la connaissance de telles données ». En fonction du cas d'espèce, la violation du secret de fonction (art. 320 CP) et du secret professionnel (art. 321 CP) pourront être invoqués.

On pourrait penser que les enjeux de la mise en conformité de la LPD avec le Règlement sont identiques à ceux qui existaient à l'époque de la transposition de la directive 95/46/CE et son impact en Suisse [1561]. 1885

Or il n'en est rien. Le rôle des données dans les modèles d'affaires des entreprises à l'ère digitale a pris un sens nouveau (voir paragraphe 183). Les données sont au cœur de stratégies d'innovations des entreprises du fait du recours aux technologies d'intelligence artificielle qui sont à l'origine d'économies d'échelle et de prédictions personnalisées à moindre coût [1562]. Le contenu de la législation en matière de protection des données influence la perception des investisseurs et la compétitivité économique d'un pays si elle réduit l'accès aux données personnelles. Du fait de la volatilité des capitaux dans le monde et de la place centrale des technologies d'intelligence artificielle, la législation en matière de protection des données constitue un enjeu géopolitique sur la scène internationale. Vladimir Putin déclarait en 2017 : « whoever leads in AI will rule the world ». L'accès aux données tant pour les acteurs privés que pour les acteurs publics revêt un caractère stratégique majeur. Toute la difficulté consiste donc à préserver la libre circulation des données, dans le respect de la protection des données. Cet équilibre dépend du cadre juridique et de l'existence de voies de recours effectives (art. 13 Convention européenne des droits de l'homme). 1886

Comme le confirme Mr. Olivier Matter, Contrôleur européen à la protection des données, la protection des données en Europe a évolué et est passée d'une approche « ex-ante » à une approche « ex-post [1563]». Dans ce contrôle de conformité *a posteriori*, l'effectivité de l'action civile est devenue centrale. La capacité des autorités de 1887

1561. Brun Alain, *La directive européenne relative à la protection des données : convergences et divergences avec le droit suisse*, in : Datenschutz in der Schweiz und in Europa = La protection des données en Suisse et en Europe, Freiburg 1999, p. 11 ss.

1562. Angwin Julia, *Machine bias : There's software used across the country to predict future criminals and it's biased against blacks*, in : ProPublica (https ://www.propublica.org/), New York 2016, p. 12.

1563. Geneva Cybersecurity Law and Policy Conference, *« Data protection in Europe has moved from an ex-ante approach to an ex-post approach »*, Geneva,

contrôle d'infliger des amendes suffisamment dissuasives joue également un rôle important (art. 83 RGPD). Ces deux éléments du contrôle a posteriori constituent la clef de voûte du système du Règlement et devraient être transposés en droit suisse.

21 June 2018.

Chapitre 2: Vers une responsabilité croissante ?

Lors de l'analyse des buts du Règlement, il a été relevé que la responsabilité constituait quasiment l'un des buts principaux du Règlement, au même titre que la libre circulation des données à caractère personnel. 1888

Cette responsabilité est mise en œuvre par une action a posteriori des autorités de contrôle et par une action civile effective. 1889

Se contenter de limiter l'intervention aux autorités de contrôle a posteriori n'aurait pas permis d'assurer un niveau de protection cohérent des personnes physiques. 1890

L'action civile facilitée et efficace est la clé de voûte du système conçu par le Règlement, c'est-à-dire d'un système dans lequel la protection des personnes physiques dépend d'interventions *a posteriori*. C'est grâce à une action civile aussi efficace que possible, que le Règlement relève le défi de l'incompatibilité des deux buts concurrents du Règlement, placés au même niveau, sans hiérarchie de l'un envers l'autre. Seule l'action civile permet en définitive d'atteindre pleinement la libre circulation des données à caractère personnel et simultanément la protection des personnes physiques de tous les États membres. 1891

À cette fin, le cadre juridique doit non seulement renforcer les droits des personnes concernées, mais prévoir également des instruments juridiques spécifiques pour leur mise en œuvre effective [1564]. 1892

Concrètement, comment exercer ces droits sans un recours juridictionnel effectif, c'est-à-dire sans un accès facilité aux tribunaux ? Sans la reconnaissance d'actions collectives et de droit de recours des associations au nom de leurs membres, dans le domaine de la protection des données ? Sans le renversement de la charge de la 1893

1564. Walter Jean-Philippe, *L'effectivité des mécanismes de mise en oeuvre du point de vue du PFPDT*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015, p. 117.

preuve ?

1894 Le Règlement apporte cet élément nouveau du recours juridictionnel effectif des personnes physiques. Il offre ainsi la possibilité aux personnes physiques d'ouvrir une action civile et en fait un instrument d'« Enforcement » du droit de la protection des données, en parallèle du contrôle a posteriori des autorités publiques.

1895 Compte tenu de cet État de fait, renverser la charge de la preuve dans le contexte d'une intervention *a posteriori* comme le fait le Règlement, constitue une mesure essentielle.

1896 Au-delà de sa fonction comme outil de réparation des dommages, l'action civile peut aussi se voir confier un rôle particulier dans la mise en œuvre du droit de la protection des données, de manière similaire au droit de la concurrence [1565].

§1 Les fonctions du droit de la responsabilité

1897 Le droit européen de la protection des données autorise une action civile facilitée et efficace pour obtenir le versement de dommages-intérêts en cas de violation des dispositions du Règlement européen.

1898 Il importe d'analyser quelles sont les fonctions du droit de la responsabilité civile, afin de comprendre comment les actions civiles facilitées et efficaces peuvent jouer un rôle dans la mise en œuvre du droit de la protection des données.

1899 Traditionnellement, le droit de la responsabilité civile a pour fonction aussi bien la compensation que la prévention des dommages, et aussi la création de normes de comportement et la sanction des comportements contraires au droit [1566].

I. La compensation des dommages

1900 La violation du droit européen de la protection des données à caractère personnel donne le droit à la compensation des préjudices moraux et patrimoniaux dans le cadre de la mise en œuvre de la

1565. Hurni, *L'action civile en droit de la concurrence*, p. 5.
1566. *Idem*, p. 64 ss.

responsabilité civile du responsable du traitement (art. 79 RGPD).

L'action en responsabilité civile détermine à quelles conditions une personne lésée par un traitement de données illicite peut répercuter les conséquences d'un fait dommageable sur le responsable du traitement ou du sous-traitant. La compensation des dommages constitue le but principal de l'action en responsabilité civile pour de nombreux auteurs [1567]. Elle vise à réparer le dommage (notion du justice corrective) [1568]. Il s'agit de restaurer l'équilibre perturbé par le comportement de l'auteur, en répercutant sur celui-ci les conséquences de son comportement pour les victimes [1569]. Seule la personne qui a subi un dommage peut intenter une action en réparation. 1901

Établir la responsabilité de l'auteur du dommage, c'est-à-dire du responsable du traitement ou du sous-traitant dans le domaine de la protection des données est le but d'une action civile. La reconnaissance en responsabilité est indépendante de l'existence d'une assurance qui compense financièrement le dommage [1570]. Elle ne sanctionne pas le comportement dommageable, mais vise uniquement à dédommager financièrement une personne. 1902

II. L'aspect dissuasif

L'existence d'actions en responsabilité civile contribue en général à la prévention des dommages ; elle a un effet dissuasif [1571]. Les responsables sont en effet plus diligents. Ils veulent limiter le risque de devoir verser des dommages-intérêts dans le cadre d'une action en responsabilité. 1903

Ainsi l'action civile peut renforcer le respect des règles en droit de la protection des données, en dissuadant les entreprises d'adopter des comportements illicites. La menace d'actions civiles collectives et de sanctions civiles incite les responsables du traitement et les sous-traitants à traiter les données personnelles de manière conforme au Règlement. L'action en responsabilité participe en ce sens à la régulation des relations entre les responsables du trai- 1904

1567. Roberto Vito, *Schweizerisches Haftpflichtrecht*, 1e éd., Zürich 2002, p. 20.
1568. Wells Catharine Pierce, *Tort Law as Corrective Justice : A Pragmatic Justification for Jury Adjudication*, in : Michigan Law Review 1990 88/8, pp. 2348-2413.
1569. Goldberg John CP, *Twentieth-Century Tort Theory*, in : Georgetown Law Journal 2002/91, p. 574.
1570. *Idem*, p. 532.
1571. Hurni, *L'action civile en droit de la concurrence*, p. 69.

tement, les sous-traitants et les personnes concernées. Elle joue donc un rôle de prévention des comportements illicites dans le domaine de la protection des données. En effet, l'action civile augmente le risque pour les responsables du traitement et les sous-traitants de voir leur réputation ternie et d'être obligés de verser des dommages-intérêts au demandeur. Ainsi, elle présente un caractère dissuasif pour les acteurs économiques.

1905 Ceux-ci sont incités à prendre des mesures préventives de protection appropriées aux risques pour protéger les traitements de données personnelles de toute perte ou violation (art. 24 et 32 RGPD et voir aussi paragraphe 941). À défaut, leur responsabilité peut être engagée (art. 79 RGPD et voir aussi paragraphe 1294).

1906 En pratique, les responsables du traitement et les sous-traitants établis dans l'UE veilleront à prendre des mesures techniques et organisationnelles appropriées et les documenteront afin de démontrer, en cas de litige, pour les cas où ils sont attaqués en responsabilité, qu'ils ont traité les données à caractère personnel avec précaution. Cela renvoie à la notion juridique de traitement diligent en « bon père de famille ». Le contrôle s'effectue cependant *a posteriori*, ce qui va à l'encontre d'une vision plus idéaliste de la justice et de la responsabilité, ayant pour fonction de protéger en amont les droits des personnes concernées et d'achever un idéal de justice [1572].

1907 Pour une prévention optimale des dommages en droit de la protection des données et pour renforcer l'effet dissuasif de l'action civile, la CJUE pourait décider de tripler les dommages-intérêts alloués au lésé (treble damages du droit américain de la concurrence). Dans la conception américaine, la personne lésée est encouragée à saisir la justice et à intervenir en tant que *private attorney general* [1573].

1908 En comparaison avec le montant des sanctions allouées au titre du Public Enforcement, c'est-à-dire du contrôle a posteriori effectué par les autorités publiques, les sanctions civiles en droit américain de la concurrence se seraient élevées entre 1990 et 2011 à près de 30 milliards de dollars, contre 8,8 milliards pour les autorités pu-

1572. Hurni, *L'action civile en droit de la concurrence*, p. 74 ; Goldberg, *20th Century Tort Theory*, p. 560.

1573. Hurni, *L'action civile en droit de la concurrence*, p. 109.

bliques, durant la même période.

Spécificité du droit américain, le mécanisme du Private Enforcement a suscité l'intérêt de la Commission européenne. En 2005, la Commission européenne a reconnu l'aspect dissuasif du droit de la concurrence dans un document de travail, annexé au Livre vert : « tant l'octroi de dommages et intérêts que l'imposition d'amendes contribuent au maintien d'une concurrence effective et découragent tout comportement anti-concurrentiel [1574]». 1909

La position de la Cour européenne se fonde sur une jurisprudence de la CJUE [1575] : « le droit pour toute personne de demander réparation du dommage renforce le caractère opérationnel des règles de concurrence de l'Union et il est de nature à décourager les accords ou pratiques souvent dissimulés, susceptibles de restreindre ou de fausser le jeu de la concurrence, en contribuant ainsi au maintien d'une concurrence effective au sein de l'UE ». 1910

Cette perspective n'est pas partagée par la doctrine suisse qui considère quant à elle que seules les autorités administratives détiennent cette prérogative de dissuasion qui relève de l'autorité publique et que l'action civile est uniquement limitée à la réparation des dommages [1576]. 1911

III. La création d'un standard de comportement

La responsabilité civile contribue à la création d'un standard de référence pour juger le comportement d'un responsable du traitement ou d'un sous-traitant et vient préciser leurs devoirs respectifs et les droits des personnes concernées. La jurisprudence qui découle de l'exercice de la mise en œuvre de la responsabilité civile en droit européen de la protection des données sanctionne la violation aux règles de protection des données et détermine les standards qui définissent les normes de conduite. 1912

Comment vérifier que le responsable du traitement a rempli son 1913

1574. Commission européenne, *Livre Vert du 19 décembre 2005 - Actions en dommages et intérêts pour infraction aux règles communautaires sur les ententes et les abus de position dominante (SEC(2005) 1732)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2005, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52005DC0672 » (02/04/2020), p. 8.

1575. Arrêt CJUE, Courage du 5 juin 2014, *Kone AG et al. c. ÖBB-Infrastruktur*, C-557/12, EU :C :2014 :1317, consid. 23.

1576. Hurni, *L'action civile en droit de la concurrence*, p. 112.

devoir de diligence ? En comparant celui-ci de manière concrète et objective avec le devoir de diligence qu'une personne raisonnable aurait montré dans son activité de traitement et dans les mêmes circonstances.

1914 En pratique, les traitements de données de grande dimension et la multiplicité des acteurs, des architectures, objets et applications connectées à Internet sur lesquelles reposent les échanges massifs de données, la multitude de juridictions impliquées et la rapidité, le volume et la vélocité des échanges de données rendent en pratique tout contrôle a priori non seulement illusoire, mais encore inefficace.

1915 On ne peut espérer que de la jurisprudence des tribunaux, à travers des interventions a posteriori, l'élaboration de règles de comportement plus précises [1577].

1916 Les traitements de données sensibles (données génétiques, données d'enfants mineurs) pourraient faire l'objet d'un régime de responsabilité objective aggravé du fait du haut niveau de risque qu'ils entraînent pour les droits et libertés des personnes concernées et de la complexité des projets émergeant en lien avec la médecine personnalisée. Ces projets requièrent une structure en réseaux entre plusieurs institutions de droit public et de droit privé, des clouds et des juridictions multiples. De même, les traitements de données à caractère personnel de mineurs pourraient également faire l'objet d'une responsabilité objective aggravée. L'émergence d'une éducation personnalisée fondée sur l'analyse de données à caractère personnel de personnes vulnérables requiert des garanties strictes. Il en va de même des données personnelles collectées dans les villes intelligentes et des données des personnes âgées échangées avec des robots dans les EMS ou dans des hôpitaux.

1917 Quand bien même, un responsable du traitement se comporterait de manière diligente et mettrait en place des mesures techniques et organisationnelles appropriées, un traitement de données à caractère personnel peut produire des dommages, car une maîtrise absolue des risques en lien avec une activité de traitement de don-

1577. Ces règles, créées a posteriori dans le cadre d'actions en responsabilité, donneront le jour à de nouveaux droits et pourront modifier le comportement des responsables du traitement et des sous-traitants.

nées, est désormais illusoire.

De manière similaire au droit de la concurrence, le droit de la protection des données est aujourd'hui largement un droit à caractère économique, guidé par des considérations économiques [1578]. L'économie étant désormais largement fondée sur l'analyse de données de grande dimension (Big Data), les règles de droit qui encadrent l'accès, le traitement, la supervision et la responsabilité des dommages en lien avec un traitement de données personnelles a une influence sur la compétitivité économique d'un pays. En matière économique, le législateur doit à la fois créer un environnement propice aux innovations technologiques de l'ère digitale, tout en définissant un cadre juridique respectueux des personnes concernées dont les données sont traitées. La responsabilité des acteurs, qui doivent répondre de leurs actes, aussi bien dans le cadre d'actions en responsabilité initiées par les personnes lésées que dans le cadre d'interventions a posteriori des autorités de contrôle, est le corollaire d'une économie fondée sur les données et le profilage des individus dans un société démocratique. Les États-Unis commencent à s'interroger sur la nécessité d'adapter le droit de la concurrence aux Big Data afin de protéger la sphère privée. Droit de la protection des données et Private Enforcement en droit de la concurrence sont donc deux notions intéressantes à analyser conjointement [1579]. 1918

§2 Vers une meilleure compréhension du contrôle a posteriori

Le Règlement accroît l'effectivité des règles de mise en œuvre traditionnelle de la responsabilité. Cette effectivité accrue résulte du mécanisme de Private Enforcement, connu en droit américain de la concurrence. 1919

Ce mécanisme impacte l'action civile telle que définie par le Règlement. Ainsi, certains mécanismes du droit américain de la concurrence, comme celui du Private Enforcement, peuvent éclairer la ré- 1920

1578. Hurni, *L'action civile en droit de la concurrence*, p. 57.

1579. Editorial Board, *US Department of Justice must make antitrust fit for the age of Big Tech*, in : Financial Times (https ://www.ft.com/), London 2019, p. « https://www.ft.com/content/fca13e16-ae32-11e9-8030-530adfa879c2 » (06/08/2019).

flexion en droit de la protection des données [1580].

1921 Droit suisse ou droit européen de la protection des données, tous deux soulèvent des réflexions similaires au droit de la concurrence : contrôle a posteriori et non plus a priori, intervention Étatique ou théorie néo-libérale favorable à la libre circulation des données pour promouvoir l'innovation, l'accès aux données et la croissance économique.

1922 La plupart des notions centrales du projet de LPD révisé et du RGPD (traitement, données, principe de neutralité technologique, responsable du traitement et sous-traitant) sont des concepts économiques. La demande faite par le Conseil fédéral à l'entreprise PwC de conduire une analyse d'impact de la révision de la LPD sur l'économie suisse s'inscrit dans cette perspective. Le Département fédéral de justice et de police a confirmé cette approche [1581]. Afin de ne pas brider l'innovation et la croissance économique, l'élaboration de l'avant-projet de LPD nécessitait une collaboration des milieux économiques. En Suisse, Economie Suisse a représenté les milieux économiques [1582].

1923 Comme l'illustre la Suisse, les différents ordres juridiques ne traduisent pas de manière identique, l'objectif d'efficience économique assigné au droit de la protection des données. Le Règlement européen tente de trouver un équilibre entre des intérêts multiples. Dans le respect des finalités économiques, le Règlement introduit des garanties fortes pour les personnes concernées : pouvoirs des autorités de contrôle renforcés et action civile en responsabilité pour la compensation des dommages et le versement de dommages et intérêts contribuent à la protection de la sphère privée. La Suisse fait face à cette question d'équilibre des rapports de force et de la prise en considération d'autres finalités que les finalités économiques. La prise en considération d'objectifs d'ordre politique ou social voire la reconnaissance de l'action civile en responsabilité

1580. Pato Alexia, *The Collective Private Enforcement of Data Protection Rights in the EU*, in : MPI-IAPL Summer School 3rd edition 2019, p. 10.

1581. Conseil fédéral, *Une meilleure protection des données et un renforcement de l'économie suisse.*

1582. Djonova Ivette, *La coexistence de plusieurs normes en matière de protection des données pèse sur les entreprises suisses*, in : Economiesuisse (https ://www.economiesuisse.ch/), Zürich 2019, p. « https : / / www . economiesuisse . ch / fr / articles / la - coexistence - de - plusieurs - normes - en - matiere-de-protection-des-donnees-pese-sur-les » (22/12/2019).

avec possibilité de *class action*, comme une condition au sein de l'activité économique apparaissent comme des éléments de réflexion essentiels à toute élaboration normative aujourd'hui.

La protection des données personnelles était à l'origine une question éthique et est devenue plus tard une question économique. Les développements technologiques et la convergence de la biologie, des sciences cognitives et de l'informatique combinée à la disponibilité d'un grand nombre de données à caractère personnel renforcent encore la dimension éthique de ce droit. 1924

Preuve en est que des considérations de protection des données sont intégrées dans l'analyse de l'éthique des projets de recherche dans l'UE [1583]. 1925

Quant au droit européen de la protection des données, il se fonde sur des considérations éthiques comme l'illustre l'obligation faite au responsable du traitement de faire preuve de loyauté et de respecter le principe de transparence (art. 5 RGPD). 1926

Ces deux exemples illustrent l'interdépendance croissante entre les considérations éthiques, la protection des données et l'activité économique. Ce courant s'inscrit dans le cadre de la responsabilité sociale des entreprises. Cette perspective est spécifique à l'UE, comme le confirme l'adoption du Règlement européen et des lignes directrices en matière éthique pour le développement de l'intelligence artificielle [1584]. 1927

Ces outils législatifs deviennent cependant des standards de référence au niveau mondial. 1928

De manière similaire au droit de la concurrence, le droit de la protection des données détient une dimension politique. Le choix fondamental qui sous-tend ce droit, en faveur de l'économie de marché, est lui-même politique. La protection des acteurs économiques 1929

1583. Directorate-General for Research and Innovation, *Horizon 2020 Programme - Guidance - How to complete your ethics self-assessment*, in : European Commission (https ://ec.europa.eu/), Brussels 2019, p. « http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf » (22/12/2019).

1584. High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, in : European Commission (https ://ec.europa.eu/), Brussels 2019, p. « https://ec.europa.eu/futurium/en/ai-alliance-consultation » (21/06/2019).

et des stratégies nationales correspond aux orientations du Conseil fédéral. Le Règlement européen présente quant à lui une conception du droit de la protection des données favorable tant à l'intervention de l'État qu'à la libre concurrence du marché.

I. L'action civile - Private Enforcement

A. La notion de Private Enforcement

1930 La notion de Private Enforcement est issue du droit de la concurrence, notamment en droit américain. Cette notion signifie qu'on va compter sur l'action en responsabilité civile, non pas tant pour sa fonction de compensation des dommages subis par les personnes qui intentent cette action, mais pour son effet dissuasif sur les autres acteurs, donc sur son effet « d'enforcement » de ce droit en parallèle de la mise en œuvre du contrôle a posteriori par les autorités de contrôle Public Enforcement.

1931 Le Private Enforcement est apparu en 1890 aux Etats-Unis avec l'adoption du Sherman Act. Le Clayton Act le consacre aujourd'hui aux Etats-Unis et reconnaît le principe de triplement du montant de réparation des dommages (Treble damage) [1585]. Les systèmes juridiques qui recourent au mécanismes du Private Enforcement adoptent un dispositif incitant les personnes lésées à ouvrir l'action civile pour obtenir la réparation de leur préjudice et ainsi à dissuader les autres acteurs de commettre des infractions en droit de la concurrence.

1932 Les États ayant une culture romano-germanique ne sont pas habitués au mécanisme de Private Enforcement. Si en droit européen, le Private Enforcement est quasi inexistant, les citoyens américains recourent en revanche largement à lui. Le Private Enforcement représente en effet 90 pour cent de la mise en œuvre du droit antitrust américain, contre 10 pour cent pour le mécanisme de Public Enforcement [1586].

1585. Arrêt de la Cour suprême américaine, 15 U.S.C. § 15. En offrant aux justiciables la perspective d'un recouvrement au triple du montant du dommage, le Congrès a encouragé ces personnes à endosser le rôle de « procureur général privé ».

1586. Hurni, *L'action civile en droit de la concurrence*, p. 536.

B. Les éléments principaux du Private Enforcement en droit américain

Le Private Enforcement, en droit américain se caractérise par plusieurs éléments : 1933

- un dédommagement au triple (treble damages),
- l'exclusion de la répercussion des surcoûts (passing-on defence),
- la procédure de discovery, qui permet à une partie d'accéder aux preuves détenues par son adversaire, des accords de paiement d'honoraires conditionnels dépendant du succès de l'action intentée (contingency fees agreements),
- la limitation de responsabilité des bénéficiaires de clémence, et
- le modèle des *class action* [1587].

C. Le Private Enforcement en droit européen

a) Le principe

Le Règlement européen consacre l'apparition de mécanismes de Private Enforcement en droit de la protection des données. Possibilités de class action et renversement du fardeau de la preuve, autant d'éléments qui renvoient aux mécanismes constitutifs du Private Enforcement en droit américain (sauf toutefois l'élément de treble damages). 1934

Si l'action civile en responsabilité ne constitue pas une nouveauté du Règlement et est propre à tout État de droit, (elle était déjà prévue par la directive 95/46/CE à l'art. 23, al. 1), la possibilité d'agir de manière collective en réparation des dommages (class action) et de demander le versement de dommages-intérêts en plus des sanctions administratives dissuasives, constitue un changement de paradigme, qui mérite d'être souligné [1588]. 1935

La class action peut avoir un effet transfrontalier. Citons á titre d'exemple la class action britannique qui impacte la banque UBS 1936

1587. Guerin Antoine, *Quelle doit être la place du public enforcement et du private Enforcement en droit de la concurrence ?*, thèse, Paris 2016, pp. 1-85.
1588. Kern / Epiney, *Durchsetzungmechanismen im EU*, p. 27.

établie en Suisse, dans le domaine financier [1589]. Ce mécanisme de class action a vocation a obtenir le versement de dommages et intérêts pour des personnes physiques, en réparation d'un dommage. Dans le cas d'espèce, ce dommage trouvait sa source dans des manipulations des marchés des changes.

1937 Comme dans tout État de droit, l'action civile en responsabilité garantit à toute personne victime d'une violation des dispositions légales, l'accès à un juge, indépendamment de la politique menée par l'autorité de contrôle national. Le Règlement standard d'un recours juridictionnel effectif, posé par le Règlement est quant à lui, beaucoup plus élevé.

1938 Le Règlement exige que l'action en responsabilité offerte par les États soit réellement « un recours juridictionnel effectif » (art. 79 RGPD) pour les personnes physiques (voir section B.). Les tribunaux européens pourraient ultérieurement introduire en droit européen de la protection des données, l'obligation de la gratuité de la représentation voire la pratique américaine des « triple damages ». La jurisprudence européenne marquerait ainsi sa volonté de renforcer à la fois l'effectivité des recours et l'aspect dissuasif de l'action civile en responsabilité.

1939 La personne lésée par la violation d'une disposition du Règlement « a droit à un recours juridictionnel effectif à l'encontre du responsable du traitement (art. 79 RGPD), si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement » (voir section B.).

1940 La jurisprudence de la CJUE viendra préciser l'interprétation de cette notion et éventuellement créer de nouveaux droits pour les personnes concernées, comme la gratuité de la représentation.

b) Les conditions de l'action civile

1941 La personne concernée doit pouvoir justifier qu'elle a subi un dommage ayant pour cause la violation des dispositions du Règlement. L'intérêt à agir du demandeur constitue également une condition

1589. ATS, *UBS visée par une action collective en Grande-Bretagne*, in : Le Temps (https ://www.letemps.ch/), Lausanne 2019, p. « https://www.letemps.ch/economie/ubs-visee-une-action-collective-grandebretagne » (30/07/2019).

de recevabilité de la demande.

En droit européen de la protection des données, il y a cependant renversement du fardeau de la preuve. C'est au responsable du traitement et au sous-traitant de démontrer qu'il a pris les mesures techniques et organisationnelles appropriées eu égard au risque du traitement (voir paragraphe 941). 1942

Le droit européen de la protection des données accorde ainsi une protection spécifique au demandeur. Cela s'explique par la volonté du législateur européen de protéger la personne dont les données sont traitées. 1943

c) Les caractéristiques du Private Enforcement en droit européen de la protection des données

1. La class action

Le Règlement donne le droit aux personnes concernées d'ouvrir une action collective en responsabilité pour obtenir la condamnation d'un responsable du traitement et d'un sous-traitant ainsi que le versement de dommages-intérêts, en cas de traitement illicite en vertu du Règlement (art. 80 RGPD). 1944

Ainsi les personnes qui s'estiment lésées par un traitement de données personnelles et qui ont subi un même dommage de la part d'un responsable du traitement, ont le droit de se regrouper pour agir en justice. 1945

Une class action pourra par exemple être intentée au motif d'une violation des obligations du responsable du traitement ou sur le fondement d'un abus d'exploitation [1590]. Le Règlement renforce les obligations du responsable du traitement et du sous-traitant, notamment la place du consentement dans le cadre de la collecte de données. En effet, le consentement doit être donné librement, être spécifique, éclairé et univoque. L'acceptation de la personne concernée doit résulter d'un acte positif clair. Si « l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas 1946

1590. Bundeskartelamt, *Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung (B6 26/16, CCE 2019, Étude 13)*, in : Bundeskartelamt (https://www.bundeskartellamt.de/), Bonn 2019, p. « https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html » (30/06/2019).

nécessaire à l'exécution dudit contrat » (art. 7 RGPD), le consentement ne sera pas libre. En outre, seules les données strictement nécessaires aux finalités du traitement peuvent être collectées, en vertu du principe de minimisation.

1947 Le Réglement introduit les actions collectives en responsabilité civile et en réparation des dommages avec le versement de dommages-intérêts. L'article 80 RGPD accorde à la victime subissant un dommage ayant pour cause la violation des dispositions du Règlement, le droit de mandater un organisme, une association ou une organisation afin qu'il/elle la représente dans l'exercice de ses droits devant les tribunaux ou l'autorité de contrôle. Cet article requiert des législateurs nationaux la transposition de ce principe de Private Enforcement en droit interne. Cela constitue une nouveauté, car un Règlement européen ne requiert aucune transposition en droit interne contrairement à une directive européenne [1591]. Ainsi la mise en œuvre effective du Private Enforcement sur la base de la class action dépend des spécificités nationales. Bien que le Règlement ne soit pas d'application directe en Suisse, car la Suisse ne fait pas partie de l'UE, le maintien de la décision d'adéquation pourrait être influencé par l'intégration ou non de l'article 80 RGPD en droit suisse.

1948 L'art. 80 du Règlement précise que « la personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, pour qu'il introduise une réclamation en son nom et exerce en son nom les réclamations et recours juridictionnels afin d'obtenir réparation ».

1949 Le Règlement offre donc la possibilité aux personnes lésées d'obtenir une réparation financière du préjudice subi dans le traitement de leurs données personnelles. Cette possibilité d'une action collective constitue l'innovation majeure du Règlement.

1950 Cette réglementation européenne constitue la concrétisation d'une

1591. Pato, *The Collective Private Enforcement of Data Protection Rights in the EU*, p. 6.

volonté politique d'encourager les class action dans l'Union [1592].

Les personnes lésées en Suisse pourront intenter une action civile sur la base de l'art. 41 CO uniquement. Une action collective en réparation sera envisageable, si le projet de modernisation du code de procédure civile est approuvé par le Parlement [1593]. 1951

2. Le renversement du fardeau de la preuve

Le Règlement impose au responsable du traitement et au sous-traitant qui traite des données personnelles de prouver la conformité des traitements au Règlement. En particulier, la preuve du caractère approprié des mesures techniques et organisationnelles devra être apportée, en cas de contrôle a posteriori des autorités de contrôle ou en cas d'action civile (voir paragraphe 941). 1952

La preuve de la conformité pourra être apportée grâce aux éléments suivants : 1953

- un registre des activités de traitements pour les responsables de traitements.
- des analyses d'impact sur la protection des données.
- la preuve de la licéité des traitements (ex : recueil du consentement).
- la preuve de l'information des personnes.
- la preuve du respect des principes de l'art. 5 RGPD.
- la documentation des procédures permettant l'exercice effectif des droits des personnes.
- les contrats avec les sous-traitants qui doivent être conformes au Règlement.
- les procédures instaurées en cas de violations de données.

1592. Commission européenne, *« Vers un cadre horizontal européen pour les recours collectifs » - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 11 juin 2013 (COM(2013) 401 final)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2013, p. « https : / / eur - lex . europa . eu / legal - content/FR/TXT/PDF/?uri=CELEX:52013DC0401 » (03/04/2020).

1593. OFJ, *Modification du code de procédure civile*, in : OFJ (https ://www.bj.admin.ch/), Berne s.a., p. « https : / / www . bj . admin . ch/bj/fr/home/staat/gesetzgebung/aenderung-zpo.html » (30/06/2019).

1954 Des amendes dissuasives pourront sanctionner un responsable du traitement ou un sous-traitant non diligent (art. 83 RGPD) et une action en responsabilité pourra nuire à l'image de l'organisation.

D. Vers un mécanisme de Private Enforcement en droit suisse ?

1955 Il n'existe pas de procédure similaire au Private Enforcement en droit suisse.

1956 Le projet de LPD révisée n'apporte aucun élément pouvant laisser penser que la notion de Private Enforcement va être incorporée au droit suisse. En effet, le droit de la protection des données ne reconnaît pas les concepts de *class action*, ni de renversement de la charge de la preuve, reconnus par le Règlement.

1957 Cette absence pourrait potentiellement soulever un problème politique dans le maintien de la décision d'adéquation entre la Suisse et l'UE.

1958 Seule la procédure de consultation du Conseil fédéral relative à la révision du Code de procédure civile, qui envisage la reconnaissance du mécanisme de « class action » et la jurisprudence récente du Tribunal fédéral constituent des indices tendant à démontrer une réflexion dans cette direction.

1. Le mécanisme de Class Action

1959 Le 2 mars 2018, le Conseil fédéral a ouvert une consultation sur une modification générale du code de procédure civile, qui s'est achevée le 11 juin 2018. Cette réforme vise à faciliter l'accès aux tribunaux et à améliorer l'exercice des droits civils. En particulier, le Conseil fédéral veut « développer la mise en œuvre collective des droits [1594] ». Le Conseil fédéral suit ainsi l'approche de plusieurs pays européens dont la France et le Portugal.

1960 Le Conseil fédéral propose « l'institution d'une transaction de groupe, qui déploie ses effets sur l'ensemble des lésés. Il prévoit en outre un élargissement de l'action des organisations permettant aux asso-

1594. DFJP, *Procédure civile : faciliter l'accès aux tribunaux des particuliers et des entreprises - Communiqué du Conseil fédéral du 2 mars 2018*, in : DFJP (https ://www.ejpd.admin.ch/), Berne 2018, p. « https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2018/2018-03-02.html » (03/04/2020).

ciations et organisations de faire valoir des prétentions collectives en réparation des dommages ».

Les entreprises auront ainsi un point de contact avec une seule organisation représentant les intérêts des personnes lésées en cas de dommages collectifs. Cela facilitera le règlement des litiges. 1961

Selon l'avant-projet de réforme du code de procédure civile, les organisations sans but lucratif seront fondées à demander des dommages-intérêts au nom de leurs membres ou la remise d'un gain illicite, dans l'éventualité d'un enrichissement illégitime. Les statuts devront expressément mentionner cette capacité de représentation. Le Conseil fédéral propose le système de l'opt-in : les personnes qui souhaitent se joindre à l'action devront s'annoncer explicitement. Une baisse des avances de frais et un système de transaction de groupe à l'amiable sont prévus. Un groupe de personnes pourra ainsi faire valoir un dommage économique (art. 89 AP-CPC) et exercer une action en réparation du dommage [1595]. 1962

En droit suisse, comme dans tout État de droit, les personnes physiques ou morales peuvent agir devant les juridictions civiles pour exercer leurs droits et faire valoir leurs prétentions juridiques [1596], tant en droit de la concurrence qu'en droit de la protection des données. Les montant des dommages-intérêts perçus sont cependant limités lorsqu'il n'y a pas d'atteinte au patrimoine [1597]. Le demandeur doit démontrer la faute ou la négligence du responsable du traitement ce qui pourrait être qualifié d'entrave à l'effectivité du recours juridictionnel exigé en droit européen en vertu du Règlement (art. 79 RGPD). 1963

Or un nombre croissant de dommages patrimoniaux est susceptible d'apparaître du fait de la transformation digitale en cours et de l'accroissement du nombre de traitements de données personnelles par des objets connectés avec l'essor de la 5G. 1964

Bien que le Conseil fédéral envisage l'évolution vers une class action, le droit suisse en vigueur ne reconnaît pas le mécanisme des *class action* de manière générale, ni en droit de la concurrence ni en droit de la protection des données. Pourtant, les *class action* fa- 1965

1595. *Ibidem.*
1596. Hurni, *L'action civile en droit de la concurrence*, p. 88.
1597. Widmer Pierre, *Aspects de responsabilité civile*, in : « La nouvelle loi fédérale sur la protection des données » (CEDIDAC), Lausanne 1994/28, p. 194.

vorisent un plus grand accès à la justice [1598]. En effet, cette action collective permet aux lésés de se regrouper pour faire valoir leurs droits, ce qui est particulièrement important dans les cas de dommages collectifs ou dispersés [1599].

1966 La *class action* a également une fonction préventive : elle garantit la réparation du dommage et la sanction du responsable du traitement ou du sous-traitant. Elle responsabilise les acteurs économiques et incite ces derniers être diligents dans le traitement des données, afin de prévenir l'apparition des dommages. Enfin, elle favorise les économies de procédure en limitant les frais de justice [1600].

1967 Les opposants au système de *class action* en Suisse invoquent la tradition juridique suisse et le risque « d'adversarial legalism », du droit américain [1601].

1968 Rejoignant l'avis de la doctrine et du législateur européen, il apparaît que le droit de la concurrence comme le droit de la protection des données sont deux domaines pour lesquels la reconnaissance de moyens collectifs d'actions se justifient, voire s'imposent. Reconnaître la capacité d'agir en réparation du dommage subi par ses membres à l'association constituerait une première étape importante.

1969 Lorsque le montant du dommage individuel est insuffisant pour justifier économiquement une action civile individuelle, (rapport coût/bénéfice négatif du fait des frais du procès par rapport à la probabilité d'obtenir gain de cause), le mécanisme de *class action* est central pour responsabiliser le responsable du traitement et réparer le dommage subi qui peut être partagé entre un grand nombre de personnes. L'absence de *class action* en droit suisse a pour conséquence l'absence de réparation du dommage. À titre d'exemple, il est possible de citer l'action en justice, intentée contre l'entreprise Volkswagen, par l'association allemande de consommateurs VZBV pour avoir truqué 11 millions de ses véhicules dont 2,4 millions vendus en Allemagne. Au 2 janvier 2019, plus de 372'000 propriétaires étaient inscrits au registre ouvert par VZBV pour lancer une *class*

1598. Hurni, *L'action civile en droit de la concurrence*, p. 451.
1599. *Ibidem.*
1600. *Idem*, p. 452
1601. *Idem*, p. 452

action [1602].

En Suisse, le système juridique impose aujourd'hui que chaque demandeur fasse valoir ses prétentions de manière individuelle. Seul l'art. 89 CPC autorise expressément une organisation à « défendre les intérêts d'un groupe de personnes déterminé ». Une association peut ainsi en son nom propre, agir pour l'atteinte à la personnalité des membres de ce groupe. Toutefois, il s'agit d'une action défensive uniquement et non pas d'une action en responsabilité du tort moral et en réparation du dommage. L'association peut demander au juge l'interdiction d'une atteinte illicite si elle est imminente, la cessation de l'atteinte, si elle dure encore, ou le constat de son caractère illicite, si le trouble qu'elle a créé subsiste [1603]. Elle ne peut pas demander de réparation du dommage sous la forme du versement de dommages-intérêts, à moins qu'une loi fédérale en dispose autrement ce qui n'est pas le cas à ce jour. Une révision du code de procédure civile constituerait ainsi une avancée majeure dans la protection effective des personnes physiques, dont les données personnelles sont traitées. 1970

Le Conseil fédéral exclut les actions collectives en réparation dans le projet de LPD révisée. Or, le but principal du Règlement, tel qu'il ressort du considérant 13 RGPD, au même titre que la libre circulation des données à caractère personnel, est de rendre l'action civile aussi efficace que possible. Dès lors, comment la Suisse va-t-elle démontrer à la Commission européenne qu'elle offre un cadre juridique adéquat, justifiant le maintien de la décision d'adéquation, si elle ne peut pas attester que le droit suisse de la protection des données accorde une place centrale à l'action civile, en sachant qu'elle constitue justement la clé de voûte du système conçu par le Règlement ? 1971

A défaut de reconnaissance officielle des actions collectives dans le projet de LPD révisée, le Parlement devra approuver la modernisation du code de procédure civile [1604]. Cette approbation sera déterminante pour l'évolution de l'action civile en droit suisse, la réparation effective des dommages et le maintien de la décision d'adé- 1972

1602. Tribune de Genève, *372'000 clients rejoignent l'action groupée contre VW*, in : Tribune de Genève (https ://www.tdg.ch/), Genève 2019, p. « https://www.tdg.ch/economie/372-000-clients-rejoignent-laction-groupee-vw/story/16603789 » (30/06/2019).

1603. Hurni, *L'action civile en droit de la concurrence*, p. 445.

1604. OFJ, *Modification du code de procédure civile.*

quation.

1973 Si le Conseil fédéral renonce à l'action collective pour réparation des dommages en droit suisse, alors la personne lésée pourra uniquement intenter une action défensive, en constatation de droit, à l'encontre du responsable du traitement (art. 28, al. 2 CC), devant le juge civil compétent. Si le responsable du traitement est un organe fédéral, il pourra agir défensivement contre l'organe responsable sur le fondement de l'art. 37 P-LPD en recourant le cas échéant contre la décision de celui-ci auprès de l'autorité de recours compétente. Il ne s'agira pas d'une action en réparation. En parallèle, le Préposé fédéral pourra ouvrir, d'office ou sur dénonciation, une enquête contre un organe fédéral ou contre une personne privée (art. 43 P-LPD). En droit européen de la concurrence, la Commission européenne a également le droit discrétionnaire d'ouvrir une enquête à la suite d'une plainte, lorsqu'un intérêt public est en jeu [1605]. Il en est de même en droit suisse. La Comco peut ouvrir une enquête préalable en droit suisse, lorsque l'intérêt public est en cause.

1974 Si l'action collective proprement dite n'est pas reconnue en droit suisse de la protection des données, les demandeurs peuvent cependant regrouper leurs actions (notion de consorité [1606]). Ainsi plusieurs demandeurs peuvent agir conjointement pour des faits ou des prétentions juridiques semblables, sur le fondement de l'art. 71, al. 1 et 2 CPC. Le Message du CPC indique que la « consorité joue en quelque sorte le rôle d'action collective [1607] ». Chaque demandeur dispose de la qualité de partie et procède de son propre gré [1608].

1975 Si une association peut demander au juge l'interdiction, la cessation ou la constatation de l'atteinte [1609], elle ne peut pas demander réparation du dommage subi par ses membres [1610]. Quant au consommateur, il n'a pas qualité pour agir sur la base de l'art. 12LCArt [1611]. Il peut en revanche intenter une action civile en application de l'art.

1605. Hurni, *L'action civile en droit de la concurrence*, p. 150 ; Arrêt Tribunal de première instance du 18 septembre 1992, *Automec Srl c. Commission*, T-2490, Rec. 1992, p. II-2223.
1606. Hurni, *L'action civile en droit de la concurrence*, p. 444.
1607. *Ibidem.*
1608. Message du 28 juin 2006 relatif au code de procédure civile suisse (06.062), FF 2006 p. 6895.
1609. art. 89 al. 2 CPC.
1610. Hurni, *L'action civile en droit de la concurrence*, p. 295.
1611. *Idem*, p. 296.

41 CO [1612]. Pour démontrer l'illicéité du comportement, le consommateur doit établir que le dommage résulte de la violation d'une norme de comportement dont le but est de protéger son patrimoine [1613].

2. La jurisprudence du Tribunal fédéral

1976 En droit américain, la procédure de « Pre-Trial Discovery » impose à la partie adverse la communication de toute information pertinente pour le litige [1614]. Cette procédure facilite la production de preuves pour la partie lésée qui fait valoir ses prétentions dans le cadre d'une procédure civile. Cette procédure de « Pre-Trial Discovery » n'existe pas en droit suisse. L'art. 8 LPD et l'art. 400 CO offrent cependant des garanties aux personnes concernées pour obtenir accès aux données personnelles les concernant.

1977 Le Tribunal fédéral a précisé le champ d'application de l'art. 8 LPD dans un arrêt récent [1615]. Dans cet arrêt, deux personnes ont demandé à leur banque de leurs communiquer toutes les données personnelles les concernant, sur le fondement de l'article 8 LPD. Le Tribunal fédéral a analysé l'argument de la banque qui contestait l'exercice par ses clients du droit d'accès prévu par la LPD et le qualifiait d'abus de droit au sens de l'art. 2, al. 2 CC, au motif que la demande viserait exclusivement un accès à des preuves dans le but d'exercer une action civile en dommage-intérêts et ne serait donc pas liée à la protection des données. Le Tribunal fédéral a rappelé que le droit d'accès de l'art. 8 LPD n'était pas destiné à faciliter la récolte de preuves ou à interférer dans le droit de procédure civile [1616]. Le Tribunal fédéral a rejeté le recours de la banque au motif qu'elle n'avait pas démontré l'abus de droit, c'est—à-dire que « les clients voulaient se procurer un avantage qui n'est pas prévu par la procédure civile, ou ont intenté une fishing expedition interdite ». Le Tribunal a retenu que « la banque ne disposait pas d'intérêt prépondérant qui s'opposait à la communication des

1612. Stoffel Walter A., *Das neue Kartell - Zivilrecht*, in : Zäch Roger (édit.), *Neue schweizerische Kartellgesetz*, 1e éd., Zürich 1996, p. 102.
1613. Hurni, *L'action civile en droit de la concurrence*, p. 296.
1614. Fischer Philipp / Richa Alexandre, *U.S. pretrial discovery on Swiss soil*, 1e éd., Basel 2010 ; Von Burg Johanna, *L'exécution fidèle : le devoir de discrétion / le secret bancaire du négociant*, in : Bizzozero Alessandro / Falleti André / Meregalli Do Duc Samantha (édit.), *Le mandat de gestion de fortune*, 2e éd., Zürich 2017, p. 341.
1615. ATF 138 III 425.
1616. Hirsch Célian, *L'accès aux données d'une procédure au regard de la LPD : une tentative abusive de Pre-Trial Discovery ?*, in : Jusletter 2018/17, p. 6.

données personnelles ».

1978 Cette jurisprudence restreint l'application de l'abus de droit lors d'une requête d'accès aux données au sens de la LPD. « En effet, il suffira que le demandeur invoque le fait de vouloir vérifier l'exactitude de ses données personnelles et la partie adverse ne pourra que difficilement prouver l'abus de droit [1617] ».

1979 La doctrine considère que « le droit d'accès reste donc envisageable même pour obtenir des moyens de preuve pour un potentiel litige à venir, sauf s'il s'agit d'un abus manifeste parce que la demande vise un but exclusivement étranger à la LPD [1618] ».

1980 Cette jurisprudence du Tribunal fédéral a été confirmée pour des salariés de l'entreprise : « la requête de l'employé visant à obtenir les données le concernant en vue d'une éventuelle action en dommages-intérêts contre le maître du fichier n'est (...), en soi, pas abusive [1619] ».

1981 Ainsi, invoquer l'abus de droit pour restreindre le droit d'accès a peu de chances d'aboutir, même si l'action est motivée par la volonté de la partie de se constituer des éléments de preuve dans le cadre d'un litige ultérieur.

1982 Lorsqu'un tiers non impliqué dans une procédure exerce son droit d'accès [1620], le Tribunal fédéral est d'avis que la LPD est applicable sans restriction au tiers. Si une personne n'est pas partie à la procédure, alors elle doit être protégée par la LPD, car elle ne peut pas invoquer les droits de procédure qui lui permettraient d'avoir accès au dossier.

1983 Les tiers ont le droit de consulter le dossier selon la LPD, unique-

1617. Fuhrer Stephan, *Anmerkungen zu privatversicherungsrechtlichen Entscheidungen des Bundesgerichts*, in : HAVE : Haftung und Versicherung = REAS : responsabilité et assurance 2013, p. 141.
1618. Benhamou Yaniv / Braidi Guillaume / Nussbaumer Arnaud, *La restitution d'informations : quelques outils à la disposition du praticien*, in : Pratique juridique actuelle 2017/11, p. 1314.
1619. ATF 141 III 119, consid. 7.1.1.
1620. ATF 4A 188/2015 du 31 août 2015, consid. 3.2.1 ; Hirsch, *L'accès aux données d'une procédure au regard de la LPD*, p. 13 ss.

ment lorsque la procédure est clôturée [1621].

Désormais, les tribunaux devront vérifier s'il « existe ou non, au point de vue fonctionnel, un lien immédiat avec une procédure (devant un tribunal). Ce sera le cas lorsque l'exercice de ce droit a des effets concrets sur cette procédure ou sur son issue, ou sur les droits procéduraux des parties [1622] ». 1984

En droit suisse, l'action du demandeur conditionne l'ouverture d'une action civile en responsabilité. En droit européen de la protection des données, le demandeur a le choix entre la saisine du juge civil (Private Enforcement) ou le dépôt d'une réclamation auprès d'une autorité de contrôle (Public Enforcement), en cas de violation des dispositions du Règlement (art. 77 RGPD). Il nous faut donc analyser le concept de Public Enforcement. 1985

II. L'action administrative - Public Enforcement

A. Droit européen de la protection des données

Le Règlement européen respecte la double compétence des juridictions civiles et administratives. En application du principe d'indépendance des procédures [1623], la procédure de Public Enforcement co-existe avec la procédure civile (chapitre VIII RGPD). 1986

L'action administrative de Public Enforcement s'exerce tout d'abord au niveau européen. Le Contrôleur européen sur la protection des données a le pouvoir de prendre des décisions contraignantes et de rendre des avis, dans le but de garantir l'application cohérente du Règlement dans l'Union [1624]. 1987

L'action administrative de Public Enforcement s'exerce également au niveau de chaque État membre de l'Union par l'intermédiaire des autorités de contrôle nationales. Celles-ci « exercent en toute indépendance les missions et les pouvoirs » dont elles sont investies (art. 52 RGPD). Ces autorités disposent de prérogatives étendues et d'un pouvoir de contrainte (art. 58 RGPD). À titre d'exemple, elles peuvent mener des enquêtes tant à l'égard des personnes physiques que des organes fédéraux. Elles peuvent également conduire des 1988

1621. Message du 15 septembre 2017, p. 6635.
1622. *Idem*, note 92.
1623. Hurni, *L'action civile en droit de la concurrence*, p. 167.
1624. art. 68 - 76 ss. RGPD.

investigations et des audits. Elles sont autorisées à lancer des poursuites et prononcer des amendes administratives (art. 83 RGPD). Elles peuvent interdire certains traitements ou les limiter, voire retirer un certificat de conformité au Règlement [1625]. Elles détiennent des prérogatives d'admonestation, de suspension ou d'interdiction du traitement à l'autorité de contrôle. Elles peuvent exiger la notification de la violation de données en cas de risque élevé pour les droits des personnes concernées (art. 34, al 4 RGPD). Dans le cadre d'un fonctionnement en réseau, elles coopèrent entre elles et échangent des informations notamment dans le cadre du mécanisme du contrôle de la cohérence.

1989 L'action de Public Enforcement des autorités de contrôle nationales est renforcée par le régime des sanctions institué par le Règlement.

1990 Les sanctions imposées par les autorités nationales en cas de violation du Règlement sont dissuasives dans leur montant (art. 83, al. 6 RGPD). Les autorités de contrôle peuvent en effet imposer des sanctions administratives d'un montant pouvant atteindre jusqu'à EUR 20 millions ou 4 pour cent du chiffre d'affaires (art. 83 RGPD). Si le système juridique d'un État membre ne prévoit pas d'amende administrative, l'amende sera imposée par une juridiction nationale compétente avec effet équivalent aux amendes administratives prononcées par une autorité de contrôle [1626].

1991 Tous ces éléments démontrent que la mise en œuvre du droit européen de la protection des données repose également sur des mécanismes de Public Enforcement. Ce cadre juridique a pour objectif d'assurer l'effectivité des règles de protection des données dans l'UE.

1992 L'action administrative du Public Enforcement présente cependant uniquement un caractère punitif. Elle relève de l'ordre public, rend les acteurs économiques responsables des violations du Règlement, mais ne poursuit pas un objectif de réparation du dommage. En 2013, la Commission européenne a publié un rapport mentionnant le faible nombre de recours en réparation dans les États-membres de l'UE, à l'exception du Royaume-Uni, de l'Allemagne et des Pays-

1625. Paal / Pauly, *Datenschutz - Grundverordnung Bundesdatenschutzgesetz*, p. 722 ss.
1626. art. 83, al. 9 RGPD.

Bas, qui affichaient un taux satisfaisant [1627].

Quelle est la situation en droit suisse ? 1993

B. Droit suisse

En droit suisse, la mise en œuvre du droit suisse de la protection des données incombe au Préposé fédéral à la protection des données et à la transparence. 1994

Le Conseil fédéral renforce les pouvoirs du Préposé. Celui-ci devrait disposer de pouvoirs d'enquête, d'investigation et d'intervention [1628]. Ces pouvoirs sont cependant très insuffisants au regard du mécanisme de Public Enforcement mis en œuvre par le Règlement européen, qui repose sur des pouvoirs de sanction, octroyés aux autorités de contrôle des États membres de l'Union (art. 58 RGPD). 1995

Dans ces conditions, comment être, pour le Préposé fédéral, le garant du respect effectif du droit fondamental à la protection des données personnelles ? 1996

Le Public Enforcement poursuit un objectif injonctif et dissuasif. Les autorités de contrôle en Suisse n'auront pas le pouvoir de prendre des sanctions administratives dissuasives et de faire cesser les pratiques illicites en droit de la protection des données. Les sanctions seront prononcées par les autorités pénales des cantons (voir paragraphe 1877 et art. 59 P-LPD), à l'encontre des parties à la procédure (personne concernée ou organe fédéral), lorsqu'une enquête a été ouverte. Les pouvoirs des autorités de contrôle devraient viser à faire cesser une atteinte, à dissuader une entreprise condamnée de réitérer son comportement illégal en droit de la protection des données et à décourager les autres entreprises de s'engager dans des pratiques similaires. 1997

À l'issue de la réforme de la LPD, le Préposé devrait pouvoir dé- 1998

1627. European Commission, *Impact Assessment Report : Damages actions for breach of the EU antitrust rules. Accompanying the proposal for directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (COM(2013) 404 final / SWD(2013) 204 final)*, in : EUR-Lex (https ://eur-lex.europa.eu/), Brussels 2013, p. « https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0203 » (03/04/2020), consid. 52.

1628. Message du 15 septembre 2017, p. 6706.

clencher une action sur plainte ou sur dénonciation, prendre des décisions, dans le cadre de ses pouvoirs d'enquête ou sur mesures provisionnelles (art. 43 et 44 P-LPD), ou au titre de mesures administratives (art. 45 LPD), en cas de violation des disposition légales. Le Préposé ne pourra pas ouvrir d'action en réparation du dommage, ni prendre de sanction pénale.

1999 Le projet de LPD révisé prévoit le droit pour le Préposé d'échanger des données personnelles avec une autorité étrangère chargée de la protection des données et une assistance administrative entre autorités de contrôle. Ce mécanisme d'assistance administrative repose sur les principes de réciprocité entre la Suisse et l'État étranger et sur le principe de spécialité. Si les données transmises doivent être utilisées ultérieurement dans le cadre d'une procédure pénale, les dispositions sur l'entraide judiciaire internationale en matière pénale s'appliqueront. Le Conseil fédéral préconise le respect des secrets professionnels, d'affaires et de fabrication et l'interdiction que les informations et les données échangées soient communiquées à des tiers sans l'accord préalable de l'autorité qui les a transmises.

2000 Enfin, le cumul des fonctions de surveillance et de conseil du Préposé limite la prise d'initiative des responsables du traitement, dans le domaine de la protection des données [1629]. Une séparation stricte des fonctions de conseil et de surveillance serait nécessaire pour que le Préposé remplisse pleinement sa double fonction de conseil et d'autorité de contrôle. On aurait pu imaginer un modèle basé sur une double institution : le rôle de conseil aurait pu être attribué à un établissement fédéral autonome de la Confédération et le Préposé aurait pu conserver la mission de surveillance uniquement. Les acteurs économiques et les citoyens auraient ainsi bénéficié d'un guichet unique d'information sur la protection des données.

2001 Le Préposé aurait également pu, tel le ministère public de la Confédération représenter la protection des données en tant qu'institution et obtenir le pouvoir d'agir en responsabilité et en réparation des atteintes issues d'une violation de la protection des données. Cette prérogative de Public Enforcement serait venue compléter l'action civile des personnes physiques et aurait facilité le maintien

1629. Sauvain Monique Cossali, *L'effectivité des mécanismes de mise en oeuvre du point de vue de l'OFJ*, in : Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015, p. 128.

de la décision d'adéquation de l'Union en contribuant au double but du Règlement : la libre circulation des données et la responsabilisation des acteurs traitant des données à caractère personnel.

Chapitre 3: La portée extraterritoriale du RGPD

§1 Le caractère extra-territorial du Règlement général sur la protection des données

L'objet de cette partie est d'analyser la portée du champ d'application extra-territoriale du Règlement général sur la protection des données (ci-après RGPD), qui est entré en vigueur le 25 mai 2018. Le RGPD a bénéficié d'un retentissement international certain depuis son entrée en vigueur et tend à se positionner dans le monde, comme l'une des normes de référence en matière de protection des données personnelles [1630]. Il annule et remplace la Directive européenne 95/46/CE (JOUE L 207, 1er aout 2016, p. 1) [1631]. Le RGPD a le double objectif de favoriser, d'une part, la libre circulation des données personnelles au sein de l'UE (art. 1 RGPD), tout en protégeant, d'autre part, les personnes physiques en garantissant un niveau de protection élevé contre les traitements de données [1632] et en responsabilisant les acteurs traitant des données personnelles (art. 1 RGPD). 2002

L'un des aspects novateurs du Règlement est son caractère extra-territorial, tel que stipulé à l'article 3 RGPD. Le législateur européen manifeste ainsi sa double volonté de garantir un niveau élevé de protection des données à la hauteur du droit fondamental à la protection des données qui est consacré à l'art. 8 de la Charte des droits fondamentaux de l'Union européenne et de l'art. 16 du Traité sur le fonctionnement de l'Union européenne [1633] et d'étendre le niveau de protection des données á des États tiers. Il crée un cadre géné- 2003

1630. Deroudille / Fatah, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, p. 442.

1631. Parlement européen et Conseil de l'UE, *Règlement (UE) 2016/679 du 27 avril 2016*, p. 1.

1632. Arrêt CJUE du 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI :EU :C :2019 :772, consid. 54.

1633. Gallardo Meseguer Marc, *Aperçu de la dimension internationale du Règlement général sur la protection des données à caractère personnel*, in : Grosjean Alain (édit.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e éd., Bruxelles 2015, p. 117.

ral de protection des droits de la personnalité, contre des atteintes á ce droit par des responsables du traitement établis en dehors de l'Union européenne [1634]. Il favorise ainsi une concurrence équitable entre les entreprises situées en-dehors de l'UE et dans l'Union européenne [1635]. La Commission européenne exporte ainsi son modèle de protection des données en-dehors de l'Union à tous les États bénéficiant d'une décision d'adéquation des législations.

2004 La question de l'extraterritorialité dans le domaine de la protection des données n'est pas nouvelle [1636] et a déjà suscité une abondante littérature dans le cadre de la Directive 95/46/CE [1637]. La jurisprudence de la Cour de Justice a également traité cette question dans l'arrêt Google vs. Spain [1638]. Dans cette affaire, la Cour de justice de l'Union européenne (CJUE) a estimé que le droit européen en matière de protection des données s'appliquait aux activités de Google

1634. Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*, p. 85.

1635. Gayrel Claire, *L'expansion des standards européens de protection des données dans le monde*, in : L'Europe des droits de l'homme à l'heure d'internet Bruxelles 2019, pp. 473-488.

1636. Moniz Graça Canto, *Finally : a coherent framework for the extraterritorial scope of EU data protection law - the end of the linguistic conundrum of Article 3 (2) of the GDPR*, in : UNIO–EU Law Journal 2018 4/2, p. 105 ss.

1637. Poullet Yves, *Transborder data flows and extraterritoriality : The European Position*, in : Journal of International Comercial Law and Technology 2007 2/3, p. 141 ; Bauchner Joshua S., *State sovereignty and the globalizing effects of the Internet : A case study of the privacy debate*, in : Brooklyn Journal of International Law 2000 26/2, p. 696 ; Bygrave Lee A., *European Data Protection : Determining Applicable Law Pursuant to European Data Protection Legislation*, in : Computer Law & Security Review 2000 16/4, p. 252 ; Moerel Lokke, *Back to basics : when does EU data protection law apply ?*, in : International Data Privacy Law 2011 1/2, p. 97 ; Moerel Lokke, *The long arm of EU data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ?*, in : International Data Privacy Law 2010 1/1, p. 30 ; Groupe de Travail de l'Article 29, *Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE - Adopté le 30 mai 2002 (WP 56)*, in : CNPD (https ://cnpd.public.lu/), Luxembourg 2002, p. « https://cnpd.public.lu/dam-assets/fr/dossiers-thematiques/nouvelles-tech-communication/cybersurveillance-lieu-travail/wp56_fr_pdf.pdf » (03/04/2020).

1638. Arrêt de la CJUE du 13 mai 2014, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12, ECLI :EU :C :2014 :317, consid. 55.

Inc. établie à l'étranger [1639].

Les dispositions relatives au champ d'application territorial de la législation de l'UE en matière de protection des données ont gagné en importance avec l'adoption du RGPD, puisque le champ d'application spatial de l'article 3 RGPD s'étend potentiellement au monde entier et qu'un mécanisme de coopération entre autorités de contrôle est désormais formellement prévu au sein de l'UE (mécanisme du guichet unique). 2005

La question de la portée du principe de l'applicabilité extra-territoriale du droit européen de la protection des données est régulièrement soulevée. Parmi les questions qui se posent figurent celle de la légitimité d'une telle application extra-territorialité, et de sa mise en oeuvre effective. Il s'agit donc d'examiner la licéité et l'effectivité de ce texte face aux ordres publics d'États tiers [1640]. 2006

La présente contribution se propose de comprendre les enjeux du caractère extraterritorial du Règlement et d'analyser une problématique spécifique dans ce contexte, à savoir la question de savoir comment un État tiers de l'Union, comment la Suisse doit appréhender la portée du caractère extra-territorial du RGPD. Pour cela, il convient de s'interroger sur la compétence extraterritoriale, normative et d'exécution des États ou plus précisément dans le cas d'espèce d'entités supranationales telles que l'Union européenne. 2007

Pour analyser cette problématique, un bref rappel de la réglementation applicable et de ses éléments essentiels, en particulier des spécificités du RGPD s'impose. Nous examinerons ensuite la question de la légitimité du caractère extra-territorial du RGPD et de la licéité de l'article 3 al. 2 RGPD au regard des concepts et principes du droit international public. Nous analyserons ensuite les conditions de mise en oeuvre effective des dispositions extraterritoriales du Règlement. Les problèmes posés seront examinés á la lumière de la loi, de la jurisprudence et de la doctrine récente sur ce sujet. Finalement, nous résumerons les principaux résultats de l'analyse 2008

1639. A l'exception du droit de déréférencement : Arrêt CJUE du 24 septembre 2019, *Google LLC contre Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17 et C-507/17, ECLI :EU :C :2019 :772, consid. 64, la Cour exige que le déréférencement soit effectif à l'échelle européenne, mais considère qu'il n'est pas obligatoire au niveau mondial.

1640. Deroudille / Fatah, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, p. 442.

et formulerons une brève conclusion.

I. Un champ d'application étendu du Règlement : Aperçu et caractéristiques des critères de l'art. 3 al. 2 RGPD

2009 L'article 3 al. 2 RGPD est structuré en trois points :

- le premier détermine l'applicabilité du RGPD à raison de la localisation de l'établissement du responsable du traitement ou du sous-traitant.
- le second, à raison de la localisation des personnes concernées par le traitement sur le territoire de l'Union.
- le troisième étend l'application du RGPD aux établissement déjà visés situés hors de l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public [1641].

2010 L'article 3 al. 2 RGPD pose ainsi deux critères de rattachement : le critère de l'établissement, c'est-à-dire le lieu d'établissement du responsable du traitement ou du sous-traitant, et le critère du ciblage, c'est-à-dire le lieu de situation des personnes concernées par le traitement [1642].

2011 Innovation majeure du Règlement, ce texte va s'appliquer indépendamment du lieu de traitement effectif des données. Ainsi, le territoire sur lequel les activités de traitement des données sont effectuées n'a aucun impact sur l'application du Règlement [1643].

A. La notion d'extra-territorialité

2012 Il y a extraterritorialité lorsqu'un « État prétend appréhender, à travers son ordre juridique, des éléments situés en dehors de son territoire [1644]».

2013 Or, le RGPD s'applique aux responsable du traitement ou aux sous-

1641. Pailler Ludovic, *L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) : Commentaire de l´article 3*, in : Journal du droit international 2018 145/3, p. 829.
1642. Thierache Corinne, *RGPD vs. Cloud Act : Le nouveau cadre légal américain est-il anti RGPD ?*, in : La Revue juridique Dalloz IP/IT 2019 2019/6, p. 368.
1643. Gallardo Meseguer, *Aperçu de la dimension internationale*, p. 120.
1644. Salmon Jean (édit.), *Dictionnaire de droit international public*, Bruxelles 2001, p. 211.

traitants qui ne sont pas établis dans l'UE, lorsque les traitements visent des personnes dans l'Union et sont liés á des offres de biens ou de services (même gratuits) dans l'Union, ou au profilage du comportement de ces personnes sur le territoire de l'Union.

Par conséquent, il présente un caractère extra-territorial. 2014

L'extra-territorialité du RGPD constitue une exception au principe de rattachement au territoire de l'Union, qui est courant en droit international privé et en droit européen. Ce critère de rattachement au territoire trouve son fondement dans la souveraineté étatique qui est un attribut essentiel de l'État et implique son indépendance. Celle-ci s'exerce sur un territoire défini et sur lequel un État est légitime á prendre des mesures de coercition, par le truchement d'autorités de contrôle administrative comme la CNIL en France ou par l'intervention du juge [1645]. 2015

Pour des raisons technologiques et économiques, les activités humaines dépassent de plus en plus fréquemment les frontières des États. Cet état de fait remet en cause les coutumes internationales relatives à l'étendue des compétences édictives et adjudicatives des États [1646]. 2016

Les tenants du droit international privé, comme Ludovic Pailler [1647], analysent le caractère extra-territorial du RGPD, sous l'angle de la détermination du droit applicable à un traitement de données personnelles. Il fonde l'applicabilité spatiale du RGPD sur deux critères de localisation géographique, définis par rapport au territoire de l'Union : le lieu d'établissement du responsable du traitement ou du sous-traitant, et la localisation des personnes concernées par le traitement. Ce second critère contraint potentiellement de nombreux acteurs établis hors de l'Union. 2017

B. Le critère de rattachement de l'établissement

Le premier critère de rattachement du RGPD est le critère de l'établissement. Ce critère fait abstraction de toute exigence de person- 2018

1645. Arrêt CJUE du 5 juin 2018, *Witschaftsakademie Schleswig-Holstein*, C-210/16, ECLI :EU :C :2018 :388, point 52.

1646. Rigaux François / Delpérée Francis, *Le concept du peuple*, 1e éd., Bruxelles 1988, p. 216.

1647. Pailler, *L'applicabilité spatiale du Règlement géneral sur la protection des données (RGPD)*, p. 823.

nalité morale domiciliée sur le territoire de l'Union [1648]. En effet, l'établissement suppose « l'exercice effectif et réel d'une activité au moyen d'un dispositif stable [1649] », quelle que soit la forme juridique de ce dispositif (succursale ou filiale, consid. 22 RGPD). Le RGPD donne ainsi la priorité au caractère effectif et permanent des activités de l'établissement dans la continuité de la directive 95/46/CE (consid. 19 RGPD). Le CEPD rappelle l'importance du lien de causalité entre le traitement de données personnelles et l'activité du responsable du traitement ou du sous-traitant. Ainsi, seuls les traitements qui s'inscrivent « dans le cadre des activités » de l'établissement sont soumis aux dispositions du Règlement. Ce critère apparaît de prime abord cohérent car l'établissement sert de référentiel à l'application du Règlement. Cependant, cette règle pourrait ne pas servir l'objectif du Règlement qui est de protéger les personnes physiques dont les données sont traitées. Dans le cadre d'un groupe multinational, il n'est pas exclu qu'une activité de santé personnalisée soit opérée en-dehors du territoire de l'Union, tandis qu'un établissement établi dans l'Union traite des données personnelles dans le cadre d'une autre activité. Par conséquent, la règle posée par le CEPD risque de favoriser le forum shopping entre les États, les activités les plus risquées et portant sur des données sensibles pouvant faire l'objet d'un dumping juridique dans des juridictions moins protectrices des droits des personnes concernées.

2019 Ce critère de rattachement s'inscrit en cohérence par rapport à la jurisprudence de la CJUE [1650] sur la notion d'établissement. Dans l'arrêt Weltimmo, la Cour de justice a retenu l'existence d'un établissement en présence d'un représentant, d'un compte bancaire et d'une boîte aux lettres. Dans l'arrêt Google Spain, la CJUE a considéré que le droit espagnol transposant la directive 95/46/CE s'appliquait aux activités de Google, bien que l'établissement principal

1648. Arrêt CJUE du 1 octobre 2015, *Weltimmo s.r.o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, ECLI :EU :C :2015 :639, points 29 et 31 ; Deroudille / Fatah, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, p. 442.

1649. EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Adopted on 12 November 2019*, in : EDPB (https ://edpb.europa.eu/), Brussels 2019, p. « https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf » (04/04/2020), p. 7.

1650. Arrêt CJUE *Weltimmo*, C-230/14, Rev. crit. DIP 2016, p. 377, note Haftel B., RUE 2016, p. 597, note Perray R. ; Arrêt *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González du 13 mai 2014*, C 131/12, ECLI :EU :C :2014 :317, consid. 55.

de Google se situait aux États-Unis. Le fait que l'une de ses filiales soit établie en Espagne, suffisait pour qualifier d'établissement, la filiale espagnole de Google. Pour la Cour, la notion d'établissement s'étend « à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable ». Elle retient en particulier le critère déterminant de la « *direction des activités en lien avec le traitement* [1651]». Dans cette jurisprudence, la Cour interprète l'art. 4.1 lit. a de la directive 95/46/CE, de manière extensive.

Le critère de rattachement de l'établissement était déjà prévu dans la Directive 95/46/CE. 2020

Le RGPD pose comme unique condition que le traitement soit effectué dans le cadre de l'activité de l'établissement localisé dans l'Union. Le Contrôleur européen à la protection des données recommande de rechercher dans un premier temps à identifier qui est le responsable du traitement et le sous-traitant dans le cas d'espèce, en application des définitions de l'art. 4, al. 7 et 8 RGPD [1652]. Le CEPD renvoie à la définition du considérant 22 RGPD et à la jurisprudence de la Cour de justice de l'UE pour définir l'établissement [1653]. 2021

Cependant, la localisation effective du traitement ne constitue pas un critère d'applicabilité du Règlement. Cet aspect particulièrement novateur revêt un caractère essentiel du fait notamment des enjeux liés á la gestion des données dans le cloud [1654]. 2022

Le contrôleur européen à la protection des données (ci-après « CEPD ») est venu préciser dans une directive les notions « d'offres de biens ou de services », afin d'éviter que tout site de commerce en ligne d'une entreprise établie en-dehors de l'Union ne tombe dans le champ d'application du Règlement. De même, la notion de « suivi de comportement », associée aux traitement aux fins de profilage 2023

1651. Arrêt CJUE du 28 juillet 2016, *Verein für Konsumenteninformationen c/ Amazon*, C-191/15, ECLI :EU :C :2016 :612, consid. 81.

1652. EDPB, *Guidelines on the territorial scope of the GDPR (Article 3)*, p. 5 ss.

1653. *Idem*, p. 6 ; Arrêt CJUE du 13 mai 2004, *Google Spain SL, Google Inc. contre AEPD, Mario Costeja González*, C-131/12, ECLI :EU :C :2014 :317 ; Arrêt CJUE du 1 octobre 2015, *Weltimmo contre NAIH*, C-230/14, ECLI :EU :C :2015 :639 ; Arrêt CJUE du 28 juillet 2016, *Verein für Konsumenteninformation contre Amazon*, C-191/15, ECLI :EU :C :2016 :612 ; Arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig - Holstein*, C-210/16, ECLI :EU :C :2018 :388.

1654. Métille, *L'utilisation de l'informatique en nuage par l'administration publique*, pp. 609-621.

des personnes concernées, a été définie [1655]. Le CEPD invite les autorités de protection des données à évaluer *in concreto, au cas par cas*, si le RGPD est applicable et adopte une perspective très souple de la notion d'établissement. Ainsi, le CEPD considère que « la présence d'un seul employé ou agent d'une entité non communautaire dans l'Union peut être suffisante pour constituer un arrangement stable [1656] ». Encore faut-il que le traitement concerne les activités du responsable du traitement dans l'UE. Inversement, la simple présence d'un salarié dans l'UE ne suffit pas en soi à déclencher l'application du RGPD, si le traitement des données est externalisé en-dehors de l'UE. Pour que le traitement en question relève du champ d'application du Règlement, il doit également être effectué dans le cadre des activités du salarié basé dans l'UE, peu importe le lieu effectif du traitement. La présence d'un salarié dans l'UE n'est pas en soi suffisante pour l'application du Règlement. De même, la seule accessibilité du site web de l'entreprise depuis le territoire d'un des États-membres de l'Union n'est pas suffisante pour appliquer les dispositions du Règlement. Enfin, l'existence de l'activité commerciale dans l'UE ne suffit pas à faire entrer le traitement des données par l'établissement étranger dans le champ d'application de la législation de l'UE en matière de protection des données [1657].

2024 Si les activités de traitement des données du responsable du traitement ou du sous-traitant établi en-dehors de l'Union, par exemple en Suisse sont inextricablement liées aux activités d'un établissement local établi dans un État membre de l'Union, elles peuvent déclencher l'applicabilité du droit communautaire, même si cet établissement local ne joue en fait aucun rôle dans le traitement des données lui-même. Le CEPD rappelle ainsi la jurisprudence de la cour de justice Google Spain (Case C-131/12). L'existence d'un lien inextricable entre les activités de traitement du responsable du traitement et du sous-traitant et la nature de ce lien constituent les critère pertinents pris en compte par le CEPD pour déterminer l'applicabilité du Règlement, indépendamment du rôle effectif de l'établissement situé dans l'Union [1658].

2025 Par exemple, si une chaîne d'hôtels et de centres de villégiature en

1655. EDPB, *Guidelines on the territorial scope of the GDPR (Article 3)*, p. 5.
1656. *Idem*, p. 6.
1657. Article 29 Data Protection Working Party, *Update of Opinion 8/2010 of Article 29 Data Protection Working Party*.
1658. EDPB, *Guidelines on the territorial scope of the GDPR (Article 3)*, p. 8.

Suisse propose des forfaits sur son site Internet, disponible en anglais, allemand, français et espagnol, sans détenir de bureau, de représentation ou d'arrangement stable dans l'UE, aucune entité liée à ce responsable du traitement des données en Suisse ne peut être considérée comme un établissement dans l'UE au sens du RGPD. Par conséquent, le traitement en question ne peut pas être soumis aux dispositions du Règlement, conformément à l'art. 3, al. 1 RGPD.

2026 En revanche, un site de commerce électronique exploité par une société basée au Suisse, qui aurait une activité de traitement des données personnelles exclusivement effectuées en Chine, mais disposant d'un bureau européen à Paris afin de diriger et de mettre en œuvre des campagnes de prospection commerciale et de marketing vers les marchés de l'UE, ne pourrait pas échapper à la qualification de lien inextricable entre les activités du bureau européen à Paris et les traitements des données à caractère personnel effectués par le site brésilien de commerce électronique, car la prospection commerciale et la campagne de marketing vers les marchés de l'UE servent notamment à rentabiliser le service offert par le site de commerce électronique. Le traitement des données à caractère personnel par la société brésilienne en relation avec les ventes dans l'UE est en effet inextricablement lié aux activités du bureau européen de Paris en matière de prospection commerciale et de campagne de marketing vers le marché de l'UE. Le traitement des données à caractère personnel par la société brésilienne en relation avec les ventes dans l'UE peut donc être considéré comme effectué dans le cadre des activités du bureau européen, en tant qu'établissement dans l'Union. Cette activité de traitement par la société chinoise sera donc soumise aux dispositions du Règlement, en application de l'art. 3, al. 1 RGPD [1659].

2027 Si les lignes directrices visent à fournir une unité d'interprétation du Règlement aux autorités de protection des données de l'Espace économique européen. Si l'intention d'apporter des précisions supplémentaires sur l'application du Règlement dans diverses situations mérite [1660] d'être saluée, leur longueur et le langage utilisé

1659. *Idem*, p. 9.

1660. Par exemple lorsque le responsable du traitement ou le sous-traitant est établi en dehors de l'IEEE, y compris sur la désignation et le rôle d'un représentant en vertu de l'article 3, al. 2 RGPD.

soulèvent le doute quant à l'atteinte de cet objectif [1661].

2028 Le RGPD innove également en étendant son champ d'application aux traitements effectués dans le cadre des activités du sous-traitant [1662]. Il formalise ainsi la position du groupe de travail de l'Article 29 sur ce thème [1663]. Si le RGPD prend en considération le lieu d'établissement du sous-traitant, il s'agit d'une conséquence logique du fait que sa responsabilité est reconnue par le RGPD.

2029 Le sous-traitant ne détermine ni la finalité, ni les moyens du traitement, mais réalise effectivement le traitement. Le RGPD le définit comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des donnés à caractère personnel, pour le compte du responsable du traitement ». Ainsi, si un responsable du traitement est établi en Chine, ses activités de traitement pourront entrer dans le champ d'application territorial du RGPD, dès lors qu'il recourt à un sous-traitant établi dans l'UE pour collecter, analyser ou stocker des données personnelles.

C. Le critère du ciblage

2030 Le critère du ciblage du RGPD permet de ne pas restreindre le champ d'application du règlement au seul cas des citoyens ou résidents des États membres. Ainsi, seul compte le fait d'être présent sur le territoire de l'Union au moment où a lieu le traitement, conformément au principe d'universalité du droit à la protection des données proclamé par l'article 8 de la Charte des droits fondamentaux [1664]. Doit être établie la volonté d'atteindre un public cible sur le territoire de l'Union [1665].

2031 Ainsi il ne suffit pas qu'un traitement de données concerne des ressortissants de l'Union européenne à l'étranger pour que le RGPD s'applique. Une analyse au cas par cas permettra de déterminer si un responsable du traitement a vocation à offrir des biens et services à des personnes physiques sur le territoire de l'Union euro-

1661. Poullet, *La vie privée à l'heure de la société du numérique*, p. 97.
1662. *Idem*, p. 5.
1663. Groupe de Travail de l'Article 29, *Avis 8/2010 du Groupe de travail de l'Art. 29 sur le droit applicable - Adopté le 16 décembre 2010 (WP 179)*, in : CNPD (https ://cnpd.public.lu/), Luxembourg 2010, p. « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp179_fr.pdf » (04/04/2020), p. 23.
1664. EDPB, *Guidelines on the territorial scope of the GDPR (Article 3)*, p. 13.
1665. *Ibidem.*

péenne. Il s'agira de relever un faisceau d'indices comme la monnaie européenne, l'emploi d'une des langues nationales d'un pays membre, la livraison sur le territoire de l'Union [1666].

Le critère du ciblage figurait déjà dans l'avant-projet de la Commission européenne en 2012 [1667]. Ainsi il était prévu que les règles de l'Union devraient s'appliquer, si des données à caractère personnel faisaient l'objet d'un traitement à l'étranger par des entreprises implantées sur le marché européen et « *proposant leurs services aux citoyens de l'Union* [1668] ». 2032

Il s'agit d'une nouvelle approche, qui représente un progrès pour le droit fondamental à la protection des données. Le législateur européen entend soumettre au Règlement les sociétés qui ne sont pas dans l'Union, indépendamment de savoir si ces biens ou services sont fournis à titre onéreux ou résultent de l'observation de leur comportement [1669]. Il abandonne le critère des « moyens de traitement » situés dans l'UE de l'art. 4, par. 1, c de la directive 95/46/CE. 2033

D. Le critère du suivi de comportement

Indépendamment des critères précédemment cités, le RGPD est également applicable, en cas de *suivi de comportements de personnes* situées sur le territoire de l'Union européenne. Le RGPD « s'applique au traitement des données à caractère personnel relatives à des personnes concernées *qui se trouvent* sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union ». 2034

Ces dispositions visent le profilage des individus par le biais d'algorithmes et du traitement de leurs données personnelles. Le Groupe de travail de l'Art. 29 inclut dans la notion de profilage l'usage des cookies, les données de suivi de santé, les études de marché me- 2035

1666. Arrêt CJUE du 7 décembre 2010, *Peter Pammer c/ Reederei Karl Schülter GmbH & Co. KG et Hotel Alpenhof GmbH c/ Oliver Heller*, C-585/08 et C-144/09, ECLI :EU :C :2010 :740, point 70 ss.

1667. Commission européenne, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises - Communiqué de presse du 25 janvier 2012*, in : Commission européenne (https ://ec.europa.eu/), Bruxelles 2012, p. « https://ec.europa.eu/commission/presscorner/detail/fr/IP_12_46 » (04/04/2020).

1668. *Ibidem.*

1669. Gallardo Meseguer, *Aperçu de la dimension internationale*, p. 120.

nées sur des populations de l'Union européenne, les données des caméras de surveillance, etc.

2036 La question se pose de savoir si les personnes concernées qui ne résident pas dans l'Union mais se trouvent de manière temporaire dans l'Union, bénéficient des garanties du RGPD. Pour la doctrine, « le verbe se trouver est moins exigeant que résider et témoigne de la volonté d'appliquer le RGPD chaque fois que la situation a un lien avec l'Union européenne [1670] ». Si cette perspective présente en effet un intérêt certain pour les personnes concernées par un traitement de données du fait des garanties offertes dans l'Union, l'adopter reviendrait à consentir une protection du fait de la localisation géographique des personnes concernées (ex : un touriste chinois visitant Paris), sans considération de la durée de séjour de la personne concernée sur le territoire de l'Union. La juridiction serait donc liée à la localisation de la personne, sans tenir compte de son lieu habituel de résidence ou de sa nationalité.

E. Le critère du droit international public

2037 Indépendamment des critères de rattachement précités, le RGPD peut également s'appliquer en vertu du droit international public (consid. 25 RGPD). Il en est ainsi lorsque le droit d'un État membre s'applique hors du territoire de cet État, en application de la coutume et des traités - notamment du fait des représentations diplomatiques des États de l'UE à l'étranger. Il en est ainsi des ambassades et des consulats [1671].

2038 Le critère du droit international public figurait déjà dans la directive 95/46/CE (art. 4.1, *litt.* a et b. de la directive 95/46/CE). Ce article prévoyait que les dispositions extra-territoriales de la directive 95/46/CE s'appliquaient au responsable du traitement « qui n'est pas établi dans l'Union, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public ».

2039 Les règles délimitant les compétences des États font partie du droit international coutumier. Afin de résoudre les conflits de compétences entre Etats hors UE, il importe de préciser les limites de la compétence extraterritoriale des États et de considérer les in-

1670. Jault-Seseke Fabienne, *La portée extraterritoriale ou a-territoriale du RGPD*, in : Revue des affaires europeennes 2018/1, pp. 43-51.

1671. Bensoussan, *Règlement européen sur la protection des données (2e éd.)* p. 9.

térêts des États parties au conflit [1672]. Une coopération bilatérale et multilatérale, respectueuse de la balance des intérêts en présence, est particulièrement utile, pour éviter le recours à des politiques unilatérales de résolution des conflits [1673]. Les normes spécifiques du droit fiscal, pénal, économique ou de protection des données auxquelles certains États donnent parfois un champ d'application extraterritoral appartiennent au droit interne, en l'espèce au droit communautaire pour le RGPD. En fonction de la place que l'ordre juridique interne confère au droit international (monisme avec primauté du droit international ou du droit interne, dualisme), un conflit de normes peut apparaître entre le « droit interne » et le droit international.La jurisprudence de la Cour européenne des droits de l'homme est de plus en plus favorable au droit international général, notamment concernant l'applicabilité extraterritoriale de la CEDH [1674].

F. Le caractère extra-territorial en lien avec les transferts internationaux

Le RGPD présente également une spécificité du fait de son champ d'application extra-territorial en lien avec les transferts internationaux (Chapitre V du Règlement (art. 44 à 50 RGPD)). Il exige en effet du responsable du traitement ou du sous-traitant, qu'il vérifie préalablement à tout transfert de données personnelles vers un État tiers, que ce pays offre un niveau de protection adéquat. 2040

L'art. 28, al. 3 RGPD impose au responsable du traitement de s'assurer par contrat que le sous-traitant « présente des garanties suffisantes » quant à la conformité au Règlement et à la protection des personnes concernées dont les données sont traitées. Si le sous-traitant est établi dans un État tiers, les dispositions du RGPD sont ainsi applicables au-delà des frontières de l'Union. 2041

Les clauses obligatoires des contrats doivent stipuler que le sous-traitant ne peut procéder au traitement des données que sur instruction documentée du responsable du traitement, sauf lorsqu'il 2042

1672. Arrêt de la Cour suprême américaine, *re-Uranium Antitrust Litigation*, 617 F.2d 1248, 1980, *Laker Airways contre Sabena, Belgian World Airlines*, 731 F.2D 909, 1984.

1673. Friedel-Souchu Evelyne, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*, thèse, Paris 1992, p. 424.

1674. Arrêt CourEDH du 12 décembre 2001, *Bankovic et autres c. Belgique et 16 autres pays*, requête n° 52207/99, consid. 59.

est tenu d'y procéder, en vertu du droit de l'Union ou du droit d'un État membre. Par conséquent, le droit d'un État tiers ne constitue pas un fondement licite.

2043 Seuls les États ayant reçu une décision d'adéquation de la Commission européenne, sont en droit d'effectuer un transfert international sans contrainte juridique supplémentaire. Seuls Andorre, l'Argentine, le Canada, les Îles Féroé, Guernesey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay bénéficient d'une décision d'adéquation de la Commission européenne.

2044 En principe, les entreprises américaines adhérant au programme « EU-US Privacy Shield », bénéficient également d'une reconnaissance d'un niveau de protection adéquat lors du transfert de données personnelles entre les États-Unis et l'Union européenne.

2045 Cependant, dans son opinion du 19 décembre 2019, l'avocat général Henrik Saugmandsgaard a émis des doutes sur la conformité de la décision Privacy-Shield. Son raisonnement se fonde sur les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et sur l'article 8 CEDH. Cet avis justifie la préparation de nouvelles négotiations entre la Suisse et les États-Unis concernant l'accord Privacy Shield, en vue de l'ouverture vraisemblables de nouvelles discussions sur ce thème entre l'UE et les États-Unis.

2046 Ainsi, le champ d'application extraterritorial du Règlement contribue-t-il à élever la norme de référence de la protection des données personnelles en-dehors de l'Union du fait des garanties demandées par les dispositions du chapitre V du RGPD lors des transferts internationaux, analysées à la lumière de la Charte et de la CEDH.

2047 En l'absence d'une décision d'adéquation, le responsable du traitement doit offrir des garanties appropriées (art. 46 du RGPD). Le RGPD reconnait comme étant des garanties appropriées les clauses contractuelles types et les règles d'entreprise contraignantes, ou « binding corporate rules » (art. 46.1 b). Ces dispositions réglementent le transfert de données personnelles au sein d'un même groupe. Approuvées obligatoirement par les autorités de contrôle compétentes de l'Union européenne dans le respect de l'art. 47, al. 2 RGPD, elles légalisent le libre flux de données personnelles au sein de groupe de dimension internationale. En France, Axa Private Equity, Hermès, LVMH ou Novartis ont déclaré des BCR auprès de

la CNIL.

A défaut de BCR, les entreprises peuvent signer des clauses contractuelles types avec leurs sous-traitants (art. 28, al. 6 à 28, al. 8 RGPD). La CJUE vient de confirmer la validité du recours aux clauses contractuelles types pour les transferts de données personnelles vers des États tiers [1675]. 2048

Les garanties contractuelles offertes lors des transferts de données personnelles vers des pays tiers ont pour but d'assurer la continuité du niveau élevé de protection des données à caractère personnel. Elles sont la preuve que le pays tiers garantit un niveau de protection des droits fondamentaux des personnes dont les données sont transférées, équivalent à celui prévu par le RGPD, à la lumière de la Charte. 2049

Cependant, dans son opinion du 19 décembre 2019, l'avocat général Henrik Saugmandsgaard a considéré que l'art. 58, al. 2 RGPD « oblige les autorités de contrôle, lorsqu'elles estiment, au terme d'un examen diligent, que des données transférées vers un pays tiers ne bénéficient pas d'une protection appropriée en raison du non-respect des clauses contractuelles convenues, à prendre les mesures adéquates pour remédier à cette illégalité, si nécessaire en ordonnant la suspension du transfert ». 2050

Il existe ainsi selon l'avocat général, une « obligation - imposée aux responsables du traitement et, en cas d'inaction de ces derniers, aux autorités de contrôle - de suspendre ou d'interdire un transfert lorsque, en raison d'un conflit entre les obligations découlant des clauses types et celles imposées par le droit du pays tiers de destination, ces clauses ne peuvent être respectées ». 2051

Ainsi, les autorités de contrôle aurait une obligation positive « d'agir de façon à assurer la bonne application du règlement [1676]» et de s'acquitter pleinement de la mission de surveillance attribuée dans le Règlement. Cette obligation va renforcer la responsabilisation effective des entreprises soumises au Règlement et le rôle des autorités de contrôle de l'Union en tant que gardien du droit fondamental à la protection des données. 2052

1675. Saugmandsgaard, *Conclusions de l'avocat général dans l'affaire C-311/18 Facebook Ireland et Schrems*.

1676. *Idem*, point 145.

§2 La question de la légitimité du caractère extra-territorial du RGPD

I. Une dérogation au principe de souveraineté territoriale

2053 L'article 3, al. 2 RGPD peut s'interpréter de prime abord comme une violation du principe de souveraineté étatique des États qui ne sont pas membres de l'Union européenne, comme la Suisse.

A. Le principe de souveraineté

2054 La souveraineté d'un État constitue le fondement de son indépendance. Il s'agit d'un statut juridique découlant du droit international public, mais non supérieur à celui-ci [1677]. Cette souveraineté est politique, juridique mais aussi économique. Selon l'article 1 de la Charte des droits et devoirs économiques des États, adoptée par l'assemblée générale des Nations-Unis le 12 décembre 1974, « chaque État a le droit souverain et inaliénable de choisir son système économique, de même que ses systèmes politique, social et culturel, conformément à la volonté de son peuple, sans ingérence, pression ou menace extérieure d'aucune sorte [1678]».

2055 Le caractère exclusif des compétences de l'État leur donne la liberté de régir des situations pouvant comporter des éléments d'extranéité. La compétence territoriale d'un État a été précisée dans l'affaire de l'île de Palmas (RSA 1928 vol. II, p. 829-838). L'arbitre Max Huber a rappelé que « la souveraineté dans les relations entre États, signifie l'indépendance ». L'indépendance est le droit d'y exercer, à l'exclusion de tout autre État, les fonctions étatiques. Cela renvoie à la notion d'« Imperium », en droit romain [1679]. Sur ce territoire, un État est légitime à prendre des décisions par le truchement d'au-

1677. Steinberger Helmut, *Sovereignty*, in : Encyclopedia of Disputes Installment 1987/10, p. 408.

1678. Assemblée générale des Nations-Unies, *Résolution 3281 (XXIX) du 12 décembre 1974 (29ème session) - Charte des droits et devoirs économiques es Etats*, in : Nations-Unies (https ://undocs.org/), Genève 1974, p. « https://undocs.org/fr/A/RES/3281(XXIX) » (04/04/2020) ; Friedel-Souchu, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*, p. 18.

1679. Lebon Lydia, *La territorialité et l'Union européenne : approches de droit public*, thèse, Bordeaux 2013, p. 478 ss.

torités de contrôle administrative ou par l'intervention du juge [1680].

En pratique, l'État délègue un nombre croissant de services publics à des entreprises privées, parfois dans le cadre de la gestion d'infrastructures critiques ce qui soulève la triple question de l'indépendance effective, de la souveraineté réelle de l'État et de la protection des données personnelles [1681]. 2056

Du fait de leur indépendance et souveraineté les États sont compétents pour élaborer des législations de portée internationale [1682]. 2057

La portée de cette compétence normative a été précisée en examinant en première partie les critères de rattachement du RGPD. La jurisprudence de la Cour de Justice de l'Union européenne et le CEPD sont venus préciser l'étendue de ces critères pour garantir l'exercice de la compétence extraterritoriale dans le respect du droit international. 2058

B. Les principes du droit international

Le RGPD engage plusieurs États et s'applique sur la somme des territoires des États parties ou l'espace juridique des États contractants (Décision CourEDH, *Bankovic et autres c. Belgique et 16 autres pays*, op.cit., consid. 80). Comme les obligations d'un Etat-membre de l'UE partie au RGPD peuvent s'étendre à des faits situés dans un autre État membre, le RGPD présente une application extraterritoriale « relative » pour chaque État de l'UE eu égard aux autres États de l'UE. En revanche, le RGPD est également applicable à des faits situés en-dehors du territoire de l'UE [1683]. Comment résoudre les conflits de juridictions et limiter le risque de la double peine, qui 2059

1680. Arrêt CJUE du 5 juin 2018, *Witschaftsakademie Schleswig-Holstein*, C-210/16, ECLI :EU :C :2018 :388, consid. 52.

1681. Bembaron Elsa, *Emmanuel Macron fait de la 5G un enjeu de souveraineté européenne*, in : Le Figaro (https ://www.lefigaro.fr/), Paris 2019, p. « https://www.lefigaro.fr/secteur/high-tech/emmanuel-macron-fait-de-la-5g-un-enjeu-de-souverainete-europeenne-20191107 » (06/01/2020).

1682. Nous assimilons l'UE à un État dans cette étude, ce qui pourrait bien entendu faire l'objet d'une analyse critique, puisque le Traité établissant une constitution pour l'Europe (TECE) a été refusé par les français et les néerlandais au référendum de 2005.

1683. Decaux Emmanuel, *Le territoire des droits de l'homme*, in : Liber amicorum Marc-André Eissen 1995, p. 69.

serait contraire au principe *non bis in idem* ?

2060 Si une loi nationale comme le Cloud Act américain considère comme licite ce que l'autre, par exemple le RGPD, condamne, alors il existe une situation de conflit de lois [1684] et une concurrence *de facto* entre plusieurs juridictions. La seule règle de droit international qui existe est qu'un État ne doit pas faire de sa compétence un usage tel qu'il risque de porter atteinte à la souveraineté d'un autre État [1685]. En droit de la protection des données, se pose la question se savoir si des solutions ne pourraient pas être négociées dans le cadre d'accords bilatéraux ou multilatéraux qui régleraient le conflit, afin d'éviter le recours à la voie diplomatique.

2061 Le droit international pose plusieurs principes clefs que chaque État s'engage à respecter.

2062 La charte des Nations-Unies reconnaît le principe d'égalité souveraine de tous les États membres (art. 2, § 1). Ce principe d'égalité juridique entre États est au coeur des relations diplomatiques. Il rend légitime la contestation d'un État par la voie diplomatique en cas de comportement non conforme aux normes internationales (par exemple en cas « d'abus de droit d'un autre État, par exemple dans le cas des interceptions de la NSA révélées par Edward Snowden »).

2063 Le principe de territorialité en droit international donne compétence à l'État à l'égard des biens et des personnes situées sur son territoire et des situations rencontrées. Chaque État bénéficie d'une garantie d'inviolabilité et d'intégrité de son territoire en application des principes du droit international public. La plupart des questions qui touchent aux rapports internationaux et aux conflits éventuels sont réglés en vertu du principe de la compétence exclusive de l'État sur son propre territoire. Depuis la décision « Bancovic », la théorie des compétences, déjà consacrée en droit international, a été reconnue en droit européen en mentionnant que « du point de vue du droit international public, la compétence juridictionnelle d'un

1684. van Hecke Georges, *Le droit anti-trust : aspects comparatifs et internationaux*, in : Recueil des Cours / Collected Courses Leiden 1962/106, p. 309.
1685. *Idem*, p. 323.

État est principalement territoriale [1686].

Cependant, ce principe de territorialité peut se retrouver en conflit avec le principe de la compétence territoriale d'un autre État. En l'espèce, le caractère extraterritorial du RGPD se retrouve en conflit avec le principe de la compétence territoriale des États situés en-dehors de l'Union. Brigitte Stern définit l'application extraterritoriale d'une norme en ces termes : « il y a extraterritoralité de l'application d'une norme, si tout ou partie du processus d'application se déroule en-dehors du territoire de l'État qui l'a émise [1687] ». Nous verrons ultérieurement comment le droit international public et le droit international privé offrent des solutions à cette problématique. 2064

Le principe de personnalité donne compétence á l'État pour légiférer à l'égard de ses nationaux, personnes physiques ou morales, indépendamment du lieu où ils se trouvent. Les normes applicables aux résidents étrangers ont un caractère extraterritorial [1688]. 2065

Le principe de protection justifie une action extraterritoriale pour protéger son intégrité territoriale (droit de légitime défense) [1689]. 2066

Le principe d'universalité utilisé en droit pénal traite des infractions commises á l'étranger par des étrangers, personnes physiques ou morales. Si un État considère qu'un acte est préjudiciable à l'ensemble de la communauté internationale, alors un État peut appliquer sa législation nationale à condition que l'infraction soit reconnue comme telle universellement. Le droit à la protection des données vise la protection de la personne humaine dont les données sont traitées et qui risque de subir un dommage du fait de ce traitement. Le droit de la protection des données est un droit fondamental consacré par la Charte des droits fondamentaux de l'Union 2067

1686. CourEDH du 12 décembre 2001, *Bankovic et autres c. Belgique et autres*, requête n° 55207/99, consid. 59, obs. Cohen-Jonathan Gérard, *La territorialisation de la juridiction de la Cour européenne des droits de l'homme*, in : Revue trimestrielle des droits de l'homme 2002/52, p. 1055 ; chron. Weckel (Ph.), RGDIP, 2002,n°52, p. 438 ; Sudre (F.), JCP G, 16 janvier 2002, Vol.I p. 105 et Flauss (J-F.), AJDA, 2002, p. 501. De manière plus générale, voir obs. Sudre (F.), in : *GACEDH*, n° 68, p. 731.

1687. Stern Brigitte, *L'extra-territorialité « revisitée » : où il est question des affaires Alvarez-Machain, Pâte de Bois et de quelques autres...*, in : Annuaire français de droit international 1992 38/1, p. 242.

1688. *Idem*, p. 25.

1689. *Idem*, p. 25 ; Friedel-Souchu, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*, p. 25.

européenne, à l'article 8. Or, les droits de l'homme ont une prétention à l'universalité [1690]. Par conséquent, un État de l'Union pourrait appliquer le RGPD de manière universelle, sur la base d'une infraction à la protection des données en tant que violation d'un droit humain fondamental. La Convention 108 ayant une valeur juridique contraignante et une portée internationale pourrait également servir de référence en droit international pour sanctionner des infractions commises à l'étranger, sur le fondement du principe d'universalité. Une violation des dispositions de la Convention 108 pourrait être interprétée comme étant préjudiciable à l'ensemble des États. Si le droit à la protection des données était reconnu comme essentiel à la sécurité, à la souveraineté étatique et à la communauté internationale alors, les principes d'universalité et de protection du droit international pourraient s'appliquer. Cette conception n'est cependant pas partagée sur la scène internationale et il n'est pas exclu que certains pays comme la Chine ou les États-Unis s'opposent á cette reconnaissance.

2068 A l'initiative du gouvernement canadien, une commission internationale de l'intervention et de la souveraineté a été mise en place en 2001 et a reconnu un nouveau principe de droit international public : la « responsabilité de protéger ». L'État a ainsi non seulement le droit de contrôler ses activités sur son territoire, mais également l'obligation de protéger les personnes vivant à l'intérieur de ses frontières, du fait de sa souveraineté [1691].

2069 Cette responsabilité de protéger s'inscrit dans le cadre de la protection des droits de l'homme. Or le droit à la protection des données est un droit fondamental consacré par la Charte des droits fondamentaux de l'UE et la Convention 108 du Conseil de l'Europe. Par conséquent, ce principe pourrait être invoqué pour obliger les États à garantir un recours effectif pour la protection des données personnelles, dans le cadre de contentieux transfrontières. En pratique, l'architecture stockant les données étant mise á disposition par des entreprises privées, il serait pertinent d'étendre cette responsabilité de protéger aux entreprises privées, dans l'esprit du « duty of

1690. Voir en particulier la Déclaration universelle des droits de l'homme du 10 décembre 1948.

1691. CIISE, *La Responsabilité de Protéger - Rapport de la commission internationale de l'intervention et de la souveraineté (Décembre 2001)*, in : Centre de recherches pour le développement international, Ottawa 2001, pp. 1-120.

care » du droit de common law.

Cette souveraineté de responsabilité peut s'analyser comme reconnaissant la légitimité d'intervention extra-territoriale d'un État tiers, par exemple en cas de violation des droits de l'homme. 2070

Pour les tenants de l'approche jusnaturaliste, la validité du droit international échappe à la volonté des États et trouve son fondement dans le fait social [1692]. Cette approche sociologique de la validité du droit international est pertinente pour le RGPD, dont le caractère extraterritorial est valable du fait de la nature de droit fondamental du droit à la protection des données, dans un contexte technologique et économique rendant possible l'échange de renseignements instantanés sans barrière géographique. L'extension internationale des activités humaines créent un risque nouveau du point de vue de la protection des droits de l'homme [1693] et justifient la volonté de certains États d'étendre leur pouvoir de façon à contrôler ces activités et à offrir une protection des personnes concernée, par le biais d'un recours juridictionnel effectif. 2071

C. Les mutations du principe de souveraineté territoriale

La construction européenne engendre des mutations du principe de territorialité, dans les matières pénale, fiscale, constitutionnelle et administrative [1694]. Le constat de l'effacement du principe de territorialité est perceptible à l'égard de l'ensemble de la matière publique. La disparition des frontières en droit de l'Union [1695] ainsi que l'avènement de l'espace de liberté de sécurité et de justice [1696]. 2072

Le RGPD contribue à l'unification d'un espace de libre circulation des données au sein de l'UE. Il crée un mécanisme de coopération entre autorités administratives sous la direction du CEPD pour l'application effective et harmonisée du RGPD dans l'Union. Cette évo- 2073

1692. Besson Samantha, *Droit international public*, 1e éd., Berne 2019, p. 37.
1693. Grisel Guillaume, *Application extraterritoriale du droit international des droits de l'homme*, thèse, Lausanne 2010, p. 4.
1694. Lebon, *La territorialité et l'Union européenne*, p. 478.
1695. Nardi, *« Courtoisie internationale »*, p. 1.
1696. L'espace de liberté, de sécurité et de justice est un espace qui s'est construit par étapes. Le Traité de Maastricht a constitué la première étape de cette construction, puisqu'il consacre la coopération en matière de justice et d'affaires intérieures (CJAI). Le traité d'Amsterdam a poursuivi ce processus en communautarisant les politiques migratoires et la coopération en matière civile. Enfin les accords de Schengen et de Dublin ont largement ébranlé ce dogme de la territorialité.

lution s'inscrit dans le prolongement de la construction d'un espace de coopération judiciaire en matière civile entre les États-membres de l'UE, afin de constituer un espace judiciaire européen.

2074 Le droit français reconnaît que le territoire national constitue le champ d'application de normes en provenance d'un autre ordre juridique. Ainsi la Constitution française, sous l'effet de la construction européenne, a été modifiée à plusieurs reprises et a. abouti à une extension de la compétence de l'État. Ainsi, selon M. Wojtyczek, « La constitution de l'État cesse d'être la loi fondamentale d'un territoire et devient la loi fondamentale d'un ordre juridique qui, tout en gardant une assise territoriale certaine, entre en concurrence avec d'autres ordres juridiques sur le territoire national, tout en essayant d'étendre son champ d'application extraterritorial [1697] ».

2075 La Suisse qui n'est pas membre de l'Union européenne a conservé un lien étroit entre son territoire, ses prérogatives étatiques et la Constitution. La Constitution helvétique insiste sur le caractère central de l'indépendance du pays. Dans son article 1, elle stipule : « la Confédération suisse [...] assure l'indépendance [...] du pays ». La Constitution commande donc aux représentants des cantons et de la Confédération de prendre toutes les mesures nécessaires pour garantir l'indépendance de la Suisse envers d'autres États, l'intégrité et l'inviolabilité de son territoire. Cette obligation constitutionnelle peut s'interpréter dans le domaine économique comme une invitation à privilégier les acteurs suisses sur des acteurs étrangers dès lors que l'indépendance pourraient être menacée. Ainsi le choix d'équipements et d'infrastructures digitales (clouds, réseaux, ...) doivent pouvoir servir l'indépendance de la Suisse [1698].

2076 Dans le même temps, la Constitution helvétique pose le principe du respect du droit international par la Confédération et les cantons (art. 5). La Suisse adopte le principe moniste. Ce principe de la pri-

1697. Wojtyczek Krzysztof, *Les fonctions de la Constitution écrite dans le contexte de la mondialisation*, in : UMK (https ://www.umk.ro/), Iasi 2011, p. « https: //www.umk.ro/images/documente/publicatii/masarotunda2007/10_les_fonctions.pdf » (04/01/2020).

1698. La question se pose de savoir si l'extra-territorialité imposée par le RGPD pourrait s'analyser comme une atteinte á l'indépendance de la Confédération ? Inversement, le principe d'indépendance est-il applicable à l'action extraterritoriale menée par la Suisse à l'étranger ?

mauté du droit international a été consacré par la jurisprudence [1699]. Ainsi une Convention internationale est directement applicable, sans transposition en droit interne. Dès sa ratification, une convention internationale fait partie de l'ordre juridique suisse et ses dispositions sont directement applicables par les autorités suisses sans devoir adopter une loi fédérale d'exécution.

Se pose donc la question de l'indépendance effective de la Suisse. 2077

Si l'extra-territorialité du RGPD était interprétée comme une disposition de droit international, alors la Confédération et les cantons devraient s'y conformer, sans interpréter cette extra-territorialité comme une violation de la Constitution, mais au contraire comme un élément de son application. La Suisse n'étant pas membre de l'UE, ni de l'EEE, ce raisonnement serait uniquement valable avec une reconnaissance du RGPD par le Parlement suisse. 2078

D. La déterritorialisation du droit

La doctrine constate une déterritorialisation du droit, qui s'accélère en raison de la mondialisation des échanges de personnes, de biens et de données entre des acteurs multiples [1700]. 2079

Internet joue un rôle central dans ce phénomène de déterritorialisation du droit et de déclin lent mais constant du principe de souveraineté des États [1701]. Réseau mondial sans frontières, Internet rend possible des communications et transactions dématérialisées à titre gratuit ou onéreux, qui s'affranchissent des territoires sur lequels s'exerce la souveraineté des États [1702]. 2080

Face au déclin constant de la souveraineté territoriale, certains ont revendiqué la création de nouveaux territoires, de la taille du ré- 2081

1699. ATF 122 II 485 (f) et ATF 96 II 4, SJ 1971, p. 174.
1700. Wojtyczek, *Les fonctions de la Constitution*, p. 109.
1701. Lebon, *La territorialité et l'Union européenne*, p. 478 ss.
1702. de Clercq Chloë / Dechamps Frédéric, *« Internet à l'épreuve du droit ou le droit à l'épreuve d'Internet : une analyse au regard de la problématique de l'étendue géographique du droit européen au déréférencement »*, in : Féral-Schuhl Christiane (édit.), *Cyberdroit : le droit à l'épreuve de l'Internet*, 7e éd., Paris 2018, p. 680.

seau internet [1703] ou de la taille des plateformes en ligne [1704]. L'émergence de cette réflexion autour de la création d'un espace d'échange de données a-territorial, a émergé de manière concomitante avec les mécanismes de Soft Law. Comme le souligne Rolf Weber, ces normes constituent « un modèle de régulation qui développe et établit des règles indépendamment du principe de territorialité [1705] ».

2082 Cette approche a-territoriale a été critiquée en doctrine notamment par Jack L. Goldsmith [1706].

2083 Progressivement le débat a évolué en faveur de la règle du conflit de loi pour déterminer quel droit était applicable supprimant la réflexion autour de la pertinence de l'existence d'un droit national pour les activités du cyberespace [1707].

2084 Le droit international privé revêt ainsi un intérêt majeur dans la résolution des conflits de lois.

2085 A l'intérieur de l'Union, le droit international privé se limite aux contentieux émergeant de la disparité des mesures d'exécutions entre États, lorsque le RGPD offre une liberté aux États (ex : détermination de l'âge du consentement au traitement des données personnelles des mineurs, art. 8 RGPD) [1708]. La résolution des conflits éventuels est prévu dans le RGPD au moyen d'un contrôle a posteriori, sur la base d'une structure de gouvernance en réseau. Le RGPD met en place un système de coopération des autorités de

1703. Johnson David R. / Post David, *Law and Borders–The Rise of Law in Cyberspace*, in : Stanford Law Review 1995/48, p. 1367 ; Kulesza Joanna / Balleste Roy, *Signs and Portents in Cyberspace : The Rise of Jus Internet as a New Order in International Law*, in : Fordham Intellectual Property Media and Entertainment Law Journal 2012/23, pp. 1333-1346 ; Thelisson Eva, *Un État mondial via Internet ?*, 1e éd., Paris 2012, p. 2.

1704. Lutzi Tobias, *The Platform Economy and Private International Law*, in : Pretelli Ilaria (édit.), *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales : actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, 1e éd., Genève 2018, p. 32.

1705. Weber Rolf H., *Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises*, in : Journal of Governance and Regulation and Volume 2012 1/1, pp. 8-14.

1706. Goldsmith Jack L., *Against cyberanarchy*, in : The University of Chicago Law Review 1998 65/4, pp. 1199-1250.

1707. Lutzi, *The Platform Economy*, p. 131.

1708. Le législateur a limité cette liberté au maximum afin d'éviter la pratique de forum shopping au sein de l'UE, en adoptant un Règlement et non une directive.

contrôle sur le territoire de l'UE par le biais de la désignation d'une autorité chef de file et par un mécanisme de contrôle de la cohérence des décisions des autorités de contrôle.

Le Conseil de l'Europe vise, avec raison, à étendre ce réseau de coopération aux États tiers de l'Union, signataires de la Convention 108. Cet instrument à la vocation universelle [1709], prévoit dans son rapport explicatif de la Convention 108 une coopération internationale entre les autorités de contrôle. Il s'agit en effet d'un « élément clé de la protection efficace des personnes [1710] ». En favorisant « l'assistance mutuelle et en fournissant la base juridique appropriée pour l'établissement d'un cadre de coopération et d'échange d'informations à des fins d'enquête et d'application des lois », une protection effective des personnes dont les données personnelles sont traitées pourra être mise en place. 2086

Le Conseil de l'Europe aligne ainsi sa vision sur celle de la Cour de Justice de l'UE, qui donne, elle aussi, comme le RGPD, la priorité à la protection juridictionnelle effective [1711]. 2087

Cette procédure d'assistance mutuelle vise à renforcer la sécurité juridique en cas de contentieux transnational. Elle prévoit un contrôle a priori et a posteriori [1712]. 2088

La CJUE reconnaît dans sa jurisprudence que « [l]'institution, dans les États membres, d'autorités de contrôle indépendantes constitue [...] un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel [1713] ». L'obligation d'instaurer des autorités de contrôle indépendantes figure dans la Charte des droits fondamentaux, à l'art. 8, al. 2089

1709. Conseil de l'Europe, *Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, in : Série des traités du Conseil de l'Europe, Strasbourg 2018 2018/223, p. 1.

1710. *Idem*, p. 3.

1711. Arrêt CJUE du 17 novembre 2011, *Hypotecni Banka contre Udo Mike Lindner*, C-327/10, ECLI :EU :C :2011 :745, comm. 53 ; Arrêt CJUE du 11 sept. 2014, *A contre B e.a.*, C-112/13, ECLI :EU :C :2014 :2195, pt. 50 ; Voir aussi art. 47 Charte des droits fondamentaux de l'UE.

1712. Counseil de l'Europe, *Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes*, p. 25, point 137.

1713. Arrêt CJUE 9 mars 2010, *Commission européenne contre République fédérale d'Allemagne.*, C-518/07, ECLI :EU :C :2010 :125, consid. 23.

3 et dans le traité à l'art. 16, al. 2, TFUE.

2090 Un fonctionnement en réseau d'autorités de contrôle indépendantes, sur le modèle du RGPD, non pas limité au territoire de l'Union mais étendu à toutes les parties signataires de la Convention 108, limiterait les incertitudes juridiques du recours au droit international privé.

E. Le rôle croissant du droit international privé

2091 Les données personnelles, dont la protection est un droit fondamental, constituent la marchandise de base de la nouvelle économie numérique mondiale. Elles constituent ainsi un terrain d'élection pour des conflits, qu'ils soient de nature juridique ou économique [1714].

2092 En l'absence d'un droit global, le droit international privé [1715] joue un rôle central dans la résolution des contentieux entre personnes privées au niveau international. « Il coordonne en effet les systèmes juridiques au moyen de règles déterminant quel système a la légitimité requise pour s'appliquer. Il régit les relations juridiques relevant du droit privé et présentant un ou plusieurs éléments d'extranéité [1716] ».

2093 Le droit international privé est essentiel dans la résolution de conflits entre les États tiers et l'UE, pour les secteurs qui n'entrent pas dans le champ d'application des accords bilatéraux.

2094 Il présente également un intérêt entre les États-membres de l'Union. Cependant, le RGPD limite le recours à la règle de conflit de lois dans le domaine de la protection des données au sein de l'UE. Il harmonise d'une part le niveau de protection des personnes privées au sein de l'UE [1717], par le recours à un Règlement et par un mécanisme spécifique de règlement des différents, par le mécanisme spécifique du guichet unique (art. 56 RGPD).

2095 Ce mécanisme du guichet unique peut cependant avoir un impact extraterritorial. L'autorité de contrôle autrichienne a ainsi donné

1714. Nardi, *« Courtoisie internationale »*, p. 330.
1715. « Droit de la coordination des ordres juridiques » pour Pierre Mayer.
1716. Guillaume Florence, *Droit international privé : partie générale et procédure civile internationale*, 4e éd., Bâle 2018, p. 1.
1717. Évitant ainsi la pratique du « forum shopping » par les entreprises.

partiellement suite à une plainte à l'encontre d'une entreprise établie en Suisse [1718].

Il s'agit de la première procédure d'une autorité de contrôle étrangère qui impacte une entreprise suisse sur le fondement du RGPD. Cette procédure confirme l'effectivité du contrôle a posteriori même en présence d'un élément d'extranéité. Elle démontre que les entreprises suisses peuvent être concernées par l'application du RGPD, si elles remplissent les conditions de l'art. 3, al. 2 RGPD du fait de leur modèle d'affaire. L'autorité autrichienne retient que le facteur décisif réside dans l'intention exprimée par l'entreprise d'offrir à des personnes situées dans l'UE des biens ou des services. La décision retient comme critère déterminant de matérialisation de cette intention dans le cas d'espèce : l'utilisation d'un domaine de premier niveau (.at), la langue d'un site web (l'allemand) ou la possibilité de recevoir des offres par le biais d'une lettre d'information émise par la sociéte établie en Suisse. Tout élément permettant de démontrer que l'offre a ciblé le marché de l'UE pourra être retenu par l'autorité de contrôle pour l'application du RGPD dans l'Union. 2096

Cette décision est importante pour le domaine touristique et une analyse précise de l'applicabilité du RGPD devra être conduite. Si le RGPD est applicable au cas d'espèce, alors les mesures appropriées doivent être prises et les obligations mises en œuvre. La désignation d'un représentant dans l'UE est obligatoire pour les entreprises suisses soumises au RGPD. Ainsi tout responsable du traitement ou sous-traitant établi en Suisse qui offre des biens ou des services à des personnes situées dans l'UE et traite leurs données personnelles dans le cadre de cette activité (art. 3 al. 2 LPD) sera concerné. Ce représentant constitue le point de contact dans l'UE pour les autorités de contrôle et les personnes concernées pour toute question relatives au respect du RGPD ou à l'exercice des droits des personnes concernées. 2097

A la demande des autorités autrichiennes, le défendeur a désigné un représentant. La décision autrichienne confirme que le représentant ne porte pas la responsabilité du traitement de données 2098

1718. Autorité autrichienne de protection des données, *Décision DSB - D130.206/0006-DSB/2019 du 22 août 2019*, ECLI :AT :DSB :2019 :DSB.D130.206.0006.DSB.2019, consid. a-e.

illicite.

2099 La désignation d'un représentant donne compétence aux autorités de contrôle de l'UE pour l'application effective du RGPD. Cette compétence est justifiée du fait de l'autonomie du droit de l'Union, reconnue par la Cour de Justice de l'Union européenne dans sa jurisprudence [1719]. Cette autonomie repose sur les droits fondamentaux de nature constitutionnelle dont le droit de la protection des données est un des éléments.

2100 La règle du conflit de loi demeure cependant entière avec les pays tiers de l'union, comme la Suisse. Cela signifie, que le juge suisse pourrait également être saisi dans le cadre d'un recours juridictionnel a posteriori, par la voie judiciaire ou administrative. Cette concurrence de juridictions crée une insécurité juridique en lien avec l'autorité de la chose jugée (res iudicata) et la règle non bis in idem. Ce risque a été soulevé par l'Autriche lors du vote du RGPD par le Conseil de l'UE le 14 avril 2016. De manière pragmatique, la personne concernée choisira vraisemblablement le rattachement au territoire de l'Union afin de bénéficier de la protection juridique la plus étendue possible. Le RGPD offre des droits plus étendus que la LPD suisse. En outre, l'obligation de désigner un représentant dans l'Union pour les responsables du traitement ou les sous-traitants, qui remplissent les conditions de l'art. 3, al. 2 RGPD, rendent illusoire l'exclusion de l'applicabilité du RGPD [1720].

F. Applicabilité du droit étranger impératif

2101 La Suisse a conclu des conventions internationales multilatérales et bilatérales de droit international privé. Certaines conventions occupent un rôle central, comme la Convention de Lugano du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale [1721].

1719. Arrêt CJUE du 3 septembre 2008, *Kadi*, C-402/05 P et C-415/05 P, ECLI :EU :C :2008 :461, consid. 282.

1720. Frei Nula, *Die Datenschutz-Grundverordnung und die Schweiz*, in : Epiney Astrid / Sangsue Déborah (édit.), *Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé*, 1e éd., Zürich 2019, p. 91.

1721. Conseil fédéral, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Convention de Lugano, CL) - Conclue à Lugano le 30 octobre 2007 (RS 0.275.12, RO 2010 5609)*, in : Conseil fédéral (https ://www.admin.ch/), Berne 2007, p. « https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html » (04/04/2020).

Cette convention clarifie les règles de conflit de juridiction et les règles de reconnaissance et d'exequatur des décisions étrangères. Le champ d'application de cette convention est limité aux litiges en matière civile et commerciale. Les litiges en matière administrative sont exclus du champ d'application de la convention (art. 1, al 1 et 2 CL). Cela signifie donc que les sanctions des autorités de contrôle européennes en application du RGPD ne sont pas exécutables en Suisse à ce jour. Une nouvelle convention internationale serait nécessair [1722]. La Suisse est également membre de la conférence de La Haye depuis le 6 mai 1957 et a conclu plusieurs conventions de La Haye.

Le juge suisse saisi par une affaire dotée d'un élément d'extranéité appliquera les règles de conflit de lois pour déterminer sa compétence et le droit applicable, en-dehors des secteurs spécifiques des accords bilatéraux et multilatéraux. Les accords bilatéraux et multilatéraux conclus par la Suisse et les accords d'association à Schengen et Dublin engagent la Suisse à reprendre le développement de l'acquis communautaire dans les secteurs spécifiques de ces accords. 2102

Le législateur suisse a repris la directive (UE) 95/46/CE dans le champ d'application de l'accord Schengen et de Dublin [1723]. Il a cependant refusé d'intégrer la Directive dans le droit interne suisse de manière générale. Cette interprétation restrictive n'a pas pour autant empêché la Suisse d'obtenir une évaluation satisfaisante lors de l'évalua- 2103

1722. Voir les motions 16.3752 du 28 septembre 2016 et 17.5528 du 4 décembre 2017 de Fiala Doris au Parlement sur ce thème.

1723. Accord du 9 novembre 2004 entre la Confédération suisse et la Communauté européenne modifiant l'accord entre la Confédération suisse et la Communauté économique européenne du 22 juillet 1972 pour ce qui concerne les dispositions applicables aux produits agricoles transformés, FF 2004 p. 5965 ; Accord du 9 novembre 2004 entre la Confédération suisse et la Communauté européenne prévoyant des mesures équivalentes à celles prévues dans la directive 2003/48/CE du Conseil en matière de fiscalité des revenus de l'épargne sous forme de paiements d'intérêts (avec annexes et mémorandum d'entente), FF 2004 p. 6175 ; Message du 3 novembre 2009 relatif à la politique climatique suisse après 2012 (Révision de la loi sur le CO2 et initiative populaire fédérale «pour un climat sain») (09.067), FF 2009 p. 6749 et p. 6769.

tion de la mise en oeuvre des accords de Schengen [1724].

2104 Concernant le RGPD, il existait un conflit entre la Commission européenne et le Conseil de l'UE sur la portée extraterritoriale du RGPD pour les pays tiers, ayant signé comme la Suisse l'accord Schengen. Dans sa décision du 14 avril 2016, la Commission européenne considère que le RGPD « constitue un développement de l'acquis de Schengen pour les quatre pays associés à la mise en œuvre, à l'application et au développement de cet acquis [1725]». La Commission indique expressément qu'elle « déplore les changements apportés à la proposition initiale de la Commission par la suppression des considérants 136, 137 et 138 liés à l'acquis de Schengen ». Ainsi, elle confirme l'existence d'un conflit entre la Commission europeéenne et les États membres de l'Union concernant la reprise de l'acquis communautaire par les États tiers, comme la Suisse, qui sont parties à l'accord Schenghen.

(a) Analyse critique

2105 Du fait de la souveraineté de responsabilité [1726] des États, qui est une responsabilité de protection des personnes physiques, il serait cohérent que les États tiers ayant signé des accords bilatéraux avec l'UE, appliquent les dispositions du RGPD aux personnes concernées par un traitement de données personnelles dans le cadre des accords bilatéraux.

2106 Si le RGPD n'a pas été formellement repris dans le cadre des accords bilatéraux, il a cependant influencé le législateur pour développer la nouvelle loi sur la protection des données en suisse, ce qui était conseillé par la doctrine [1727].

2107 Le droit européen de la protection des données étant harmonisé au sein de l'UE, la Suisse a intérêt a adopter ce standard de réfé-

1724. Epiney Astrid / Nüesch Daniela (édit.), *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, 1e éd., Zürich 2015, p. 43.

1725. Conseil de l'UE, *Décision 7920/16 du 14 avril 2016 - Dossier interinstitutionnel (2012/0011 (COD))*, in : EUR-Lex (https ://eur-lex.europa.eu/), Bruxelles 2016, p. « https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CONSIL:ST_7920_2016_INIT&from=LV » (04/04/2020), Annexe 2, p. 3.

1726. Besson, *Droit international public*, p. 118.

1727. Epiney / Nüesch, *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, p. 43.

rence pour renforcer la sécurité juridique et l'attractivité du marché suisse pour les entreprises multinationales. L'adoption de ce standard de référence en Suisse apparaît comme une condition nécessaire pour conserver la décision d'adéquation des législation octroyée par la Commission européenne.

La Suisse n'est pas un État membre de l'UE et le RGPD ne fait pas partie des accords bilatéraux. Par conséquent, le mécanisme du guichet unique tel qu'il est prévu dans le RGPD et qui permet de régler les contentieux résultant d'un conflit de lois au sein de l'UE, ne semble pas applicable au Préposé fédéral de la protection des données en Suisse. En tant qu'État tiers, le juge suisse appliquera les règles de conflit de lois du droit international privé, dans le cas d'une affaire internationale de droit privé [1728]. 2108

Une personne concernée par une violation des dispositions du RGPD devra effectuer un recours dans l'UE, au lieu d'établissement du responsable du traitement ou du sous-traitant établi dans l'UE. En pratique, le handicap de la langue et la méconnaissance du droit de procédure civile dans l'État membre constituent un frein à l'accès à la justice et à un recours juridictionnel effectif. C'est pourquoi, les associations qui représentent les intérêts des personnes concernées par une violation des dispositions du RGPD sont particulièrement utiles (art. 80 RGPD). 2109

Au sein de l'Union, le RGPD impose le recours à l'assistance administrative (art. 55 RGPD) pour les conflits entre États-membres ou en cas de conflit entre la Commission européenne et un État membre. La question se pose de savoir si la procédure serait transposable dans les États tiers, comme la Suisse [1729]. Afin de renforcer la sécurité juridique et la protection effective des personnes privées, des accords bilatéraux ou multilatéraux entre États pourraient prévoir l'assistance mutuelle entre autorités de contrôle, préalablement à sa formalisation sous l'égide de la Convention 108 modernisée. C'est ce que prévoit l'art. 49 du projet de LPD. Au sein de l'UE, une coopération entre autorités compétentes est prévue sur la base du mécanisme du contrôle de la cohérence (art. 57 RGPD) et de l'autorité chef de file en présence d'une base légale (art. 56 2110

1728. Sauf si la Convention de Lugano est applicable.

1729. Epiney / Nüesch, *Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes = La mise en oeuvre des droits des particuliers dans le domaine de la protection des données*, p. 39.

RGPD). En cas de sanction, le requérant peut intenter un recours (art. 74 RGPD). Les tribunaux compétents sont ceux de l'État sur lequel les autorités compétentes ont leur siège (art. 74 RGPD).

2111 Ces règles internes à l'Union sont importantes pour faciliter la résolution des litiges entre États membres lorsque le RGPD laisse une marge de manoeuvre aux États membres dans les mesures d'exécution [1730]. Lorsque les lois des États membres différents des dispositions du RGPD, et que le RGPD délègue aux États membres les mesures d'exécution des dispositions du Règlement (ex : art. 8 RGPD, art. 49, al. 5 RGPD et art. 23, al. 1 RGPD), alors les règles de conflit de lois du droit international privé s'appliquent. L'art. 82, al. 6 RGPD qui donne le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi, par voie judiciaire renvoie au droit de l'État membre. Le RGPD laisse ainsi une marge de manoeuvre aux États qui disposent de dispositions nationales différentes. En l'absence de règle de conflits de lois, les parties pourraient procéder à du forum shopping en fonction des régimes juridiques des 28 État-membres (27 après la sortie du Royaume-Uni).

2112 Lorsque le Règlement laisse les États membres de l'Union prendre des mesures d'exécution nationales quelle loi nationale sera applicable en cas de compétences concurrentes ?

2113 La détermination du droit applicable se posera lorsqu'un État est libre de prendre des mesures d'exécution du RGPD dans son droit national. Une vérification des critères choisis pour l'application de la législation sur la protection des données est nécessaire : lieu d'établissement principal du responsable du traitement ou lieu de résidence de la personne concernée ? La réponse à cette question a des conséquences sur la protection juridique effective des personnes concernées. En effet, le RGPD laisse parfois une marge de manoeuvre aux États dans le domaine du traitement de données personnelles. C'est le cas de l'art. 8 RGPD et de l'âge du consentement.

1730. Jault-Seseke Fabienne / Zolynski Célia, *Le règlement 2016/679/UE relatif aux données personnelles*, in : Recueil Dalloz 2016/32, p. 1876.

§3 La Jurisprudence de la CJUE

I. La portée géographique du droit au déréférencement

Quels enseignements tirer de la jurisprudence de la Cour de justice de l'Union européenne ? 2114

La Cour de justice a tranché la question de la portée territoriale du droit au déréférencement en-dehors de l'Union, tel qu'il ressort de l'art. 17 RGPD [1731]. La Cour était saisi par le Conseil d'État français pour déterminer de quelle manière l'exploitant d'un moteur de recherche, devait mettre en œuvre ce droit au déréférencement. Si, à la date de l'introduction de la demande de décision préjudicielle, la directive 95/46 était applicable, celle-ci a été abrogée avec effet au 25 mai 2018, date à partir de laquelle est applicable le règlement 2016/679 [1732]. Il s'agissait pour la Cour de déterminer si Google est tenu d'opérer ce déréférencement sur l'ensemble des versions de son moteur ou si, au contraire, il n'est tenu de l'opérer que sur les versions de celui-ci correspondant à l'ensemble des États membres, voire, uniquement, sur celle correspondant à l'État membre dans lequel la demande de déréférencement a été introduite [1733]. 2115

Pour la Cour, la question de la portée géographique du droit au déréférencement se limite aux versions du moteur de recherche correspondant à l'ensemble des États membres ou consultées depuis l'un de ces États. Dans le respect du principe de proportionnalité, la Cour refuse l'application mondiale du droit au déréférencement, telle que demandée par la CNIL. Elle respecte ainsi le principe de compétence territoriale exclusive des États tiers. 2116

Elle adhère ainsi à l'argument de Google qui relève que le droit au déréférencement tel que reconnu dans la jurisprudence de la Cour de Justice de l'Union européenne [1734] « n'implique pas nécessairement que les liens litigieux soient supprimés, sans limitation géo- 2117

1731. Arrêt CJUE du 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI :EU :C :2019 :772, consid. 513.
1732. *Idem*, consid. 40.
1733. *Idem*, consid. 43.
1734. Arrêt CJUE du 13 mai 2014, *Google Spain et Google*, C-131/12, ECLI :EU :C :2014 :317, consid. 82.

graphique, sur l'ensemble des noms de domaine de son moteur ».

2118 Elle confirme ainsi la perspective de Google selon laquelle une telle interprétation, la CNIL aurait méconnu les principes de courtoisie et de non-ingérence reconnus par le droit international public et porté une atteinte disproportionnée aux libertés d'expression, d'information, de communication et de la presse garanties, notamment, par l'article 11 de la Charte des droits fondamentaux de l'Union européenne.

2119 Par conséquent, elle confirme que le droit à la protection des données n'est pas un droit absolu, et qu'il doit être mis en balance avec d'autres droits fondamentaux [1735].

2120 Elle retient également que les mécanismes de coopération tels qu'ils ressortent des art. 56, 60 et 66 RGPD ne prévoient pas de base légale au déréférencement mondial. Ainsi Google n'a pas l'obligation d'opérer un déréférencement sur l'ensemble des versions de son moteur de recherche. Dans le but de garantir un niveau élevé de protection des données dans tous les États membres de l'Union, la Cour rappelle que le règlement est directement applicable dans tous les États membre de l'Union. Au sein de l'Union, « les États conservent cependant une marge de manoeuvre et peuvent prévoir des dérogations notamment pour protéger la liberté d'information [1736]». Cette jurisprudence revêt une importance majeure car elle relativise la portée du règlement en tant qu'instrument juridique unifiant l'application de la protection des données dans les États-membres et laissant peu de marges de manœuvre aux États. Elle surprend en redonnant une latitude d'interprétation aux autorités nationales, latitude qui avait créer une fragmentation de la mise en oeuvre de la directive 95/46/CE, à l'origine de l'adoption d'un Règlement.

1735. Arrêt CJUE du 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI :EU :C :2019 :772, consid. 67 et 69. Voir aussi arrêt CJUE du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU :C :2010 :662, consid. 48, ainsi que l'avis 1/15 (Accord PNR UE-Canada) du 26 juillet 2017, EU :C :2017 :592, consid. 136.

1736. Arrêt CJUE du 24 septembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI :EU :C :2019 :772, consid. 67 et 69.

II. La portée géographique du Cloud Act

Le second exemple qui mérite d'être examiné est le Clarifying Lawful Overseas Use of Data Act [1737] (ci-après le « Cloud Act »). Considéré comme une réponse américaine au caractère extra-territorial du RGPD [1738], le Cloud Act a été approuvé par le Congrès américain et promulgué par le président Trump le 23 mars 2018. Il est intégré dans une loi fiscale américaine de plus de 900 pages dans la dernier partie [1739] (division V). Il vise à permettre aux forces de l'ordre de requérir des fournisseurs de services de communication électronique américains qu'ils transmettent aux instances étatiques des données stockées sur des serveurs situés aux États-Unis ou dans des pays étrangers (consid. 2713) [1740]. La plupart des données personnelles étant stockées sur des Clouds détenus par des entreprises américaines, le Cloud Act a une portée territoriale très vaste, car elle permet aux services de police américains d'accéder à une proportion importante des données échangées du point de vue mondial [1741]. 2121

Ni la personne concernée par l'accès, ni le pays dans lequel l'accès est opéré, ni le pays dont la personne concernée est citoyenne ne sont tenus informés de cet accès [1742]. 2122

Le Cloud Act vient enrichir le Stored Communication Act, qui fait partie du Electronic Communications Privacy Act, adopté en 1986. Le Stored Communication Act visait historiquement à protéger les citoyens contre les dérives policières et les accès trop aisés à leurs 2123

1737. United States Congress, *Consolidated Appropriations Act (H.R. 1625)*, in : US Congress (https ://www.congress.gov/), Washington D.C. 2018, p. « https : / / www . congress . gov / bill / 115th - congress / house - bill / 1625 » (04/04/2020), pp. 866-878, Pub.L. 115-141 ; Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act (White Paper)*, in : US DoJ (https ://www.justice.gov/), Washington D.C. 2019, p. « https://www.justice.gov/dag/page/file/1153436/download » (04/04/2020).

1738. Cassart Alexandre, *Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD*, in : Revue du Droit des Technologies de l'information 2018, p. 41.

1739. United States Congress, *Consolidated Appropriations Act*, p. 866.

1740. Cassart, *Premières réflexions sur le Cloud Act*, p. 41.

1741. *Ibidem.*

1742. *Ibidem.*

données [1743].

2124 Une entité gouvernementale doit disposer d'un mandat pour exiger d'un fournisseur de services de communication électronique qu'il transmette le contenu d'une communication électronique stockée pendant 180 jours ou moins [1744]. Par contre, au-delà d'une durée de conservation de 180 jours de stockage, il suffit d'une subpoena 21 et d'une notification préalable pour obtenir la divulgation. La doctrine considère avec raison que le seuil des 180 jours n'est pas adapté aux usages des services digitaux de nos jours et a donc perdu de sa pertinence.

2125 Le Cloud Act vient clarifier la portée territoriale du Stored Communication Act, en particulier concernant l'accés aux données stockées dans dans des serveurs localisés en dehors du territoire américain, mais gérés par des sociétés américaines ?

2126 Avant la clarification par le Cloud Act, la doctrine en faveur de la souveraineté étatique conseillaient d'utiliser les traités internationaux réglant les coopérations policières et pénales renforcées entre les États (Mutual Legal Assistance Treaty). En 2013, l'affaire Microsoft a été un catalyste pour trouver une solution à ce conflit de juridictions. Lors d'une enquête relative à un trafic de stupéfiants, un juge new-yorkais a lancé un mandat sur la base du Stored Communication Act, obligeant Microsoft à produire tous les courriels et informations associés à un compte utilisateur. Si ces dernières étaient stockées sur des serveurs américains de Microsoft, les courriels se trouvaient sur un serveur situé à Dublin, en Irlande. Les renseignements ont été fournis concernant le compte mais aucun message électronique n'a été envoyé sur le fondement de l'absence de compétence pour lancer un mandat visant des données situées á

1743. Cassart, *Premières réflexions sur le Cloud Act*, p. 44 ; Voir aussi les critiques de Solove Daniel J., *Reconstructing electronic surveillance law*, in : George Washington Law Review 2003/72, p. 1264 ; Kesan Jay P. / Hayes Carol M. / Bashir Masooda N., *Information privacy and data control in cloud computing : Consumers, privacy preferences, and market efficiency*, in : Washington and Lee Law Review 2013 70/1, p. 341 ; Borchert Christopher J. / Pinguelo Fernando M. / Thaw David, *Reasonable Expectations of Privacy Settings : Social Media and the Stored Communications Act*, in : Duke Law and Technology Review 2014/13, p. 36 ; ou encore Kattan Ilana R., *Cloudy privacy protections : why the Stored Communications Act fails to protect the privacy of communications stored in the cloud*, in : Vanderbilt Journal of Entertainment and Technology Law 2010 13/3, p. 617.

1744. Cassart, *Premières réflexions sur le Cloud Act*, p. 44.

l'étranger. En application de la règle du conflit de loi en droit international privé, Microsoft demandait l'application du Mutual Legal Assistance Treaty conclu entre les USA et l'Irlande. Considérant que Microsoft avait le contrôle effectif sur les données, peu importe leur localisation effective, le juge a considéré qu'il n'y avait aucune violation de la souveraineté étrangère et aucune application extraterritoriale du Stored Communication Act. Le mandat était donc valable. La Cour d'Appel a invalidé le mandat le 24 janvier 2017. La Cour a recherché l'intention du législateur lors de l'élaboration du Stored Communication Act et a retenu qu'il n'existait pas d'indices démontrant une volonté du législateur américain de conférer une portée extraterritoriale au Stored Communication Act.

C'est dans ce contexte que le Cloud Act a été adopté par le Congrès. 2127

L'objet du Cloud Act est de conférer une portée extraterritoriale au Stored Communication Act (consid. 2713). Il étend la possibilité prévue à l'article 2703 du Stored Communication Act d'obtenir d'un fournisseur de service de communication électronique qu'il conserve ou transmette à l'autorité certaines données, et ce même si les données se trouvent sur un territoire étranger [1745]. Le Cloud Act définit la notion de société américaine comme une société constituée aux États-Unis ainsi que les sociétés contrôlées par elle, ce qui contribue au caractère extraterritorial de la législation. Selon cette définition, les données stockées à l'étranger sur des serveurs gérés par une filiale américaine pourront être être soumises au Cloud Act. 2128

Le Cloud Act utilise une formulation similaire à l'accord FATCA. En effet, si les établissement bancaires étaient qualifiés de qualified intermediary (QI) dans l'accord FACTCA, ce sont les États qui sont, dans le Cloud Act, qualifiés de « qualifying Foreign Governments », c'est-à-dire de gouvernement éligibles à faire partie du programme d'échange de renseignements. A ce jour aucun accord bilatéral n'a été conclu entre les États-Unis et l'Union européenne, selon les modalités du chapitre 119 du Stored Communication Act. Le principe de réciprocité permettra à l'Union européenne et aux États tiers d'avoir accés aux communications de leurs ressortissants. 2129

La loi fiscale américaine « Foreign Account Tax Compliance Act » (FATCA) vise à permettre aux États-Unis d'obtenir l'imposition de 2130

1745. Cassart, *Premières réflexions sur le Cloud Act*, p. 46.

tous les comptes détenus à l'étranger par les personnes soumises à l'impôt aux États-Unis. Il s'agit d'une réglementation américaine unilatérale, qui est valable pour tous les pays. FATCA exige que les institutions financières étrangères transmettent aux autorités fiscales américaines des informations relatives aux comptes américains ou sinon, qu'elles perçoivent un impôt élevé.

2131 Le Cloud Act offre un nouveau recours aux fournisseurs de service pour contester la licéité des demandes de renseignements. Ce recours en modification ou annulation du mandat pourra être valable si la personne concernée par la demande n'est pas un ressortissant américain (« US person ») et ne réside pas sur le territoire américain. Ensuite il doit exister un risque de conflit de loi avec l'État étranger éligible. Dès qu'un accord exécutif existera entre les États-Unis et l'Union européenne ou des États tiers comme la Suisse, les recours seront possibles dans les 14 jours suivant la demande des autorités. Le requérant a l'obligation de conserver les documents durant la période d'attente, et ne devra les remettre qu'après un ordre du juge de produire les documents demandés immédiatement si cela est jugé nécessaire pour empêcher un résultat négatif au sens du consid. 2705(a)(2).

2132 En outre, « aucun motif d'action ne peut être invoqué devant un tribunal contre le fournisseur d'un service de communication par fil ou électronique, ses dirigeants, employés, agents ou autres personnes désignées pour avoir fourni des renseignements, des installations ou de l'aide conformément à une ordonnance du tribunal en vertu du présent chapitre ».

2133 Si le droit unilatéral dont se prémunissent les États-Unis avec le Cloud Act en violation de la souveraineté des autres États pourrait par exemple justifier des contre-mesures d'autres États, les États-tiers à l'Union européenne pourraient également s'interroger sur la licéité et l'applicabilité du RGPD sur leur territoire. Pour faire face au Cloud Act, une solution serait d'étendre les dispositions du RGPD, lequel texte pouvant constituer un standard international en matière de protection des données personnelles. Il existe une

incompatibilitté entre le RGPD est le Cloud Act [1746].

Les territoires connaissent cependant une superposition de normes juridiques internationales différentes qui peuvent entrer en conflit sans que l'on puisse toujours les ordonner les unes par rapport aux autres [1747]. Cette fragmentation du droit est source d'insécurité juridique. 2134

A. Une application extra-territoriale pour garantir un niveau de protection étendu

Le caractère extra-territorial du Règlement témoigne de la volonté que soient mieux pris en compte le droit de la protection des données en-dehors de l'UE afin de protéger les personnes situées dans l'UE dont les données sont traitées. Le RGPD étend le champ d'application territorial pour offrir une protection élargie à toutes les personnes concernées qui se trouvent dans l'Union européenne, indépendamment de la localisation effective du traitement (Schutzprinzip du droit allemand). 2135

De manière pragmatique, le caractère extra-territorial du RGPD répond aussi à des objectifs stratégiques et économiques mis en exergue par des auteurs comme Michael Reisman, Eric Posner, Andrew Guzman. Il s'inscrit dans une logique de responsabilité transnationale adhérant à une forme de morale internationale soulignés par Martin Koskenniemi, David Kennedy et Anne Orford [1748], connus des domaines de la défense des droits de l'homme, du droit de l'environnement ou du droit pénal international. 2136

La Commission européenne détient une compétence matérielle normative et est légitime à donner á ses normes une portée extra-territoriale. Pour Samantha Besson, « c'est le cas des États á l'égard de ses ressortissants hors de son territoire [1749] ». 2137

En droit international public, la théorie des effets joue également un rôle dans la résolution des litiges en lien avec un élément d'extra- 2138

1746. Gidari Albert, *What will Microsoft and Ireland do with the new Cloud Act warrant ?*, in : Center of Internet and Society - Stanford Law School (http : / / cyberlaw . stanford . edu/), Stanford 2018, p. « http ://cyberlaw.stanford.edu/blog/2018/04/what-will-microsoft-and-ireland-do-new-cloud-act-warrant » (04/01/2020).
1747. Besson, *Droit international public*, p. 23.
1748. *Idem*, p. 38.
1749. *Idem*, p. 110.

néité. En droit de la concurence américain, lorsque les activités anticoncurrentielles produisent des effets sur le territoire des États-Unis et que ces effets affectent son commerce extérieur, alors la juridiction américaine peut se reconnaître compétente [1750]. En 1949, la Cour Supréme américaine a posé l'exigence d'un effet substantiel sur le commerce [1751]. La théorie des effets a impacté la Suisse et le Sherman Act a été appliqué dans le cadre d'une entente entre producteurs suisses dans le domaine de l'horlogerie [1752].

2139 Ainsi la théorie des effets peut donner compétence á un État dans le cadre d'un litige avec une portée internationale et un élément d'extranéité [1753]. Dans ces deux cas d'espèce, la Cour suprême a reconnu sa compétence territoriale en vertu de la théorie des effets tout en considérant les intérêts étrangers en faisant application du principe de courtoisie internationale.

2140 La théorie des effets a également été défendue par la Commission européenne et la Cour de justice et a permis une extraterritorialité des lois européennes, consacrée aujourd'hui par le RGPD. L'action en justice d'un État à l'encontre d'une entreprise étrangère peut cependant être interprétée comme étant dirigée directement contre l'État étranger et être ainsi la source d'un contentieux diplomatique [1754].

2141 La divergence d'intérêts économiques peut être une source de conflits entre États. Le RGPD et le Cloud Act ont le potentiel de créer des interférence dans les relations internationales du fait du rôle stratégique des données dans l'économie et la politique des États. Un abus dans le domaine de la compétence d'exécution n'est dès lors pas hypothétique.

2142 L'action civile en droit de la concurrence joue un rôle essentiel

1750. Arrêt de la Cour suprème américaine de 1962, *Continental Ore Co v. Union Carbide Corporation*, 370 U.S 690, consid. 13.
1751. Arrêt de la Cour Suprême américaine de 1949, *US v. General Electrics Co.*, 82 F. Supp. 753, consid. 85 (D.N.J 1949).
1752. Arrêt de la Cour suprême américaine de 1962, *États-Unis c. Watchmakers of Switzerland information Center*, Trade Cases 70, 600 (S.D.N.Y 1962), consid. 50.
1753. Arrêt de la Cour suprême américaine de 1976, *Timberlane v. Bank of America*, consid. A.
1754. Lettre de l'ambassadeur de France devant le tribunal du district de New-York du 22 avril 1927, dans l'affaire de la Société Commerciale des Potasses d'Alsace.

dans certains pays comme aux États-Unis du fait de son caractère préventif et dissuasif. L'intervention d'un gouvernement étranger dans une procédure privée est perçue aux États-Unis comme une atteinte aux droits des parties et à l'indépendance du pouvoir judiciaire reconnue par la Constitution [1755].

Le recours à l'action civile peut être source de difficultés sur le plan international [1756]. L'allocation de dommages et intérêts triples et la possibilité de class actions aux États-Unis en droit de la concurrence inquiètent légitimement les États en raison des conséquences pour leurs entreprises. Le RGPD prévoient la possibilité de class action et nous recommandons l'introduction d'un modèle de sanctions similaires au droit de la concurrence américain afin d'équilibrer les rapports de force avec les États-Unis. Ces sanctions peuvent être cependant injustifiées si la pratique de l'entreprise est conforme à la politique du pays dont il est issu. En parallèle des sanction civiles, des sanctions pénales peuvent être prévues comme c'est le cas du droit de la protection des données en Suisse. Les infractions au droit de la protection des données sont considérées en Suisse comme une faute pénale, pas dans l'Union européenne. La condamnation possible des dirigeants en Suisse constitue cependant un facteur de responsabilisation des acteurs. 2143

Le concept de souveraineté territoriale a été fragilisé depuis une dizaine d'année depuis l'accord FATCA. Cette législation, suivie du RGPD dans l'UE et du Cloud Act aux États-Unis, témoigne d'une approche extensive du principe de souveraineté. Les États-Unis ont été les premiers á élaborer une loi au caractère extra-territoriale. Il s'agit du « Qualified Intermediary » en 2001, puis de l'accord « Foreign Account Tax Compliance Act » (ci-après accord « FATCA »), adopté le 18 mars 2010, par le parlement américain sous la présidence de Barack Obama et entrée en vigueur était prévue le 1er janvier 2013 par les pays signataires. 2144

La signature de cet accord FATCA le 14 février 2013 par la Suisse s'expliquait pour des raisons économiques : la Suisse souhaitait maintenir la compétitivité des banques helvétiques sur le marché américain et conserver l'accès au marché américain. Elle évitaient 2145

1755. Neale Alan Derrett / Stephens Mel L., *International business and national jurisdiction*, 1e éd., Oxford 1988, p. 30 ss.

1756. Déclaration de l'assistant attorney général Charles F. Rule devant la Senate Committee on the Judiciary, 21 juin 1985.

ainsi de devoir s'acquitter d'une taxe de 30% sur les revenus générés aux États-Unis par les banques suisses (retenue à la source à hauteur de 30% sur les produits et revenus aux États-Unis). Elle conservait des relations commerciales paisibles avec les États-Unis. La Chine et la Russie ont refusé de signer cet accord.

2146 L'accord FATCA a pris effet au 1er juillet 2014 après des échanges de notes entre les deux pays et le refus d'un référendum populaire. L'accord FATCA oblige les établissements bancaires helvétiques à respecter l'accord FATCA. En cas de violation de leurs obligations, des sanctions financières dissuasives de la part des États-Unis sont prévues. Cette loi trouve son origine dans plusieurs scandales d'évasion fiscale impliquant des institutions financières, en particulier UBS en Suisse [1757]. Il ne prévoyait pas de principe de réciprocité ni d'échange automatique de renseignements. Les banques rendaient leur transfert de données licites en faisant signer aux titulaires de comptes une déclaration de consentement.

2147 Le caractère extra-territorial de tout accord qui s'impose á la Suisse, pour des raisons économiques ou politiques soulève la problématique de la conformité des obligations de ces accords au caractère extra-territorial avec les lois en vigueur en Suisse.

2148 Si le RGPD s'applique aux citoyens européens qui résident en Suisse, l'accord FACTA s'applique quant á lui aux citoyens américains même s'ils sont binationaux.

2149 Comme le démontre l'échange de renseignements en matière fiscale, les États coopèrent davantage afin de faire face à l'internationalisation des activités humaines et d'assurer le respect de leurs ordres juridiques (entraide administrative) [1758].

2150 Le caractère révolutionnaire de cette économie de plateforme résulte de la disparition des notions de temps, d'espace et de contrainte linguistique [1759]. Le marché digital est accessible de manière ubiquitaire par chacun en tout lieu, car il n'est pas situé dans un zone

1757. United States Senate, *Tax Haven Banks and U.S. Tax Compliance - Staff Report of the Permanent Subcommittee on Investigations (Released on July 17, 2008)*, in : US Senate Committee on Homeland Security and Government Affairs, Washington D.C. 2008, p. 109.

1758. Grisel, *Application extraterritoriale du droit international des droits de l'homme*, p. 4.

1759. Pretelli, *Conflict of laws in the maze of digital platforms = Le droit international privé dans le labyrinthe des plateformes digitales*, p. 22.

géographique mais dans un cloud digital, qui pourrait couvrir la planète dans son ensemble [1760].

Ainsi le RGPD tire sa légitimité d'une volonté de réglementer un marché des données personnelles oligopolistique et décentralisé qui s'affranchit du territoire étatique du fait de l'essor des entreprises privées dont le modèle d'affaires repose sur la développement de plateformes digitales [1761] et le traitement de Big Data. Les capitalisations boursières combinées des GAFA dépassent les 3000 milliards de dollars, soit plus que le PIB de la France ou du Royaume-Uni [1762]. 2151

Face à la difficulté de la résolution des conflits de lois et de juridictions droit international privé, certains juristes ont souligné la nécessité de reconnaître une juridiction spécifique pour le cyberespace, et la disparition du droit international privé pour régir les transactions dans cet espace [1763]. Dans le domaine de la fiscalité internationale, l'échange d'informations en matière fiscale mis en place par l'OCDE a démontré que le rapport de force entre États pouvait faire émerger un espace de libre circulation des données personnelles dans un espace défini selon une architecture informatique spécifique [1764]. 2152

Pour Samantha Besson, questionner la légitimité du droit international revient à vérifier que les obligations morales que le droit international génère correspondent bien á des raisons morales d'agir qu'auraient les États et les particuliers indépendamment de ce droit [1765]. 2153

Les raisons morales d'agir du législateur européen se fondent sur la volonté de garantir un niveau élevé de protection des données dans l'Union en tant que droit fondamental à la protection des don- 2154

1760. *Idem*, p. 23.

1761. *Idem*, p. 20.

1762. Amazon, réalise 11 milliards de profits par an, et est exemptée d'impôt aux États-Unis depuis 2017. L'Europe n'a pas encore mis en oeuvre de « taxe GAFA ».

1763. McLachlan Campbell, *From Savigny to Cyberspace : Does the Internet Sound the Death-Knell for the Conflict of Laws ?*, in : Media and Arts Law Review 2006/11, p. 418.

1764. OCDE, *Echange de renseignements*, in : OCDE (https ://www.oecd.org/), Paris s.a., p. « » (04/01/2020) ; Committee of Experts on International Cooperation in Tax Matters, *The digitalized economy : selected issues of potential relevance to developing countries (E/C. 18/2017/6)*, in : United Nations Economic and Social Council (Fifteenth Session), Geneva 2017, pp. 1-5.

1765. Besson, *Droit international public*, p. 38.

nées consacré dans la Charte des droits fondamentaux de l'Union tout en favorisant la libre circulation des données personnelles dans l'Union.

2155 La légitimité de la conformité au droit international devrait moins venir de la peur des sanctions que de l'adhésion aux principes, valeurs et mécanismes qui sous-tendent ce droit et garantissent une protection juridictionnelle effective.

2156 Cette légitimité est au coeur selon nous de la durabilité et de l'intensité de la coopération internationale et repose sur l'adhésion á des valeurs communes á l'humanité dans son ensemble [1766].

III. L'extra-territorialité justifiée par une volonté de sécurité juridique

A. Vers une juridiction sans lien avec le territoire ?

2157 Alors que la territorialité joue traditionnellement un rôle central dans la détermination de la juridiction compétente, le concept de souveraineté n'exige pas toujours que la juridiction soit basée sur la territorialité, uniquement. Face à la multiplication des « exceptions » au principe de territorialité, il faut reconnaître que « La juridiction, en tant que concept jurisprudentiel n'est pas enracinée dans la territorialité [1767] ».

2158 Au-delà de la réflexion entre règlementation territoriale ou extra-territoriale, la compétence juridictionnelle territoriale et extra-territoriale est centrale.

B. Un nouvel espace de circulation des données personnelles

2159 Le RGPD abandonne en partie l'objectif de localisation de l'activité de traitement et s'efforce de traduire dans la règle de droit l'existence d'un nouvel espace transnational dédié au partage des données personnelles [1768]. Il reflète ainsi la jurisprudence de la CJUE,

1766. Delmas-Marty Mireille, *Vers une communauté de valeurs ? : les forces imaginantes du droit (IV)*, 1e éd., Paris 2011, p. 45.
1767. Lessig Lawrence, *The law of the horse : What cyber law might teach*, in : Harvard Law Review 1999/113, p. 506.
1768. Bergé Jean-Sylvestre / Grumbach Stéphane, *La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires*, in : Journal du droit international 2016/4, pp. 1153-1173.

notamment les affaires Google Spain et Amazon [1769]. Dans ces affaires, la CJUE, s'est fondée sur la nécessaire protection effective et complète des droits et libertés fondamentales des personnes physiques, pour donner une interprétation large du critère d'application spatial de la protection européenne des données personnelles, en-dehors de l'Union. Elle conclut á l'applicabilité de la protection européenne, même si le traitement se fait en-dehors de l'UE, dès lors qu'il existe dans l'Union une succursale dont la mission est de promouvoir et de vendre des espaces publicitaires (Google Spain), ou un représentant du responsable du traitement localement chargé du recouvrement de créances (Weltimmo).

Dans la logique de cette nécessaire protection effective et complète 2160
des droits et libertés fondamentales des personnes physiques, un courant doctrinal favorable à l'émergence d'un droit mondial (Global Law), sous la plume de Jean-Sylvestre Bergé, Stéphane Grumbach [1770], et Mireille Delmas Marty, considère la numérisation et le traitement de larges quantités de données personnelles indépendamment d'un territoire comme les prémisses d'un nouvel espace d'échanges de données au niveau mondial (espace qualifié de « datasphère ») [1771]. Cet espace ferait naître un nouveau rapport aux territoires institutionnels classiques [1772] et soulèverait la question du maintien des « mécanismes juridiques existants », fondés sur l'adéquation entre un territoire et l'applicabilité du droit [1773]. Cette doctrine doit être mise en rapport avec la notion de droit transnational, présentée á l'université de Yale en 1956 [1774]. Ce droit transcenderait les nations, les États. Il fait référence á un ensemble de règles transnationales communes à une pluralité de systèmes juridiques [1775]. Pour les tenants de cette doctrine, le caractère extraterritorial d'une législation est la conséquence d'une insécurité juri-

1769. Arrêt CJUE du 1 octobre 2015, *Weltimmo*, C-230/14, ECLI :EU :C :2015 :639, consid. 66 : JurisData Nr. 2015-025844 : D. 2016, p. 1045, obs. H. Gaudemett-Tallon ; Arrêt CJUE du 28 juillet 2016, consid. 82, JurisData 2016-016129.
1770. Bergé / Grumbach, *La sphère des données et le droit*, p. 1153.
1771. *Idem*, p. 1157.
1772. *Idem*, p. 1159.
1773. Fallon Marc, *Les règles d'applicabilité en droit international privé*, in : Vander Elst Raymond (édit.), *Mélanges offerts à Raymond Vander Elst*, 1e éd., Bruxelles 1986, p. 285 ; Fallon Marc, *Les frontières spatiales du droit privé européen selon le droit de l'Union européenne*, in : Frontières du droit privé européen 2012, p. 65.
1774. Jessup Philip Caryl, *Transnational law*, Yale 1956, pp. 1-113.
1775. Racine Jean-Baptiste, *Approches de droit global*, in : Journal du droit international 2019 146/3, p. 679.

dique qui fait courir un risque systémique [1776]. Il contribue á offrir des garanties et á sécuriser la stabilité d'une zone géographique dans un contexte donné. Cette perspective est partagée par les tenants d'une Convention de Genève proposée par Microsoft à la suite du ransomware Wanna Cry afin de reconnaître un espace digital sui generis. Ainsi, une législation extraterritoriale peut constituer une réponse appropriée pour atteindre une sécurité juridique. Ces États qui prennent au sérieux le risque d'insécurité juridique vont protéger leur marché intérieur, en l'espèce européen, avec une législation extra-territ-oriale [1777]. Il s'agit moins d'une volonté impérialiste que d'une volonté d'apporter des réponse nécessaire à l'interdépendance des États dans le domaine des activités digitales et aux risques systémiques potentiels. Pour Mireille Delmas Marty, cette approche d'un nouvel humanisme juridique propose de résister à la déshumanisation, de responsabiliser ses acteurs, et d'anticiper les risques à venir [1778].

C. Un nouveau rapport aux territoires institutionnels classiques

2161 Avec Samantha Besson, nous partageons l'idée du bienfondé d'intensifier la coopération basée sur des règles juridiques à valeur contraignante du fait de la multiplication des problèmes qu'il est urgent de régler de manière juridique à un niveau international : migrations, sécurité, environnement, relations économiques et financières [1779]. La protection des données s'inscrit dans cette logique universaliste et humaniste. Le choix d'une réglementation contraignante á portée extra-territoriale mérite ainsi d'être salué.

2162 Japon, Corée du Sud, Egypte nombreux sont les États hors UE appliquant le RGPD comme standard pour le droit de la protection des données. Dès lors, le RGPD pourrait-il être qualifié de nouveau Jus Cogens ?

2163 Le RGPD témoigne tout au moins d'une volonté politique d'appré-

1776. Lehmann Matthias, *Legal fragmentation, extraterritoriality and uncertainty in global financial regulation*, in : Oxford Journal of Legal Studies 2017 37/2, p. 418 ss.
1777. *Idem*, p. 433.
1778. Delmas-Marty Mireille, *International Law - Legal Theory (Lecture)*, in : UN Audiovisual Library of International Law (https ://legal.un.org/), Geneva s.a., p. « https://legal.un.org/avl/ls/Delmas-Marty_IL.html » (28/12/2019).
1779. Besson, *Droit international public*, p. 28.

hender sur le territoire des États membres un phénomène de circulation des données de grande ampleur, en créant par le biais des autorités de contrôle, des points de contrôle de traitement des données qui circulent. Le RGPD s'inscrit dans la volonté du législateur européen de mettre en oeuvre ce contrôle de manière effective. Les mécanismes du guichet unique et du contrôle de la cohérence du RGPD sont un exemple de la légalisation et de l'institutionnalisation du contrôle en droit international. La multiplication des autorités de contrôle dans l'UE justifient la formalisation de leurs compétences, et de leurs interactions dans le cadre d'un fonctionnement en réseau afin d'assurer une cohérence de leurs décisions et de contribuer à la sécurité juridique de la zone de libre circulation des données personnelles au sein de l'Union.

Certains auteurs comme Bergé et Grumbach, considèrent, que le critère de rattachement au lieu de localisation stable de la personne (lieu de résidence) constitue un bouleversement au niveau juridique. Ils considèrent, que « l'abandon d'un critère de stricte territorialité et son remplacement par un critère fondé sur la localisation stable de la personne confèrent á ce dernier un statut de siège d'un nouveau territoire d'accès á un contenu en ligne ». Cet abandon traduit l'idée « qu'il existe un territoire numérique, pour une opération déterminée, soumis á un seul régime juridique ». 2164

L'effectivité de ces points de contrôle dépend de la capacité de l'Union européenne à en assurer la prévalence sur les ordres publics des États tiers [1780]. En effet, comme on l'a vu, en particulier à travers le cas du « Cloud Act », l'ingérence des autorités publiques des puissances étrangères dans les données personnelles protégées par le RGPD constitue une limite considérable à l'application étendue et harmonieuse du texte, notamment via le jeu des clauses contractuelles types adoptées par les sous-traitants à travers le monde. 2165

Ainsi, il serait dans l'intérêt de l'Union d'adopter via des conventions internationales, des mesures permettant d'assurer une prééminence réelle de la règle européenne en matière de protection des données sur les ordres publics étrangers. 2166

1780. Deroudille / Fatah, *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »*, p. 442.

§4 La mise en oeuvre effective de l'extraterritorialité du RGPD

2167 L'application extraterritoriale par l'auteur de la législation doit être distinguée de son effet extraterritorial en territoire étranger. L'application extraterritoriale concerne la compétence de l'UE à faire exécuter des actes ou à contrôler des activités en territoire étranger. Il s'agit dans le cas de l'application du RGPD de la reconnaissance de la compétence de l'autorité de contrôle chef de file pour trancher des litiges, en application du principe de la loi du pays d'origine (art. 56 RGPD). L'effet extraterritorial concerne la capacité de l'État tiers à donner effet sur son territoire à la législation extraterritoriale de l'Union européenne [1781]. Cet effet extraterritorial donne toute son efficacité à la norme extraterritoriale et dépend de la seule volonté de l'État étranger d'admettre l'application de la loi étrangère sur son territoire. Chaque État reste en effet souverain pour reconnaître l'effet d'un acte pris par un État étranger [1782].

2168 La mise en oeuvre effective des décisions administratives ou judiciaires et des sanctions du RGPD dans les pays tiers dépend cependant des normes de droit international public et de droit international privé. En théorie, tout État tiers à l'UE, peut manifester son opposition politique et juridique à l'application extraterritoriale d'un droit étranger. La question est de savoir dans quelle mesure les autorités de l'État tiers peuvent juger au regard du droit international public, la validité des actes de l'Union cherchant à appliquer extraterritorialement son droit européen comme le ferait un État. Dans les contentieux internationaux, l'application du droit international privé joue également un rôle central dans la mise en oeuvre effective des dispositions extra-territoriales d'un droit étranger. Les deux perspectives vont être examinées ci-après.

2169 Si l'UE détient une compétence normative pour élaborer des normes par les organes législatifs ou executifs, la question se pose de savoir si elle détient une compétence pour prendre des mesures d'exécution dans un État tiers, c'est-à-dire pour accomplir des actes matériels d'instruction, pour sanctionner et imposer des amendes. La compétence d'exécution est le pouvoir de mettre en oeuvre une norme de droit par des actes matériels d'exécution, impliquant si

1781. Decaux Emmanuel, *L'application extraterritoriale du droit économique, Cahiers du CEDIN*, 3e éd., Paris 1987, pp. 158-159.

1782. *Idem*, p. 87.

besoin la mise en oeuvre de la contrainte de la puissance publique [1783] (*Jurisdiction to prescribe and Jurisdiction to renforce* aux États-Unis). Selon un principe de droit international coutumier, dont l'objet est de protéger la souveraineté et l'indépendance des États et d'éviter tout conflit de souveraineté entre eux, il est interdit à un État d'exercer sa compétence d'exécution sur le territoire d'un autre État [1784]. Par conséquent, comme la Suisse ne fait pas partie de l'UE, le RGPD ne s'applique pas directement dans l'ordre interne suisse.

§5 Une mise en oeuvre effective á confirmer

En droit international public, le principe de territorialité régit les contentieux entre États. Les dispositions de droit public de la loi suisse sur la protection des données ne sont applicables qu'au traitement des données en Suisse. 2170

Historiquement, la Cour de Justice des Communautés européennes a adopté une approche stricte du principe de territorialité. Ainsi, sa jurisprudence se fonde sur la théorie de l'unité économique [1785]. La localisation du comportement illicite sur le territoire de l'Union (par exemple par le biais d'une filiale d'une entreprise suisse sur le territoire de l'Union) suffit pour donner compétence à un État membre de l'Union. De manière analogue, le RGPD reprend cette théorie en soumettant aux dispositions du RGPD les filiales d'un groupe étranger établi dans l'Union peu importe le lieu du traitement de données. 2171

Le RGPD harmonise les législations sur le territoire de l'UE pour éviter des divergences d'interprétation comme ce fut le cas de la Directive 46/95/CE. Que dire de sa nature juridique ? Doit-elle être reconnue par les États tiers ? Le législateur européen, le juge européen et la sanction européenne sont-ils légitimes dans les États tiers, comme en Suisse, en-dehors de l'UE ? 2172

La jurisprudence a étendu le champ d'application territorial des dispositions de droit public aux situations internationales au moyen 2173

1783. Decaux, *L'application extraterritoriale du droit économique*, p. 157.
1784. Arrêt de la Cour permanente de justice internationale du 7 novembre 1927, *Lotus, Recueil des arrêts*, Série A, n° 10, Arrêt 9, 1927, p. 4 ss.
1785. Jennings Robert Y., *Extraterritorial Jurisdiction and the United States Antitrust Laws*, in : British Yearbook of International Law 1957/33, p. 164.

du principe des effets [1786].

2174 Le tribunal fédéral suisse retient [1787] que l'effet normatif peut également être conçu pour l'action étrangère. Sous réserve des obligations découlant du droit international, une norme étrangère n'est prise en compte par un autre État que volontairement ou sur la base d'une collision ou d'une norme de référence correspondante dans son propre droit. Toutefois, le principe de territorialité, c'est-à-dire la limitation de l'applicabilité des normes à un territoire, limite les conséquences de la législation nationale ayant des effets au-delà du territoire national. Du fait des interdépendances internationales - en particulier dans la vie économique - les possibilités d'application transfrontalière (succursales, filiales, etc.) sont cependant de plus en plus courante.

2175 Le droit international a apporté des clarifications dans certains domaines spécifiques comme le droit fiscal international ou l'entraide judiciaire internationale [1788]. Le droit international coutumier consacre la liberté générale d'action des différents États, comme le confirme l'arrêt « Lotus » de la Cour internationale de justice de 1927 [1789].

2176 La doctrine a encouragé cette liberté d'action des États, sur le fondement de l'interdiction d'ingérence, sur le principe d'égalité souveraine entre États, de l'interdiction de l'abus de droit et des principes de bonne foi et de courtoisie internationale. Ainsi les effets extraterritoriaux ne devraient être autorisés que dans la mesure où ils ne sont pas interdits par le droit international et où il existe un

1786. Bär Rolf, *Das Auswirkungsprinzip im schweizerischen und europäischen Wettbewerbsrecht*, in : Neue schweizerische Wettbewerbsordnung im internationalen Umfeld, Berner Tage für die juristische Praxis 1997, p. 1327 ss.

1787. Arrêt du Tribunal Fédéral du 7 au 10 Novembre 2002, XIII. « Treffen der obersten Verwaltungsgerichtshöfe Österreichs, Deutschlands, des Fürstentums Liechtenstein und der Schweiz ».

1788. Locher Peter (édit.), *Kommentar zum DBG : Bundesgesetz über die direkte Bundessteuer*, 1e éd., Basel 2001, p. 63 ss ; Arnold Martin / Meier Alfred / Spinnler Peter, *Steuerpflicht bei Auslandbezug*, in : Uebersax Peter (édit.), *Ausländerrecht : Ausländerinnen und Ausländer im öffentlichen Recht, Privatrecht, Strafrecht, Steuerrecht und Sozialrecht der Schweiz*, 1e éd., Basel 2002, consid. 17.1 ss ; Breitenmoser Stephan, *Internationale Amts- und Rechtshilfe*, in : Uebersax Peter (édit.), *Ausländerrecht : Ausländerinnen und Ausländer im öffentlichen Recht, Privatrecht, Strafrecht, Steuerrecht und Sozialrecht der Schweiz*, 1e éd., Basel 2002, consid. 20.1-20.32.

1789. A l'époque, la Cour avait jugé, que les autorités turques étaient compétentes pour poursuivre un officier français qui avait éperonné un navire à vapeur turc avec son bateau postal.

facteur de rattachement suffisant et prédominant [1790].

La question reste ouverte de savoir si ces principes sont intégrés dans le droit international coutumier en tant que délimitation juridictionnelle. 2177

La théorie des effets examine l'impact d'une réglementation sur un territoire aux normes spécifiques. Elle contribue à garantir l'efficacité de la réglementation, en appliquant à toute personne la même norme sur un marché. Cette théorie s'applique en droit de la concurrence, quel que soit le pays d'origine ou le lieu de résidence de la personne concernée. Le RGPD s'inspire de cette théorie en imposant un niveau de protection des données élevé sur un territoire, en lien avec la situation géographique de la personne physique ou avec son ciblage sur le territoire de l'UE, indépendamment de sa nationalité. 2178

Le droit suisse reconnaît la théorie des effets [1791]. En cas de conflit de juridictions, le problème doit être résolu par des accords internationaux (ATF 127 III 219 E. 219 E. 4c p. 227). 2179

La question de l'applicabilité du droit étranger impératif dépendra en grande partie du juge qui est appelé à statuer [1792]. Dans sa décision Bancovic [1793], le juge européen a confirmé son ralliement à la théorie des compétences consacrée en droit international en soulignant que « du point de vue du droit international public, la compétence juridictionnelle d'un État est principalement territoriale ». 2180

1790. Bär Rolf, *Extraterritoriale Wirkung von Gesetzen*, in : Schweizerische Rechtsordnung in ihren internationalen Bezügen : Festgabe zum schweizerischen Juristentag 1988, dargeboten von der juristischen Abteilung der Rechts- und Wirtschaftswissenschaftlichen Fakultät der Universität Bern 1988, p. 12 ss.

1791. Arrêt du TF de 1967, *Hachette SA*, ATF 93 II 192 ss ; Arrêt TF du 24 avril 2001, *Département fédéral de l'économie publique contre Commission de recours pour les questions de concurrence, ainsi que Rhône-Poulenc SA et Merck & Co. Inc.*, ATF 127 III 219 ss.

1792. Bizzozero Alessandro / Robinson Christopher, *Activités financières cross-border vers et depuis la Suisse*, 1e éd., Bulle 2010, p. 208.

1793. Arrêt CourEDH du 12 décembre 2001, *Bancovic et autres c. la Belgique, la République tchèque, le Danemark, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Italie, le Luxembourg, les Pays-Bas, la Norvège, la Pologne, le Portugal, l'Espagne, la Turquie et le Royaume-Uni*, n° 55207/99, consid. 59, obs. Cohen-Jonathan, *La territorialisation de la juridiction de la Cour européenne des droits de l'homme*, p. 1055 ; chron. Weckel (Ph.), RGDIP, 2002, p. 438 ; Sudre (F.), JCP G, 16 janvier 2002, I 105 et Flauss (J-F.), AJDA, 2002, p. 501. De manière plus générale, voir obs. Sudre (F.), in : GACEDH, n° 68, p. 731.

Il s'agit du pouvoir d'entendre une affaire, lorsqu'un tribunal a par exemple compétence sur un litige donné.

2181 A ce jour, en cas de conflit de lois, l'État victime peut se référer aux règles d'application territoriale du droit et contester ses effets extraterritoriaux sur la base d'autres règles de droit comme la Constitution, et les règles de courtoisie internationale [1794]. La question se pose de savoir si la reconnaissance d'un principe de courtoisie internationale « raisonnable », en tant que droit positif de l'Union européenne, reconnu par le législateur, afin de rééquilibrer les rapports de force entre États et limiter « un abus de droit » dans l'exercice de sa compétence extraterritoriale d'exécution pourrait constituer une solution durable et pacifique aux conflits de lois dans le domaine de la protection des données.

2182 La reconnaissance du principe de courtoisie internationale raisonnable renvoie à la théorie de la balance des intérêts étatiques [1795].

2183 Un État pourrait également alléguer le principe de la bonne foi [1796]. Ce principe est reconnu lorsqu'un État adopte dans l'exercice de sa compétence une attitude de modération et de retenue [1797]. Enfin, un État pourra invoquer la doctrine du respect mutuel résoudre un conflit de lois. Dans cette hypothèse, le RGPD doit être effectivement appliqué et il faudra démontrer qu'il existe un risque concret de condamnation pour les entreprises se trouvant en situation de conflit de lois. Cela signifie que l'État qui souhaite s'opposer à l'application du Cloud Act sur le fondement de la doctrine du respect mutuel a tout intérêt à pouvoir démontrer l'application préalable du RGPD.

I. Droit international privé

2184 Au sein de l'Union, le RGPD reconnaît le principe de la loi du pays d'origine (art. 56 RGPD), qui donne compétence à une autorité de contrôle chef de file pour trancher des litiges.

2185 En dépit des sanctions prévues par le règlement en cas de viola-

1794. Dodge William S., *International Comity in American Law*, in : Columbia Law Review 2015 115/8, pp. 2071-2141.
1795. Friedel-Souchu, *Extraterritorialité du droit de la concurrence aux Etats-Unis et dans la Communauté européenne*, p. 46.
1796. *Ibidem.*
1797. *Ibidem.*

tion de l'une des dispositions précitées, l'effectivité réelle du RGPD pour les États tiers à l'Union, est problématique et semble être aussi fonction des rapports de force entre grandes puissances.

En cas de contentieux international, le juge suisse doit déterminer le tribunal compétent et la loi applicable. Il sera donc parfois amené à appliquer le droit suisse ou le droit européen, potentiellement le RGPD. Le questionnement débute par une réflexion au niveau du droit international privé et est suivie d'un raisonnement sur le fond au niveau du droit matériel. 2186

A. Compétence du juge

En application du droit international privé suisse, le juge appliquera en premier les dispositions des conventions internationales ratifiées par la Suisse et subsidiairement, les règles de la LDIP [1798]. Il s'agit des règles de conflit du for. 2187

En pratique, le juge suisse sera uniquement compétent au titre de sa compétence internationale, si une règle de compétence d'une convention internationale ratifiée par la Suisse (ex : Convention de Lugano) ou issue de la LDIP (art. 19 ou 120 LDIP) le déclare compétent. 2188

L'action devra être intentée dans un autre État si aucune règle de conflit de juridiction helvétique n'ouvre un for en Suisse. 2189

Le juge va vérifier s'il est compétent en application des règles de conflit de juridiction (LDIP ou convention ratifiée par la Suisse). S'il n'est pas compétent (ratione loci) il se désaisira de l'affaire. Puisque le RGPD ne tient pas compte de la localisation des traitements, la présence des centres de données en Suisse ne suffira pas pour donner compétence au juge suisse. Le requérant saisira alors le juge situé dans l'UE pour trancher le litige. Le juge européen appliquera ses propres règles de conflit de juridictions, pour déterminer sa compétence. 2190

En pratique, le juge suisse sera uniquement compétent au titre de sa compétence internationale, si une règle de compétence d'une convention internationale ratifiée par la Suisse (ex : Convention de Lugano) ou issue de la LDIP (art. 19 ou 120 LDIP) le déclare 2191

1798. Guillaume, *Droit international privé*, p. 34.

compétent.

2192 Si le juge suisse est compétent au niveau du lieu, cela ne signifie pas qu'il soit compétent au niveau matériel (droit cantonal). En application des règles de conflit de loi, il déterminera le droit applicable [1799], en fonction des règles de la Loi fédérale sur le droit international privé (LDIP, R.S 201).

B. Droit applicable

2193 La question se pose de savoir si le RGPD pourra être invoqué devant le juge étranger du fait de son caractère extraterritorial. Pour Corinne Thiérache, le RGPD pourra être invoqué devant le juge américain «afin de justifier une requête en modification ou en annulation de la demande des autorités américaines en application du Cloud Act. Notons que les mécanismes de l'art. 45 RGPD en lien avec les transferts internationaux ne sont pas applicables aux entités gouvernementales américaines et qu'en ce sens il n'existe pas de décision d'adéquation entre l'UE et les USA, le Privacy Shield n'étant applicable qu'aux sociétés commerciales enregistrées dans le cadre du programme Privacy Shield. Le RGPD encadre en effet les transferts internationaux. La licéité du transfert de données personnelles vers les pays tiers est soumises à des conditions strictes (art. 46-48 RGPD).

2194 En pratique, les juridictions des États membres seront systématiquement compétentes dès lors que les conditions de l'art. 3, al. 2 RGPD sont remplies. En effet, le législateur européen impose aux responsables du traitement et aux sous-traitants établis dans des pays tiers de désigner par écrit un représentant dans l'UE. Ce représentant donne une compétence territoriale à l'État sur lequel se situe le représentant, pour traiter du litige et donc appliquer en pratique le RGPD. Il sera le point de contact pour les autorités de contrôle des données personnelles (article 27 du RGPD). Cette obligation de désigner un représentant sur le territoire de l'UE revêt une importance pratique considérable. Elle accroît ainsi le rôle des autorités de protection des données des États membres de l'Union et des tribunaux dans le cadre des actions en responsabilité (art. 82 RGPD), en limitant l'insécurité juridique résultant de l'application des règles de conflits de lois et de juridictions. L'obligation pour le responsable du traitement ou le sous-traitant de désigner un repré-

1799. Guillaume, *Droit international privé*, p. 33 ss.

sentant sur le territoire de l'Union participe d'une protection effective de la personne concernée, dont les données sont traitées. En effet, le RGPD offre un cadre juridique extrêmement protecteur de la personne, en lui octroyant des droits renforcés, en comparaison d'autres systèmes juridiques.

Lorsqu'une décision a été rendue, les règles d'exequatur et de reconnaissance s'appliqueront pour voir si la décision peut déployer ses effets. Cependant, le RGPD crée un risque au niveau de l'autorité de la chose jugée. En effet, il sera possible d'introduire une réclamation (recours administratif) auprès d'une autorité de contrôle et dans le même temps de saisir la justice pour une même affaire. Ce parallélisme pourrait poser de nombreux problème, quant à l'autorité de la chose jugée et à l'application du principe non bis in idem [1800]. Il appartient aux règles de droit matériel nationales de donner la solution au fond. 2195

§6 Conclusion

En présence d'un phénomène de déterritorialisation du droit et d'une interdépendance économique des États, la question se pose de savoir si un droit mondial de protection des données, sur la base de la Convention 108 du Conseil de l'Europe ne serait pas la solution la plus pertinente pour garantir un niveau élevé de protection des données aux personnes privées sur le plan mondial. De manière analogue au droit de la concurrence [1801], l'initiative d'un code mondial du droit de la protection des données, harmonisant les droits nationaux de la protection des données serait une solution idéale aux conflits de juridictions résultant de l'application du droit de la protection des données. Bien que théoriquement cohérente, cette proposition apparaît aujourd'hui peu réaliste tant les conceptions sur la nature de la donnée (bien marchand ou attribut de la personnalité protégé en tant que droit fondamental) varient d'un État à l'autre. 2196

La Cour de Justice de l'UE, donne, quant à elle, la priorité à la protection juridictionnelle effective [1802], comme le Règlement euro- 2197

1800. Conseil de l'UE, *Décision 7920/16 du 14 avril 2016*, p. 7.
1801. Anderson Timothy L., *Extraterritorial Application of National Antitrust Laws : The Need for More Uniform Regulation*, in : Wayne Law Review 1991/38, p. 1579 ss.
1802. Arrêt CJUE du 17 novembre 2011, *Hypotecni Banka a.s. contre Udo Mike Lind-*

péen. La CJUE a formellement reconnu ce principe d'une protection juridictionnelle effective dans sa jurisprudence [1803].

2198 Dans les affaires Google Spain et Amazon [1804], la CJUE, s'est fondée sur la nécessaire protection effective et complète des droits et libertés fondamentales des personnes physiques, pour donner une interprétation large du critère d'application spatial de la protection européenne des données personnelles, en-dehors de l'Union. Elle conclut á l'applicabilité de la protection européenne, même si le traitement se fait en-dehors de l'UE, dès lors qu'il existe dans l'Union une succursale dont la mission est de promouvoir et de vendre des espaces publicitaires (Google Spain), ou un représentant du responsable du traitement localement chargé du recouvrement de créances (Weltimmo). En revanche, la seule accessibilité d'un site web sur le territoire d'un État membre ne rend pas sa loi applicable (Amazon). Le RGPD intègre désormais ces solutions.

2199 Le tribunal fédéral a confirmé dans son arrêt Google Street View que la LPD était applicable si « un lien étroit avec la Suisse » existait. Dans cette situation, le Préposé fédéral est « compétent pour déterminer s'il y a atteinte à la personnalité au sens de l'art. 28 CC. Dans cet arrêt, le tribunal a retenu qu'un tel lien existait lorsque des données sont collectées, en Suisse, sur des personnes, des rues ou des endroits et que ces données, une fois publiées, sont accessibles depuis la Suisse. De même, la publication de ces données sur Internet depuis l'étranger, et non directement depuis la Suisse, est également susceptible de constituer une atteinte à la personnalité en Suisse ». La personne concernée est libre de choisir la juridiction de son choix en application de l'art. 139, al. 3 par. 1 LDIP. Les tribunaux suisses sont compétents si le requérant dispose de son domicile habituel en suisse.

ner, C-327/10, ECLI :EU :C :2011 :745, consid. 53 ; Arrêt CJUE du 11 sept. 2014, *A contre B e.a.*, C-112/13, ECLI :EU :C :2014 :2195, consid. 50. Voir aussi art. 47 Charte des droits fondamentaux de l'UE.

1803. Arrêt CJUE du 11 sept. 2014, *A contre B e.a.*, C-112/13, ECLI :EU :C :2014 :2195, consid. 50.

1804. Arrêt CJUE du 1 octobre 2015, *Weltimmo*, C-230/14, ECLI :EU :C :2015 :639, consid. 54, D. 2016, p. 1045, obs. H. Gaudemett-Tallon ; CJUE, 28 juillet 2016, JurisData 2016-016129, consid. 78.

Conclusion

La présente thèse a tenté d'exposer le caractère central du contrôle a posteriori, et en particulier d'une action civile en responsabilité fonctionnant bien pour garantir l'effectivité de la protection des données et la libre circulation des données á caractère personnel dans l'UE. Une action civile effective constitue la clé de voûte du système sur lequel repose le Règlement général sur la protection des données. Bien qu'ayant adopté une perspective large, notre thèse ne pouvait prétendre à l'exhaustivité. Plusieurs enseignements peuvent être tirés de l'analyse de ce nouveau texte. 2200

§1 L'effectivité de la protection des données : un enjeu majeur à l'ère digitale

Au terme de cette étude sur la protection des données, il ressort que la mise en œuvre du droit de la protection des données dépend de la facilité d'accès à l'action en responsabilité civile et en réparation du dommage pour les personnes lésées par une violation du droit de la protection des données. 2201

Historiquement, le droit européen de la protection des données est mis en œuvre presque exclusivement par le mécanisme de Public Enforcement des autorités de protection des données. En Suisse, le Préposé fédéral à la protection des données est le garant de la mise en œuvre de la protection des données à caractère personnel et de l'État de droit. 2202

La thèse s'est intéressée á la généralisation du contrôle a posteriori par le Règlement, avec transformation des autorités de protection des données personnelles en autorité de contrôle a posteriori. Ce changement externe et visible correspond à une transformation profonde de la nature du droit de la protection des données personnelles, tel qu'il est mis en place comme droit positif européen par le Règlement : ce droit positif européen de la protection des données personnelles devient un droit de nature essentiellement économique, comme le droit antitrust, qu'il complète désormais. Ce droit approche en effet la circulation des données personnelles dans le même esprit que le droit de la concurrence approche la libre 2203

circulation des personnes, des capitaux, des marchandises, etc. Cependant, si le droit antitrust se concentre sur le coût trop élevé des ententes illicites (en terme de prix des services ou des marchandises, en raison de certaines pratiques critiquables comme les pratiques cartellaires, par exemple), le droit de la protection des données se concentre quant á lui, sur le coût trop élevé (en terme d'atteinte à la sphère privée) de certaines pratiques des responsables de traitement (toutes celles qui ne sont pas conformes au Règlement).

2204 Ce changement dans la nature du droit de la protection des données correspond á une tentative de ré-équilibrage des rapports de force entre les acteurs économiques et les personnes concernées par les traitements de données personnelles. L'essor des technologies digitales (intelligence artificielle, machine Learning, Blockchain, robotique, bioingénierie...) fondées sur le traitement des données á caractère personnel et les enjeux stratégiques et financiers de l'économie fondée sur les traitements de données, rendent essentiel le recours au contrôle a posteriori, et en particulier á une action civile effective.

2205 Le droit positif de la protection des données mis en place au niveau européen poursuit, selon le Règlement, de façon égale deux buts distincts. En soi concurrents entre eux et dans une certaine mesure incompatibles, le Règlement les met expressément au même niveau. Le droit de la protection des données personnelles n'est plus construit sur la priorité de la protection de la sphère privée. La libre circulation des données personnelles, c'est-à-dire le principe de la liberté de traitement par le responsable de traitement, est placée au même niveau que le principe de la protection des personnes. En refusant expressément d'établir une hiérarchie entre eux mais au contraire en montrant bien la volonté du législateur de les placer au même niveau, cela donne une place de choix á l'action civile en responsabilité á l'encontre des acteurs économiques.

2206 Le problème majeur pour la Suisse est d'adapter sa législation au Règlement à l'avenir, et de continuer ainsi à bénéficier de la décision d'adéquation octroyée par la Commission européenne. Selon nous, les deux buts du Règlement ne peuvent être mis au même niveau et poursuivis ensemble que par la mise en place d'un contrôle a posteriori, seul moyen d'assurer une réelle libre circulation des données. Ce contrôle a posteriori doit offrir des garanties de sa

réelle effectivité.

Selon le Règlement, cela signifie que le contrôle mis en place, exige des États de l'Union : 2207

— que les personnes physiques aient certes le droit d'introduire une réclamation auprès des autorités de contrôle contre le responsable du traitement (art. 77 RGPD), ce qui n'a rien d'exceptionnel, mais également, qu'il y ait mise en place du droit à un recours juridictionnel effectif contre les décisions des autorités de contrôle. Celles-ci doivent pouvoir condamner les responsables de traitements à des amendes administratives calculées sur la base du chiffre d'affaire du groupe concerné, donc sur des montants qui peuvent représenter un multiple des bénéfices réalisés, et aussi un multiple des fonds propres et des réserves de ces groupes (art. 79 RGPD et art. 83 RGPD).

— que les personnes physiques aient non seulement un droit à la réparation du préjudice du fait d'une violation du Règlement par le responsable du traitement (art. 82 et 24, qui prévoient le renversement du fardeau de la preuve, le responsable devant désormais prouver que son comportement est conforme au règlement), mais aussi, en plus, qu'il y ait mise en place de ce qui doit représenter « un recours juridictionnel effectif » (art. 79 RGPD) pour attaquer les responsables de traitement (cela comprend en particulier, selon l'art. 80 du Règlement, la possibilité de class actions).

— que les autorités de contrôle nationales puissent sanctionner les violations du Règlement par des sanctions administratives dissuasives. Les décisions de l'autorité britannique de sanctionner British Airways pour un montant de plus de 183 millions de pounds en juillet 2019 et de 123 millions de Pounds pour la chaîne d'hôtels Marriott démontrent la volonté politique des autorités de contrôle d'appliquer le Règlement. Cependant, le montant de ces amendes doit être relativisé. En juillet 2019, la Federal Trade Commission américaine a infligé une amende de 5 milliards au groupe Facebook. Celle-ci représente l'équivalent d'un mois de revenus pour ce groupe. Par conséquent, l'action du groupe a vu sa valeur augmenter après l'annonce de l'amende. Cette amende n'a donc eu aucun impact sur les prévisions de croissance future du groupe. En 15 minutes, la valeur de marché de l'action Facebook a

gagné 5 milliards de dollars, soit le montant de l'amende [1805]. Comment ré-équilibrer les rapports de force ? Le droit de la concurrence pourrait constituer la solution, non pas seulement du fait de la possibilité de démantèlement du groupe mais aussi du fait des possibilité de Private Enforcement offertes par le droit de la concurrence. Une évolution du droit de la concurrence pour renforcer la protection des données est en cours d'examen aux USA [1806].

2208 Le contrôle a posteriori des autorités de contrôle va faciliter, avec l'action civile en responsabilité, la prise de conscience et l'acceptation pour les acteurs économiques, que le but de la protection des données est la protection des personnes et le corollaire du principe de liberté, pilier du monde digital [1807]. Cette protection des personnes est rendue possible par l'action civile en responsabilité offerte par le Règlement (voir paragraphe 1294), en plus du contrôle a posteriori effectué par les autorités de contrôle.

2209 Le Règlement prévoit l'obligation pour les Etats membres de l'Union de mettre en place un recours juridictionnel effectif contre les responsables de traitement. Faisant référence au droit américain et européen de la concurrence, cette thèse a analysé le concept de Private Enforcement qui s'est imposé en droit de la concurrence, dans la partie consacrée au développement du droit de la protection des données en Suisse. Son but est d'expliquer que les modifications du droit sont nettement insuffisantes, si l'on prend la mesure de ce que met en place le Règlement. La mise en place d'une véritable class action dans le domaine de l'action civile des personnes physique contre les responsables de traitement est particulièrement importante, dès que l'on voit l'importance pour les consommateurs et les personnes physiques d'avoir en main un instrument qui ne dépend pas de décisions publiques et donc de considérations politiques, mais seulement des tribunaux civils. C'est pourquoi une telle action civile est la clé de voûte qui permet au système de la mise á

1805. Patel Nilay, *Facebook's $5 billion FTC fine is an embarrassing joke*, in : The Verge (https ://www.theverge.com/), Washington D.C. 2019, p. « https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke » (06/08/2019).

1806. Editorial Board, *US Department of Justice must make antitrust fit for the age of Big Tech.*

1807. Frison-Roche, *L'apport du Droit de la Compliance dans la Gouvernance d'Internet, rapport demandé par le Gouvernement.*

égalité des deux buts du Règlement d'exister.

Avec l'entrée en vigueur du Règlement, le volet civil du droit de la protection des données est amené á se développer. En particulier, l'action civile sur la base d'une action collective en droit de la protection des données dans l'UE, qui est prévue par le Règlement (art. 80 RGPD). La Suisse, quant á elle, a initié la révision du code de procédure civile, afin d'introduire la possibilité d'une action collective en droit suisse, pour faciliter les actions en réparation du dommage. 2210

Le Règlement européen devient progressivement un standard au niveau mondial. Plusieurs pays, comme le Japon, la Corée du Sud, les États-Unis ou la Suisse sont en train de réviser leur droit sur la protection des données ou de négocier une décision d'adéquation avec l'UE. Ces réformes ont pour objectif de remplir les deux buts du Règlements. Le Règlement incarne ainsi « un nouvel âge de l'action publique [1808] ». 2211

Reste á déterminer dans quelle mesure un système de Private Enforcement à l'américaine pourrait être la source d'un véritable progrès, favorisant dans le même temps innovation technologique et valeurs démocratiques. 2212

1808. Algan Yann / Cazenave Thomas, *L'État en mode start-up*, 1e éd., Paris 2016, p. 30.

Annexe : Les éléments principaux de mise en conformité au RGPD pour les entreprises suisses

Voir synthèse en anglais sur ce sujet de Charlet François, *GDPR in Switzerland : 10 steps organizations should take* [1809]. 2213

§1 Identifier les traitements de données à caractère personnel et les flux de données

Il s'agit d'identifier, de documenter et de maintenir à jour les traitements de données, et de créer un registre des traitements mentionnant les caractéristiques principales des données (origine, type de traitement, finalité, caractère sensible ou non, base légale du traitement, transferts éventuels et identité du destinataire). 2214

§2 Désigner un délégué à la protection des données (DPO)

Le DPO sera responsable de la mise en conformité de la protection des données, sauf si le traitement de données à caractère personnel est occasionnel, n'implique pas de traitement de données sensibles à grande échelle ou ne présente pas de risque pour les individus [1810]. Le rôle de DPO peut être rempli par un consultant externe. 2215

1809. Charlet François, *GDPR in Switzerland : 10 steps organizations should take*, in : François Charlet Blog (https://francoischarlet.ch/), Lausanne 2017, p. « https://francoischarlet.ch/2017/gdpr-in-switzerland-10-steps-to-take/ » (08/10/2017).

1810. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, pp. 1-30.

§3 Mettre à jour la déclaration relative à la vie privée (privacy notice)

2216 Chaque organisation traitant des données à caractère personnel doit revoir sa déclaration relative à la vie privée et la mettre en conformité avec le règlement avant le 25 mai 2018.

2217 Certaines informations doivent être communiquées : identité et coordonnées du responsable du traitement, et du DPO ou le représentant, finalités du traitement, et base légale du traitement, les intérêts légitimes du responsable du traitement ou des tiers (si nécessaire), les catégories de données, la période de conservation des données, les destinataires ou catégories de destinataires des données, détail des transferts vers des pays tiers et garanties offertes, les droits de la personne concernées notamment le droit d'accès et le droit de recours auprès d'une autorité nationale, le droit de retirer son consentement de tout temps, si nécessaire la provenance des données, l'existence de décisions prises sur une base automatisée.

2218 Ces informations doivent être communiquées dans un langage simple et clair. Une révision et mise en conformité des contrats avec les fournisseurs et les tiers est requise.

§4 Identifier la base légale de chaque traitement

2219 Le règlement impose au responsable du traitement de documenter cette base légale une fois identifiée (consentement, contrat, loi...).

2220 Les droits alloués aux personnes concernées varient en fonction de la base légale.

§5 Revoir la validité des consentements reçus

2221 Les conditions du consentement ont été renforcées [1811]. Le consentement doit être donné librement, doit être spécifique, informé et non ambigu. Il peut être retiré en tout temps. Il requiert une action de la personne concernée (opt-in). Ainsi le consentement ne peut

1811. Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, pp. 1-36.

pas être obtenu valablement sur la base du silence de la personne concernée ou d'une inaction.

Le responsable du traitement veillera en particulier aux points suivants : 2222

- Adéquation entre le traitement et la base légale.
- Le consentement au traitement des données à caractère personnel doit être recueilli de façon spécifique et non pas au moment de la signature des termes et conditions du contrat.
- Ne pas recueillir un consentement par défaut, ou un consentement sur la base d'une case pré-cochée.
- Vérifier l'âge des personnes concernées et demander le consentement parental si nécessaire.
- Revoir et réactualiser le consentement sur une base régulière.
- Documenter la date et la forme du consentement.

§6 Développer des procédures pour répondre aux requêtes des personnes concernées qui voudront exercer leurs droits

Le règlement renforce les droits des individus qui bénéficient depuis le 25 mai 2018 des droits suivants : droit d'accès, droit d'information, droit à l'effacement, droit à la rectification, droit de contestation, droit de restreindre le traitement, droit de ne pas être soumis à une décision prise uniquement sur une base automatisée, droit à la portabilité des données. 2223

L'organisation devra être prête à répondre aux demandes des personnes concernées (ex : exercice du droit d'accès, exercice du droit à l'oubli...). Cela suppose de développer des procédures internes spécifiques pour enregistrer et répondre à chaque requête dans le délai légal. Le droit à la portabilité des données ne s'applique qu'aux traitements de données effectués de manière automatisé sur la base du consentement de la personne concernée, ou dans le cadre de la mise en œuvre d'un contrat. 2224

§7 Protection des mineurs de moins de 16 ans

2225 Les données à caractère personnel de mineurs constituent des données sensibles, dont le traitement est protégé par le règlement. En particulier, si le traitement de données est effectué dans le cadre de la fourniture de services de la société de l'information (services sur Internet), alors le consentement parental est obligatoire sauf, si le mineur a 16 ans ou plus. L'âge doit donc être vérifié par le biais de mesures appropriées avant la collecte de données. Il importe enfin de souligner que le mineur doit pouvoir comprendre le contenu de la déclaration relative à la vie privée qui doit être rédigée en langage clair et simple.

§8 Procédure en cas de violation des données à caractère personnel

2226 Le règlement crée l'obligation générale de reporter une violation des données à caractère personnel non seulement aux autorités nationales compétentes (dans les 72h maximum) mais également aux individus dans des cas spécifiques. Cette notification est impérative dès lors qu'il existe un risque pour les droits et libertés des individus. Si ce risque est élevé, le responsable du traitement devra informer les personnes concernées directement en plus de l'autorité nationale compétente. Le critère du domicile de la personne concernée permet de déterminer l'autorité nationale compétente. Par exemple, si un vol de données personnelles survient en Suisse et concerne principalement des personnes domiciliées en Allemagne, l'autorité nationale allemande devra être notifiée de la violation de données par le responsable du traitement suisse, en application du RGPD.

2227 L'organisation devra mettre en place une procédure pour identifier les violations de données dans les meilleurs délais, reporter cette violation et procéder à une enquête pour comprendre l'origine, la nature de cette violation et l'ampleur de ses conséquences.

§9 Protection dès la conception et Protection par défaut

Le règlement exige la mise en œuvre de mesures techniques et organisationnelles pour protéger les données à caractère personnel. Parmi ces mesures de réduction des risques figurent la protection des données dès la conception et la protection par défaut. Ces mesures consistent notamment à minimiser le volume de données personnelles collectées et leur durée de conservation. La pseudonymisation des données personnelles constitue également une mesure technique de protection des données. 2228

Les finalités du traitement ainsi que le traitement lui-même doivent être transparents. La personne concernée jouera un rôle actif tout au long du traitement. Le règlement impose aux organisations de tenir compte de la protection des données dès la phase de conception des projets et de conserver cette problématique au cœur de l'organisation. La conformité aux normes ISO 27001, 27002 devrait être recherchée. 2229

§10 Analyse d'impact en matière de protection des données

Le responsable du traitement devra conduire une analyse d'impact en matière de protection des données pour évaluer l'origine, la nature, les spécificités et la sévérité du risque pour les droits et libertés des personnes physiques. 2230

Cette analyse d'impact est obligatoire pour le traitement de grande dimension de données sensibles (Big Data), ou avant le déploiement d'une nouvelle technologie, ou si une opération de profilage est susceptible d'affecter un nombre important de personnes d'une manière significative [1812]. 2231

1812. Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 - Adopted on 4 April 2017, Last Revised and Adopted on 4 October 2017 (WP 248 rev.01)*, in : European Commission (https ://ec.europa.eu/), Brussels 2017, p. « https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 » (05/04/2020), pp. 1-22.

Annexe : Repertoire alphabétique des matières

Les chiffres renvoient aux paragraphes.

A

Accès
- Abus de droit 1978ss
- Accès à la justice 1292,
- Accès à distance 1070
- Accès à un juge 1938
- Accès au marcé 2143
- Accès aux communications 2127
- Accès aux données 2120, 2121, 2123ss
- Accès au marché européen 552
- Accès illicite 1454
- Accès non autorisé 911, 944, 1258, 1267,
- Acteurs économiques 1338
- Action civile 1186
- Autorités publiques 1278, 1442, 1452, 1602, 1432, 1443, 1582, 1707, 1791, 1839
- Chiffrement 693
- CIP-CE 1773
- Class action 1960, 1966,
- Cloud Act 1164, 1173, 2095ss
- Conseil de l'Europe 1833
- Consentement 905
- Contexte 174
- DeepMind 426
- Délégué à la protection des données 1422
- Demandes d'accès 1395
- Disponibilité 1179
- Données 77, 1225
- Droit d'accès 159, 459, 495, 533, 1065, 1069ss, 1079ss, 1087ss, 1095, 1484,
- Droit de la concurrence 1922
- Droit économique 1919
- FATCA 2128
- Frein à l'accès 2107
- Garanties 638ss, 945, 1452, 1728, 1977ss, 2187,
- Intelligence artificielle 463ss, 469,
- LPD 657, 1983
- Limitation du traitement 1109
- Marché européen 998, 1751,
- NFC 472
- Objets connectés 345
- Paiement 476
- Personnes décédées 1800ss,
- Point d'accès 285
- Politique d'accès 1189
- Pouvoirs publics, 60, 158, 637,
- Privacy Shield 152, 155, 157
- Profilage 969
- Projet de réforme LPD 1839, 1844ss
- Protection juridictionnelle effective 1498
- PwC 1761
- Recours juridictionnel 1894
- Requêtes 2194
- Responsable du traitement 1785, 1793, 1888,
- Santé 201, 205, 825
- Sécurité 530, 1224, 1240
- SIS 999ss,
- Tiers 191, 477, 1063, 1983
- Transparence 1837
- UK Care Data programme 430
- Véhicules autonomes 241, 262, 275,

Accords bilatéraux
- Accords bilatéraux 978ss, 1003, 1005ss, 1171, 2059, 2091, 2100
- Analyse critique 2103, 2104, 2106ss
- Assistance mutuelle 2108
- Cloud Act 1173
- Entraide administrative 519

Accords Dublin
- Acquis de Dublin 983ss, 992, 1002, 1739

Accords Schengen
- Accords 983, 987,
- Accords bilatéraux 988
- Acquis de Schengen 992, 994, 1014, 1739, 1741, 1764, 1824
- Acquis communautaire 2100ss
- Coopération Schengen 1866
- Directive UE 2016/680 1826ss
- Evaluation Schengen 1752
- LPD 1750
- SIS 998

Analyse d'impact

- Analyse d'impact 624ss, 829, 976, 2200
- Analyse d'impact préalable 619, 622,
- Big Data 1360
- LPD 1837
- Mécanisme du contrôle de la cohérence 1709
- PwC 1761, 1923
- Responsables du traitement 1250ss, 1540,

Anonymisation

- Adresse IP 765
- Application du RGPD 399
- Big Data 764
- Droit à l'oubli 413
- Evolution législative 419
- Garantie 769, 917,
- Pseudonymisation 693
- Unicité 415, 762

B

Bancaire

- Cloud Act 2102
- Conformité 1335
- Contrôle a posteriori 1540
- Délégué à la protection des données 1194
- FATCA 2129
- FinTech 462ss,
- Jurisprudence CJUE 2020
- Licences 473
- Lobby 113

Bâtiments et villes intelligentes

- Général 210ss, 650, 1917,

Best Practices (bonnes pratiques)

- Général 1808

Big Data

- Analyse d'impact 2201
- Anonymisation 764
- Applications 182, 409, 699
- Autodétermination informationnelle 52
- Données non structurées 698
- Droit de la concurrence 1919
- Éléments 400ss
- Exactitude 654
- Innovations 178
- IoT 406
- Minimisation 936
- Modèles économiques 397
- OFCOM 179
- RGPD 1152
- Supercalculateurs 426

Bioéthique 450

Blockchain

- Action civile effective 2174
- Application 1161ss
- Consentement 405
- Contrats intelligents 358
- Convergence avec d'autres technologies 357
- Neutralité technologique 434
- Nouvelles technologies 183, 346ss
- Questions juridiques 361ss
- RGPD 692
- Sécurité 365
- Standards 364
- Traçabilité 360, 743
- Transaction financière 359
- Transferts 740

C

Capteurs

- Autonomie 302
- Domaine médical 191, 198
- Enjeu 207
- Objets 190
- Tableau de bord de santé personnalisé 202
- Véhicules autonomes 263
- Villes intelligentes 210ss

Champ d'application

- Accords bilatéraux 2091
- Analyse d'impact 1258
- Art. 3, al. 2 RGPD 2003ss,

- Anonymisation 1153
- Art. 22 RGPD 1149
- Assistance administrative 1684
- CEPD 2022
- Champ d'application extraterritorial 2040ss
- Ciblage 2029
- CIP-CN 1874
- Convention de Lugano 2099
- Décision d'adéquation 1439ss,
- Délégué à la protection des données 1391, 1840ss
- Directive UE 2016/680 1826
- Discriminations 971
- Données de santé 833
- Enregistrements 1885
- Droit français 2073
- Extraterritorialité 2045
- Garanties 1454
- Général 662, 695, 2010, 2118, 2146
- Jurisprudence 2171
- LPD 1738
- Matériel 674ss, 686, 688ss, 692, 694, 697, 700, 977, 1066
- Personnes décédées 1799
- Pseudonymisation 764
- RGPD 2027, 2028, 2133
- Territorial 702, 709
- TF 1978
- Transparence 1236

Charge de la preuve
- Utilisateur 331
- Responsable du traitement 764, 799, 803, 851
- Inversion 868, 882, 1119, 1173, 1542, 1813
- LPD 1821, 1884, 1896, 1957

Charte des droits fondamentaux de l'Union Européenne
- Arrêt Digital Rights 636
- Arrêt Schwartz 632ss.
- Art. 1 Charte 2053
- Art. 8 Charte 586ss, 640, 647, 714, 1536. 1543, 1548, 2002, 2029, 2044
- Art. 11 2116
- Art. 47 Charte 1497ss, 1501, 20146.
- Art. 52 628
- Art. 54 648
- Autorités de contrôle 2087
- Ciblage 2031
- Droit à un recours collectif 1646
- Droit fondamental 2066, 2068, 2153
- Droit international 3, 479
- Garanties 2048
- Général 503
- Jurisprudence CJUE 147
- LIBE 108
- Niveau de protection des données 1463, 2050
- Pondération des intérêts 626
- Principes 565
- Proportionalité 529, 599
- Régulation 437
- Wikileaks 164

Chiffrement
- Notification en cas de violation de données 1282

Cloud Computing
- Art. 3 RGPD 704, 726
- Banques 891
- Cloud Act 1171, 2021, 2059, 2074, 2119ss, 2123, 2125, 2127, 2129, 2131, 2132, 2139, 2142, 2148, 2173, 2181, 2191,
- Confiance 387
- Confidentialité 1171
- Conseil fédéral 1767
- Contrat 890
- Données sensibles 1915
- FinTech 356
- Général 365ss
- Localisation 2021
- Norme ISO 489ss
- Répartition des rôles 389
- Respect mutuel 2087
- Robots 304
- Sécurité 283
- Sécurité des Clouds 466
- Stockage de données personnelles 212
- Suisse 2073

- Technologies 183
- Transfert automatique 277ss

CNIL
- Amende Google 1187
- Astreinte 1606
- BCR 2046
- Contrôle administratif 2014
- Contrôle des transferts transfrontaliers 1651
- Droit au déréférencement 2114ss
- Ethique des algorithmes 431
- Global Privacy Enforcement Network 187
- Laboratoire données et design 1217
- Lignes directrices 268
- Privacy-by-Design 270
- Test de la balance des intérêts 915

Compagnies d'assurance (et assurances)
- Biens et services personnalisés 199
- Comportements du patient 201
- Données de santé 199
- Objets connectés 200ss,
- Prime 203ss
- Risque (individualisation du) 205

Compliance
- Droit de la compliance 1336
- FATCA 2128, 2142
- RGPD 95

Conformité
- Accès au marché européen 1749
- Action civile 1886
- Autorités de contrôle 1512, 1721, 1881
- Certification 1308, 1602, 1987
- Code de conduite 1851
- Conformité au RGPD 42, 47, 785, 804, 935, 1018, 1152
- Contrats fournisseurs 2193
- Conv. 108 1005, 1868
- Cybersecurity Act 257
- Déclaration relative à la vie privée 2191
- Délégué à la protection des données 1191ss, 1394, 1397, 1424, 2190
- Documentation 1182
- Droit fondamental 1540
- Droit international 2146
- Extraterritorialité 2138
- Jurisprudence CJUE
- LPD 989, 1006, 1884
- Norme ISO 489, 491, 2204
- Organisation 1190, 1347, 1602
- Politique de conformité 974, 1333
- Privacy Shield 1484, 2044
- Responsable du traitement 1193, 1538, 1794, 1951, 2040
- Safe Harbour 142
- Sécurité 945
- Sous-traitants 1022ss
- Web Scrapping 968

Conseil fédéral
- Actions de groupe 24
- Analyse d'impact 1921
- Class action 1964ss
- Code de procédure civile 1957ss
- Communications à l'étranger 1807ss
- Consultation LPD 1740
- Délégation pour la sécurité 170
- Droit international 2143
- Groupe minoritaire 1761
- LPD 660, 1767, 1855ss, 1864, 1870ss
- Mandat 1777
- Obligations 2145
- Préposé 1575, 1835, 1994
- Prise de position 1821
- Projet de révision 1750
- Projet de révision total de la loi sur la protection des données 539
- Protocole à la Convention 108 modernisée 1831
- Rapport du groupe d'accompagnement 1754

- Rapport sur l'évaluation de la LPD 1752
- RGPD 2040
- Responsabilité pénale 1853
- Secrets professionnels 1998

Consentement
- Age du consentement 2084, 2111,
- Blockchain 740
- Caractère exprès 1945
- Charge de la preuve 802
- Clarté 1854
- Class Action 1945ss
- CNIL 269
- Communication à l'étranger 655
- Consentement parental 2200
- Déclaration de consentement 2137
- Données sensibles 753
- Exceptions 808
- Helsana 754
- ISO 491
- Liberté du consentement 801
- Licéité du traitement 265, 278, 342, 1952, 2194ss
- LPD 653
- Métadonnées 414
- Notion 793ss
- Neutralité du Net 165
- Portabilité 2199
- Principes 1779
- Recueil 1952,
- Retrait du consentement 2192
- Validité 404, 1854, 2196ss

Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

- Adéquation 1831
- Arrêt Amann c. Suisse 508
- Art. 12 1582
- Assistance mutuelle 2108
- Autorités de contrôle 1535ss, 2088
- Consentement 1854
- Convention 108 modernisée 1507
- Droit fondamental 2068
- Droit mondial 2197
- Général 509ss, 520, 1881
- LPD 1735, 1774
- Préposé 1854
- Projet de révision 117
- Protocole 543, 989, 1005
- Rapport explicatif du Protocole additionnel à la Convention 108 1569, 2085
- Responsable du traitement 1781
- Valeur juridique contraignante 2066

Convention européenne des droits de l'homme
- Art. 8 49, 504
- Art. 13 1885
- LIBE 108

Corporate Social Responsibility
- Preuves 1168

Cour de Justice de l'Union Européenne (CJUE)
- Accès sans consentement 904
- Arrêt Schwartz 883
- Clauses contractuelles types 2047
- Contrôle ex ante 1039
- Droit à l'oubli 1035
- Droit communautaire 2183
- Effacement 1057
- Établissement 2018
- Décision d'adéquation 145, 1439ss
- Données 512
- Enregistrement 775
- Garanties 1449
- Google v. Spain 2003
- Intérêt légitime 806
- Invalidation 146, 1460, 1506
- Jurisprudence 120, 208, 1094, 1121, 1129, 1155, 1253, 1313, 1317, 1427, 1489, 1491, 1573ss, 1787, 1909, 1939, 2087, 2112ss
- Questions préjudicielles 143
- LRens 171

- Niveau de protection adéquat 147, 1461ss
- Notion d'établissement 705ss
- Nouveaux droits 1939
- Privacy Shield 1466
- Proportionalité 1206
- Recours 1487, 1858
- Recours en annulation 162
- Renvoi préjudiciel 1033
- Responsable du traitement 1036ss
- Responsables conjoints 774, 1321
- Safe Harbour 149, 152
- Schrems 1452
- Test de proportionalité 528
- Triplement des dommages 1906

Crise de confiance 164

Cryptomonnaie
- Notion 354, 360

D

Décisions automatisées
- Données sensibles 1156
- Ethique 1149
- Finalités 1087
- Fraude 1131
- Groupe de travail de l'Art. 29 1141
- Information 1784
- Licenciement 1127
- Notion 1123

Décision d'adéquation
- Absence 1226, 1464, 1502, 1530, 1532, 1811, 1855ss, 1946, 1956, 2046
- Annulation 1456
- CJUE 1439
- Clauses contractuelles types 1427
- Commission européenne 1376, 1436, 1437, 1454, 1458ss, 1764, 1871, 2002
- Conditions 1440
- Conv. 108 1864, 1881
- Entreprises suisses 1828
- LPD 372
- Pays 40, 2042, 2204, 2191, 2209
- PRISM 132
- Procédure d'adoption 1444
- Publication 1441
- Maintien 38, 989, 1005, 1742, 1743, 1749, 1768, 1780, 1861, 1868, 1970, 1971
- Obligations internationales 1448
- Privacy Shield 157, 1470, 1474
- Retrait 1008, 1015
- RGPD 2105, 2000
- Safe Harbor 143ss
- Transfert 40, 740, 1428, 1436, 1437, 1453

Délégué à la protection des données
- Agostino Valerio Placco 603
- Autorité de contrôle 1596
- Contribution financière 1597
- Désignation 42, 1328, 1340, 2190
- Gouvernance 947
- Notification 814
- Rôle 975, 1192

Démocratie 51, 214, 527

Destinataire
- Annexe 2189ss
- Autorité de contrôle 1713, 263
- Catégories de destinataires 1245
- Destinataires situés hors de l'Union 1427
- Droits de la personne concernée 1075, 1079, 1112
- État destinataire 1809
- Garanties 1811ss
- Information 1784
- Jurisprudence CJUE 1431
- Notion 550, 787ss
- Prévisibilité 897
- Protocole révisé de la Conv. 108
- Registre 1245
- Responsable du traitement 1030
- Service numérique 952
- TFUE 1723
- Transfert 1439, 1480

Digital Rights (Arrêt)

- Art. 7 Charte 595
- Garanties contre les abus 635
- Jurisprudence 528,
- Pouvoir d'appréciation 645
- Recours en annulation 162, 1487
- Stricte nécessité 628ss

Dilution de responsabilité
- Cloud 391
- Robots intelligents 315

Directive européenne sur la protection des données 95/46/CE
- Accords bilatéraux 2101
- Action civile 1934
- Arrêt Commission c.Hongrie 1579
- Art. 4 Directive 702
- Art. 7 Directive 794, 807, 864, 886
- Art 25, al. 6 Directive 1442
- Art. 28 Directive 1577
- Autorités de controôle 1574
- Champ d'application 566
- Charge de la preuve 1118
- Ciblage du citoyen 63, 561
- Clauses types 1526
- CJUE 2018, 2019
- Consentement 855
- Considérant 19
- Contrat 888
- Décision d'adéquation Privacy Shield 1470
- Décisions 1446
- Définitions 741
- Délégué à la protection des données 1342
- Dispositions extraterritoriales 2037
- Directive 836
- Directive 2002/58/CE 568
- Droit à l'oubli 1032
- Droit applicable 1618
- Établissement 2017
- Extraterritorialité 2003
- Garanties 531, 557
- Inconvenients 15, 560
- Libre circulation des données 1425
- LPD 1884
- Mise en oeuvre 2118
- Moyens de traitement 2032
- Notion 14, 559, 675, 678, 696
- Pays tiers 1437
- Pesée des intérêts 905
- Principes 850, 893, 1026
- RGPD 2001
- Sous-traitant 1020, 1432

Directive 2002/58/CE
- Commission européenne 562ss
- Droits de l'homme et libertés fondamentales 566
- Notification à l'autorité de contrôle 1263
- Rapport du comité LIBE 574
- Réforme 567ss

Directive (UE) 2016/680

- Eurodac 1002
- Garanties 1810
- LPD 1777
- SIS 1000
- Sous-traitant 1795
- Transposition 990

Discrimination
- Analyse d'impact 1258
- Analyses prédictives 407
- Assurances 825
- Ciblage 749
- Crédit 409
- Dommage 1282
- Données vocales 183
- Droits et libertés fondamentales 1507, 1872
- IA 970

Disponibilité
- Centres de données 377
- Disponibilité des données 426, 944
- Ethique 1923
- Mesures techniques 1176ss, 1783,

Doctrine de Schindler
- Notion 1004

Documentation
- Autorité de contrôle 1538
- Confiance 947, 1195
- Conformité 1182, 1190, 1952
- Consentement 885
- Décisions prises 1180
- Pseudonymisation 762

Dommage
- Auteur 21ss, 251
- Jurisprudence 252
- Objets connectés 184, 242
- Réparation des dommages 10, 16, 23, 71, 79
- Responsabilité 242
- U.K. Automated and Electric Vehicles Act 248ss
- Victimes 222

Données à caractère personnel
- Acteurs 1017
- Autorité de contrôle 841, 1552ss
- Capteurs 207
- Champ d'application matériel RGPD 673ss
- Champ d'application territorial RGPD 702ss, 719
- Charte des droits fondamentaux de l'UE 3, 502ss
- Comité européen à la protection des données 1703 ss
- Conclusion 2198ss
- Clauses contractuelles types 1526
- Clouds 211, 387ss
- Commission européenne 102 ss, 119ss, 122
- Consentement 404, 793ss, 855, 881ss
- Contexte technologique 173
- Conv. 108 508, 510ss, 539, 543ss
- Convention européenne des droits de l'homme 504
- Définitions 741ss
- Délégué à la protection des données 1420
- Dérogations 534, 637
- Destinataire 787, 1030
- Directive 95/46/CE 558ss
- Directive 2002 /58/CE 563
- Directive (UE) 2016/680 4
- Discours sur l'état de l'Union 576
- Données biométriques 826
- Données concernant la santé 830
- Droit à l'information 1074
- Droit à la portabilité 1092ss
- Droit à la rectification 1090
- Droit d'accès 1068
- Droit d'opposition 1113
- Droit de propriété 341
- Effacement 1033, 1046, 1053ss, 1057
- Entreprises 33
- Etablissement principal 833
- Extraterritorialité 63, 2025ss
- Fichier 769
- Flux 536, 1425
- Garanties 532, 628, 638, 2048
- Hiérarchie des normes 478
- Interactions avec les technologies 184
- Internet 565ss
- Jurisprudence CJUE 626, 631, 645ss, 1037, 1496, 1574, 1579
- Limitation des finalités 924 ss
- LPD 1783, 1822ss, 1835
- Marché 68 ss
- Mineurs 861ss
- Normes internationales 117
- Objection pertinente et motivée 846
- Objets connectés 184, 190ss
- Niveau de protection adéquat 132, 142ss
- Notification 1263
- Notion 31
- NSA 133
- OCDE 480
- Paiements 469
- Pictogrammes 159
- Principes 850, 938ss
- Privacy-by-Design 1203ss
- Privacy-by-Default 1219ss
- Privacy Shield 1468
- Profilage 757, 1122
- Pseudonymisation 1215
- PwC 1758

- Règles d'entreprises contraignantes 838, 1510
- RGPD 14, 36
- Représentant 783
- Retrait du consentement 872
- Responsable du traitement 772
- Responsabilité 121, 1165ss, 1293ss, 1335, 1887ss
- Robots 329
- Safe Harbour 138
- Sanctions 535
- Sécurité 466
- Sous-traitant 778
- Traitements 35 ss, 842ss, 894ss, 887, 888, 906, 910ss, 923, 1355ss, 1662, 2025, 2031, 2033, 2202
- Transferts 1480
- Transparence 1232
- Villes intelligentes 210
- Violations de données 810 ss
- Voitures autonomes 262 ss, 271ss
- Volume 183, 406

Données biométriques
- Art. 9 RGPD 961
- Définitions 741ss
- Général 826ss

Données de santé
- Action civile 265
- Assurance 199, 204ss
- Big Data 408
- Cloud 277
- Deepmind 429
- Données sensibles 524, 747, 961ss
- Equilibre 79
- Notion 830ss
- Objets connectés 201, 276
- Registre des activités de traitement 1243
- Responsabilité 280
- Sécurité 283
- Sous-traitant 1338

Données génétiques
- Données sensibles 748, 961, 1915
- Notion 822

Droit à l'autodétermination informationnelle
- Art. 13 Cst 1731ss
- Droit 340, 824, 1866
- Helsana 206

Droit à l'information (droit de savoir)
- Accès 60, 159
- Acteurs économiques 208
- Amende 1087, 1089
- Audit 186ss
- Autorité de contrôle 269, 813, 1272, 1630ss, 1688ss
- Considérantt 71 RGPD 1139
- Cour européenne des droits de l'homme 508
- Décisions automatisées 1784
- Déclaration du 3 novembre 2009 494
- Délégué à la protection des données
- Dérogations 690
- Droit à l'oubli 1050, 1066
- Droit d'explication 1150
- Format 1095
- Informations à fournir à la personne concernée 957ss, 1101, 1771
- Jurisprudence CJUE 776
- Normes ISO 491,
- Notion 1074 ss, 1085 ss
- Principe de transparence 1234
- Privacy Shield 159
- Responsable du traitement 1134ss
- Utilité 1143
- Sanction 1187

Droit à l'oubli
- Administration américaine 105
- Anonymisation 412, 418ss
- Automatique ou par défaut 1044
- Blockchain et droit à l'oubli 360
- Commission européenne 122
- Droit de mémoire 1064
- Exceptions 1050
- Jurisprudence CJUE 1035
- LPD 1842
- Moteurs de recherche 1036
- Neutralité technologique 742

- Notion 1032

Droit à la limitation du traitement
- Champ d'application RGPD 694
- Garanties 531
- Information 1107ss
- LPD 1842
- Notification 1030
- Notion 1104
- Obligation du responsable du traitement 1784
- Suppression des données 1048

Droit à la portabilité
- Bonne pratique 1096
- CIP-CN 1872
- Droit à la portabilité 1091, 2198ss
- Groupe de travail Art. 29 1101ss
- Effacement 1100
- LPD 1103
- RGPD 580, 1026, 1819

Droit à la rectification des données
- Déclaration du 3 novembre 2009 494

Droit d'accès
- Abus de droit 1980
- Algorithmes 458
- Augmentation des coûts 1759
- Catalogue exhaustif 1771
- Déclaration relative à la vie privée 2192
- Doctrine 1978
- Droits 1482, 1791
- LPD 656, 1070
- Notion 1068ss
- Personnes décédées 1798
- Renonciation 659
- RGPD 2198ss
- Tiers 1981
- Transparence 1835
- Tribunal fédéral 1976

Droit d'opposition
- Doctrine 1120
- Garanties 916
- Notion 921, 1113ss, 1791, 1842
- Privacy Shield 159

Droit de conduire
- Véhicules autonomes 292

Droit fondamental à la protection des données
- Accès généralisé des autorités publiques 1451
- Art. 47 de la Charte des droits fondamentaux de l'Union 1496
- Autorité de contrôle 1537, 1545, 2051
- Charte des droits fondamentaux de l'Union européenne 585, 2152
- Ciblage 2032
- Commission européenne 1197
- Contrôle de proportionnalité 597ss, 613ss, 644ss
- Conv. 108 522, 543ss (Protocole additionnel), 1507
- Décision d'adéquation 1440
- Délégué à la protection des données 1340
- Garanties fondamentales 1449
- Groupe de travail de l'Art. 29 1452
- Jurisprudence CJUE 582ss, 645ss, 1574
- Koumpli 1540
- Limitation 627ss
- Objectif du RGPD 680
- Pondération équilibrée 621
- Préposé 1995
- Préposée britannique 1298
- Procédure d'urgence 1658
- Profilage 758
- Régulation 436
- Sensibilisation 329

E

Effacement des données
- Traitement 677

Espace économique européen
- Suivi de comportement 723

Etablissement
- Autorité de contrôle 1621, 1653
- Autorité chef de file 1639

- CJUE 2018
- Cloud Act 2108
- Considérant 36 1674
- Encaissement d'une amende 1877
- Établissement de paiement 477
- Établissement bancaire 2127
- Établissement du responsable du traitement 532, 704
- Établissement hors de l'UE 2008
- Etablissement principal 124, 1628, 1666ss, 1671, 2008, 2017ss
- Jurisprudence CJUE 705ss
- Notion 833, 2023, 2024
- RGPD 736ss, 738, 1662
- Siège 1667
- Sous-traitant 1673
- Traitement transfrontalier 1664ss

Ethique
- Cadre 87
- Code 311, 323
- Considérations 265, 278, 287, 310, 330, 429, 447, 451, 1923ss
- Doctrine 318
- Ethics-by-Design 1230
- Groupe de travail de l'art. 29 1385
- Implications
- Norme commune 497
- Opérateurs de téléphonie mobile 468
- Principe de loyauté et de transparence 955, 1149, 1234, 1544
- Principes 430
- Révolution bioéthique 450
- Robotique 325
- Vladimir Poutine 1231

Eugénisme
- Eugénisme thérapeutique 449
- Liberté individuelle 444

Exactitude des données
- Abus de droit 1977
- Devoir de diligence 1106
- Droit d'accès 458
- LPD 1779, 1841
- Principes 755, 938
- SIS 999

Extraterritorialité
- Notion 2011
- Théorie des effets 2138

F

Faisceaux d'indices 708

Fichier 352, 504, 525, 528, 532, 546, 653, 656, 672, 763, 784, 1013, 1061, 1236, 1360, 1740, 1932

Finalité
- Explicite 755

Fournisseurs
- Autorités répressives 394
- Cloud 393
- Commission européenne 567
- Directive 2006/24 636
- Données à caractère personnel 681
- Fournisseurs de services internet 1359
- Fournisseurs de services de Cloud 1767, 2119, 2129
- Obligations de sécurité 950
- Opérateurs de service essentiels 953
- Règlement e-privacy 786
- Responsabilités 391
- RGPD 695
- Services internet 165
- Tiers 477

G

Gouvernance des données
- Audits 947
- Blockchain 363
- Duty of Care 208
- Délégué à la protection des données 1378, 1387
- Dispositif 1395
- Gouvernance des données personnelles 31, 41 ss
- Organisations 941, 1191

- Qualité 1250

I

Indépendance
- États 2167
- Garanties 1582, 1645
- Indépendance des autorités de contrôle 97, 1517, 1535, 1548, 1563, 1567, 1569, 1571, 1573 ss
- Indépendance du délégué à la protection des données 1373, 1406, 1408 ss (Jurisprudence CJUE), 1579 ss, 1581, 1585, 1587, 1594, 1616, 1727, 1987
- Indépendance des procédures 1985
- Indépendance effective 2055, 2076
- Indépendance institutionnelle 1737
- Ombusdman 1473, 1477, 1498 (Privacy Shield)
- Pouvoir judiciaire 2140
- Préposé 1567, 1800, 1819, 1835
- Suisse 2074

Intégrité
- Groupe de travail de l'art. 29
- Intégrité des agents 1586
- Intégrité des données 811
- Intégrité neuronale 330
- Intégrité physique 899
- Intégrité territoriale 2065
- Mesures techniques et organisationnelles 1175
- Principe 940
- Systèmes informatiques 821

Intelligence artificielle
- Analyse de données 194
- Applications 52, 78,
- Augmentation 439
- Bio-robots 313 ss
- Cloud computing 367
- Code éthique 311
- Commission européenne 258, 325
- Contrôle à posteriori 2179
- Convergence 303, 310
- Deep Fake 285
- Ère digitale 183
- Éthique appliquée 1230
- Forum économique mondial 344
- Gouvernance 421, 1926
- Innovation 1885
- Juges 1792
- Notion 300, 422 ss
- OCDE 483
- Principe de responsabilité 1173
- Processus de décisions 433, 435
- Reconnaissance faciale 970
- Robustes 282
- Sommet de Genève 233
- Services financiers 462
- Statut légal 330
- Symbiose 446
- Transhumanisme 440
- Transparence 457, 1234
- Visage 312

Invalidation
- Clauses contractuelles types 1492
- Privacy Shield 1501

ISO
- Normes 360, 387, 489, 852, 2204

Intérêts légitimes
- Déclaration relative à la vie privée 2192
- Information des personnes concernées 912
- Opposition au traitement 1106
- Motifs légitimes 1116
- Notion 906ss, 1083
- Responsable du traitement 804
- RGPD 1130, 1138,
- Profilage 1153
- Traitement automatisé licite 1155
- Transfert 1507, 1532

J

Judicial Redress Act
- Notion 1486

Jurisprudence

- Champ d'application territorial 2171
- CJCE 1026, 1032, 1038, 1667, 2112, 2169
- CJUE 2057, 2087, 2097, 2115
- Comité européen de la protection des données 1727
- Contrôle a posteriori 85, 91
- Cour européenne des droits de l'homme 637, 647, 694, 897, 1909, 2038
- Groupe de travail de l'Art. 29 1043
- Jurisprudence CJUE 122, 171, 208, 252, 528, 541, 583, 592, 594, 600, 607, 617, 618, 626ss, 635, 643, 646, 705, 806, 904, 907, 1039ss, 1057, 1094, 1121, 1129, 1155, 1253, 1313, 1317, 1439, 1449, 1497, 1573ss, 1579, 1582, 1589, 1613, 1728, 1787, 1792, 1911, 1937, 1939, 2183
- Jurisprudence administrative ou judiciaire 1440, 1532, 1914
- Jurisprudence allemande 1068
- Monisme 2075
- Portée du Règlement 2118
- Présomption de bonne foi
- Tribunal fédéral 1563, 1569, 1570, 1882, 1957, 1975ss, 1977, 1979

L

Libre circulation

- Autorité de contrôle 1553
- CJUE 1579
- Charte des droits fondamentaux de l'UE 480
- Contrôle a posteriori 1335, 1743, 1920
- Convention 108 537
- Directive (UE) 2016/680 4
- Directive 2002/58/CE 653
- Droit de la concurrence 12
- Droit international 2152
- Enjeu 38, 1885
- Entreprises suisses 1828
- Flux transfrontaliers 1425
- Group de travail de l'Art. 29 577
- Libre circulation des données non personnelles 648ss
- LPD 1762, 1870
- OCDE 480, 2150
- Règlement 45/2001 1343
- RGPD 11, 14, 661, 663, 985, 990, 1000, 1780, 1887ss, 1970, 2001, 2072
- Réforme 118
- Sécurité juridique 2161
- Système juridique 92

Licéité

- Art. 3, al. 2 RGPD 2005, 2007
- Collecte de données personnelles 208, 755, 969
- Conformité 1952
- Conv. 108 1779
- Décision d'adéquation 1742
- Demandes de renseignements 2129
- Droit à la portabilité 1091
- Garanties 530
- Général 853
- LPD 1841, 1877
- Pseudonymisation 766
- Responsable du traitement 1543
- Retrait consentement 871, 881
- RGPD 906, 1183, 1192, 2131
- Safe Harbor 140
- Traitements 265, 1287
- Transferts 38, 40, 1436, 1456, 1488, 2191
- Transparence 1232

Localisation

- Activité de traitement 2021, 2124, 2133, 2157
- Clouds 371
- Délocalisation 115, 273ss,
- Directive 95/46/CE 63
- Directive 2006/24
- Données à caractère personnel 745
- Etablissement 2008
- Géo-localisation 469, 683, 1359, 1366
- Localisation 2016, 2189

- Métadonnées 572
- Personne 2135, 2162
- Profilage 757, 1122, 1260,
- Public cible 727
- RGPD 561
- Unité économique 2169

LPD
- Accord-cadre 1865
- Art. 49 LPD 2108
- Avant-projet de révision 1005, 1775ss, 1783, 1793, 1797, 1799ss
- Champ d'application 1736
- Concepts économiques 1921
- Conseil fédéral 660ss
- 1835ss, 1864, 1865ss, 1870ss
- Conseiller à la protection des données 1368
- Décision d'adéquation 1455
- Droits 2098
- Entrée en vigueur 1735
- Google Street View 2185
- Mise en consultation 1740
- Notification 1015
- Notion 650ss, 728
- Obligations 1785
- Préposé 1997ss
- Private Enforcement 1955, 1970, 1971ss,
- Projet de LPD révisée 1836 ss, 1840ss, 1843ss, 1846ss, 1849ss, 1852, 1855, 1860, 1875ss
- Révision 1016, 1103, 1271, 1738, 1745ss, 1818ss, 1823, 1833ss
- Traitement 2095
- Tribunal fédéral 1975, 1977 ss, 1981ss,

M

Machine Learning
- Cambridge Analytica 429
- Cloud 371
- Croissance économique 427
- Innovation 429
- Traitement des données 2179

Mécanisme de guichet unique
- Autorité chef de file 1629
- But 1660
- Coopération entre autorités 1675, 1679ss, 1688
- Exceptions 1648ss, 1656
- Institutionnalisation du contrôle 2162
- Mécanisme 2004, 2092ss
- Multinationales 1672
- Principe 1625ss
- Réclamation 1641
- RGPD 706
- Transferts 1661, 1663
- Urgence 1658

Mécanisme du contrôle de la cohérence
- Autorités de contrôle 1988, 2108, 2161
- CEPD 1702
- Notion 1706ss , 1717, 1721
- Obligations 1783
- RGPD 1515, 1562, 1635, 1637, 1640, 1659, 1688, 1698
- Suisse 1861

Mineurs
- Données sensibles 1915
- LPD 1844ss
- Notion 1158, 220
- Protection renforcée 1241

Minimisation des données
- Blockchain 1162
- Garanties 531, 554, 755, 762, 892, 935, 937, 1067
- Mise en oeuvre 1162
- Personne concernée 1105
- Principe 278, 1946, 1220, 1842, 1945
- Privacy-by-Design / Privacy-by-Default 1227
- Pseudonymisation 1215
- Responsable du traitement 1205, 1214

Mission d'intérêt public
- Effacement des données 1066
- Notion 903, 1099, 1116, 1649, 1652

N

Neutralité
- Principe de neutralité technologique 545, 553, 742, 1159, 1163, 1879, 1921
- RGPD 180, 433
- Suppression de la neutralité du Net 165ss, 2117

Normes
- Application directe 540
- Choix des normes 447
- Commission européenne 2135
- Conflit de normes 2038
- Conseil de l'Europe 510
- Décisions automatisées 1131
- Droit français 2073
- Extraterrittorialité 2064
- Groupe de travail de l'Art. 29 578
- Instrument mondial contraignant 117
- Multinationales 498
- Normes comptables IFRS 851, 1010 ss
- Normes de conduite 1911
- Normes de droit international public 2061, 2166
- Normes de sécurité 283
- Normes de sûreté 226, 234
- Normes juridiques 2132
- Normes spécifiques 2038, 2176
- Normes ISO 360, 484ss, 852
- Principe de territorialité 2172
- RGPD 2001
- Soft Law 2080
- Sources juridiques 478

O

Obligations
- Accord FATCA 2135
- Acteurs 46, 388, 394, 456, 491, 566, 664, 667, 772, 781, 784, 888, 950, 953, 1017ss, 1058, 1141, 1208, 1235, 1284, 1313, 1318ss, 1338ss, 1376, 1418ss, 1433, 1643, 1781ss, 1793ss, 1837ss
- Amendes 1183, 1329, 1423, 1876
- Class action 1945
- Conflit 2050
- Cour européenne de droits de l'homme 1570
- Délégué à la protection des données 1371, 1387, 1389
- Droit international 2172
- Diligence 208, 1105, 1181, 1192, 1296, 1545, 1849, 1859, 1876, 1912
- États 523, 1579, 1825, 1872
- Extraterritorialité 2058, 2144
- FATCA 2144
- Jurisprudence CJUE 628, 1473
- LPD 1835, 1878
- Obligations internationales 1440, 1448
- Obligations morales 2151
- Répartition des obligations 391
- RGPD 31, 120, 560, 573, 812, 941, 975, 1328, 1602, 1660, 2095
- Robots 319, 333
- Sanctions 2144
- Transferts 1480, 1494
- Urgence présumée 1659

Opacité
- Gouvernance des technologies digitales 421
- Opacité des algorithmes 1145ss, 1137, 1144

Opposition (droit d')
- Doctrine 1120
- État tiers 2166
- Garanties données par le responsable du traitement 916, 921
- LPD 1842
- Notion 1113ss, 1117, 1791
- Privacy Shield 159, 1478

Organisation de Coopération et de Développement Économiques
- Doctrine 2077
- Échange de renseignements en matière fiscale 2143
- Fiscalité 2150
- Global Privacy Enforcement Network 187

- Lignes directrices concernant la protection de la vie privée 117
- Pays membres de l'OCDE 480
- Principes directeurs pour l'IA 310, 483

P

Pacte ONU II
- Pacte international relatif aux droits civils et politiques 479

Personnalité
- Atteinte 1733, 1969, 2002, 2185
- Attributs 2197
- LPD 1870
- Personnalité juridique
  - Comité européen de la protection des données 1695
  - État 2064
  - Robots 330ss
- Profil 1883
- Violation de sécurité 1859

Personnes concernées
- Accord Privacy Shield 155
- Accord Safe Harbor 148
- Action civile 1539
- Action en responsabilité 22
- Analyse d'impact 1256
- Art. 3, al. 2 RGPD 2008ss
- Associatins 2107
- Assurance 321
- Attentes des personnes concernées 911
- Autorité de contrôle 124, 841, 1440, 1677
- Blockchain 1159
- Catégories de personnes concernées 1245
- Ciblage 712, 717, 2009
- Class Action 1943
- Clouds 211
- Confiance 973
- Consentement 265, 754, 881ss, 932, 1049
- Conv. 108 537
- Délégué à la protection des données 1344, 1353, 1424
- Dérogations 534
- Discrimination 825, 1148, 1842ss
- Droits 28, 159, 700, 722, 846, 867, 1026, 1038, 1044, 1068ss, 1074ss, 1089, 1090, 10911ss, 1104ss, 1113ss, 1135, 1503, 1528, 1735, 1819, 1835, 1872ss, 1905, 1911, 1915, 2018
- Effectivité des droits des personnes 58, 60, 1891
- Extraterritorialité 1374
- Garantie 318, 628, 1118, 1138, 1155, 1253, 1256, 1314ss, 1452, 1477, 1488, 1492, 1496, 1508, 1517, 1529, 1812, 1922, 1975
- Guichet unique 1653, 1658 (urgence)
- Identifiables (Personnes) 318, 549
- Identification des personnes concernées 524, 936
- Information 186, 265, 269, 957, 1497, 1784
- Localisation 2016,
- LRens 171
- Notification d'une violation de données 814, 818, 820 (dommages et intérêts), 1279ss, 1988
- Notion 10, 11, 12, 63, 83, 89, 105, 118, 122ss
- Personnalité 654
- Plainte 1483
- Profilage 2022
- Protection des personnes concernées 330, 701, 707, 1336, 2111, 2133, 2196
- Observation du comportement 548
- Protocole additionnel à la Conv. 108 543, 545
- Recours 1727
- Recours effectifs 159,
- Représentant 785, 1839, 2095
- Responsabilité 360, 1173, 1294, 1313, 1338, 1780
- RGPD 14, 21, 732, 2033, 2035, 2103
- Sanctions 1320, 1329ss
- Sous-traitant 2040
- Tiers 191, 1157, 1393

- Traitements à grande échelle 1344, 1689,
- Traitements transfrontaliers (1662)
- Transparence 1237
- Vie privée 57

Personnes décédées
- Champ d'application du RGPD 1797ss

Pesée des intérêts
- Avis et opinions du Comité européen à la protection des données 1728
- Class action 748
- Jurisprudence CJUE 208, 621, 807, 1121, 1129
- Législateur 27
- LPD 1763
- LRens 170
- Neutralité
- Notification d'annonce de violation de données à caractère personnel 1264
- Pesée des intérêts en présence 1554
- Privacy-by-Design 1201
- Protection de la liberté économique 1845
- Recherche 1105
- Responsable du traitement 1787
- RGPD 905, 1855
- Transparence 959

Portabilité
- Automatisation des processus 1102
- Avant-projet de la commission européenne 123
- Codes de conduite 1096ss
- Groupe de travail de l'Art. 29 1101
- LPD 1103, 1872
- Norme ISO 27018 491
- RGPD 580, 1026, 1091, 2198ss

Préposé fédéral à la protection des données
- Applicabilité du RGPD 721
- Autorité de surveillance
- Avis consultatifs 1862
- Codes de conduite 1851
- Consentement 880
- Cumul des fonctions de surveillance et de conseil 1999
- Décision d'adéquation 1764
- Déclaration du 3 novembre 2009 496
- Déni de justice 1565
- Doctrine 1567ss, 1572
- Droit de regard de l'Union européenne 1692
- Elizabeth Denham 1298
- Evaluation de la Commission européenne 1864
- Garanties pour les transferts transfrontaliers 1812ss
- Helsana 754
- Indépendance 1563
- Interprétation restrictive du ciblage 716
- Mesures provisionnelles 1875
- Mise en oeuvre du droit suisse à la protection des données et à la transparence 1993, 2177
- Nomination 1555
- Notification des violations de données 1846
- Obligations 656,
- Pouvoirs 1850, 1873, 1878, 1881, 1972, 1997, 1998
- Registre 1874
- Révision LPD 1016, 1741, 1776, 1800ss, 1816, 1819
- Sanctions administratives 1848, 1860
- Tribunal fédéral 1566

Principe d'adéquation des législations
- Application 1013,
- Compétence de la Commission européenne 1437
- Conditions 1440ss
- Décision d'adéquation 38, 40, 132, 556, 740, 755, 987, 989, 1005, 1008ss, 1015, 1226, 1428, 1438
- Doctrine 1448
- Examen périodique 1454ss

- Flux transfrontaliers 1427, 1437ss
- Invalidation 1460
- Jurisprudence CJUE 144, 1439
- Liste des pays bénéficiant d'une décision d'adéquation 1464
- LPD 372
- LRens 171
- Procédure 1444ss
- Publication 1441
- Représentant 1376
- Safe Harbor 143
- Validité 1463

Privacy Shield
- Amendment 1863
- Avis du Comité européen à la protection des données 1500
- Critiques 161, 162, 1470ss, 1487, 1490ss
- Décision d'adéquation 1445, 1474, 2043, 2161
- Garanties en cas de transfert transfrontalier vers des pays tiers 1429, 1469
- Groupe de travail de l'Art. 29 1478
- Invalidation de l'accord Safe Harbor 149, 152, 153, 1501
- Notion 154ss, 1466ss, 1476ss
- Opinion de l'avocat général de la CJUE Henrik Saugmandsgaard 1493ss, 2044
- Principes 159, 1479
- Reconnaissance de l'Accord privacy Shield par la Commission européenne 157ss
- Site de l'Accord Privacy Shield 160

Proportionnalité
- Avant-projet LPD 1779, 1841, 1875
- Droit au déréférencement 2114
- Jurisprudence CJUE 2095
- LPD 1841
- Préposé 1875
- Principe 1472, 1779

Protocole additionnel à la Convention 108
- Art. 12 bis Conv. 108
- Autorités de contrôle 1535
- Conseil fédéral 1831
- Garanties 1508
- LPD 1740, 1774, 1788
- Niveau de protection approprié 1809
- Rapport explicatif 1569
- Transferts transfrontaliers 1812

Pseudonymisation
- Analyse d'impact 1258
- Définition 741, 759ss
- Dommage 1282
- Garanties 916, 931, 937, 944, 1176,
- Technique 691, 692, 1213, 1266, 1783, 2203

R

Recours collectifs (class action)
- Accès à la justice 1965
- Adversarial legalism 1966
- Conseil fédéral 1957
- Contrôle a posteriori 1922
- Dommages et intérêts triples 2132
- Droit de la concurrence 2141
- Effet transfrontalier 1935
- LPD 1957
- Mécanisme 1958
- Mise en oeuvre effective du droit de la protection des données 1292, 1540, 1747
- Principe 11, 665, 1290, 1934, 1744,
- Private Enforcement 1932, 1945, 1946, 1949
- Recours 1291
- Réparation du dommage 1965, 1968
- Volkswagen 1968

Registre
- Jurisprudence de la CJUE 514
- LPD 656, 1835
- Organes fédéraux 1794
- Préposé 1874

- Registre des activités de traitement 1242, 1328, 1338ss, 1391, 1952
- Registre distribué (Blockchain) 352, 358, 360
- Registres publics 652
- Robot 262
- Transfert transfrontalier 1531

Règles d'entreprises contraignantes (Binding Corporate Rules)
- Avant-projet LPD 1806
- Clauses contractuelles 2047
- Notion 1510ss
- Transfert 1517

Règles prudentielles
- Opérateurs de téléphonie mobile 468

Règlement E-Privacy
- Métadonnées 414
- Projet de la Commission européenne 573
- Rapport du comité LIBE 574
- Représentant 786
- Sécurité 948

Renforcement des droits
- Analyse d'impact PwC
- Citoyens européens 159,
- Conseil fédéral 18721026
- LPD 1835ss, 1872
- Privatim 1759, 1819

Renseignement (Loi sur le Renseignement)
- Exploitation du réseau câblé 171
- Référendum 169

Représentant
- Amende 1877
- Avantage 1960
- Chambre des représentants des États-Unis 165, 226
- Consommateurs 112
- Décision d'adéquation 1444
- Déclaration sur le vie privée 2215
- Délégué à la protection des données 1377
- Établissement 705
- Notion 781ss, 2196
- Registre des activités de traitement 1245, 1247
- Représentants de chaque autorité indépendante de protection des données 577
- Représentant des cantons 2074
- Représentant de l'industrie 495, 1103
- Représentant de la Commission européenne 1694
- Représentant de la société civile 580
- Représentant du responsable du traitement ou du sous-traitant 1242, 1338, 1376, 1378, 1672, 1835, 1839, 1880, 2095ss, 2184
- Weltimmo 2018

Réputation
- Action civile 1903
- Analyse d'impact 1258
- Demandes d'accès 1031
- Gestion des risques 1333
- Protection des données 1203
- « Right of Reasonable Inferences » 971
- Risques 471, 970
- Pacte ONU II 479
- Sous-traitants 726

Responsable du traitement
- Action civile à posteriori 1118ss, 1871ss, 1901
- Action en responsabilité 1293, 1944
- Action judiciaire 1609
- Activités de base 1350
- Analyse d'impact 623, 1250ss
- Autorité chef de file 1624ss, 1648ss (exceptions), 1670, 1677
- Autorité de contrôle 841, 1601, 1602, 1603
- Charge de la preuve 798, 802, 867, 1296
- CEPD 2017, 2020
- Code de conduite 1303

- Consentement 881, 884, 885
- Consentement parental pour mineurs 1158
- Conservation des données personnelles 929
- Consultation de l'autorité de contrôle 624, 2205ss
- Contrat 888ss
- Contrôle a posteriori 1538
- Décisions automatisées 1128, 1130
- Définition 550, 1778
- Délégué à la protection des données 1340ss, 1369ss, 1396ss, 1400ss, 1411ss, 1418ss
- Déséquilibre entre la personne concernée et le responsable du traitement 801, 878
- Devoir de diligence 1105
- Détermination du droit applicable 2111
- Directive (UE) 95/46/CE 2037
- Documentation 1182ss, 1185ss
- Documentation de la violation de données 1283
- Données anonymisées 1152ss
- Droit à l'oubli 1033ss, 1046, 1047, 1050 (dérogations), 1054, 1055, 1058, 1061ss
- Droit à la limitation des données 1107ss, 1110ss
- Droit à la portabilité 1092ss, 1095, 1099
- Droit aux déductions raisonnables 971
- Droit d'accès 1068ss, 1071ss, 1078, 1082ss
- Droit d'opposition 1115ss
- Droit de rectification 1090
- Etablissement 702ss, 731, 2016, 2022, 2023, 2024
- Exactitude des données 939
- Extraterritorialité 2008, 2009, 2012
- Faisceau d'indices 2030
- Finalités 930
- Garanties 916, 1811, 1813
- Garanties à mettre en place 1138ss, 1141ss, 1155, 2041
- Groupe de travail de l'Art. 29 803
- Identification 772
- Identité 532, 869
- Information de la personne concernée 816ss, 1280
- Intégrité 811
- Intérêts légitimes 805, 905ss, 914ss, 919, 921
- Intérêt prépondérant 1798
- Intérêt public 903
- Jurisdiction 548
- Jurisprudence CJUE 775 246ss, 253ss, 273, 313, 352, 380, 444, 490, 538, 620, 658, 661, 667ss, 767, 786, 815, 844, 855, 879, 939, 965, 1012, 1157, 1163ss, 1175ss, 1194, 1215, 1228, 1235ss, 1283ss, 1293ss, 1301ss, 1316, 1317, 1332, 1376, 1389, 1518, 1520ss, 1672, 1714, 1774ss, 1807, 1820ss, 1842, 1850ss, 1865, 1869,1871, 1876, 1880, 1883, 1888, 1890, 1897,1900, 1907, 1922, 1937, 1953ss, 1962
- Libre circulation des données 661
- Localisation 561, 833
- Mesures appropriées 653, 1134, 1153ss
- Mesures techniques et organisationnelles 1295, 1299, 1300ss
- Mesures techniques et organisationnelles appropriées au risque 955, 1941
- Notification au destinataire 1030
- Notification de la violation de sécurité 813ss
- Notion 771, 778, 779
- Objection pertinente et motivée 846
- Obligations 1781, 1872, 1912
- Obligation de notification à l'autorité de contrôle 1263, 1268, 1272ss
- Obligations de rendre des comptes 554, 566
- Personne identifiable 549

- Pesée des intérêts en présence 807, 1554
- Pré-légitimation des traitements 1539
- Preuve de conformité 1190, 1193
- Principe de loyauté et de transparence 955 ss
- Principes de protection des données 848
- Privacy-by-Design, Privacy-by-Default 1196ss, 1201ss
- Profilage 1129, 1130
- Recours juridictionnels 1723, 2107
- Régime de responsabilité 1021
- Registre des activités de traitement 1242
- Règles d'entreprise contraignante 838
- Réparation et responsabilité 1310ss, 2109
- Représentant 781, 783, 784, 1376ss, 2095, 2184, 2192, 2196
- Responsabilités 664, 668, 726, 773, 1164ss
- Responsable conjoint 774
- Sanctions 1309
- Sanction pénale 1849
- Sous-traitant 834, 2028
- Suivi de comportement 2033
- Territorialité 1374
- Tiers 791
- Traitement excessif 927
- Traitement transfrontalier 843
- Transferts fondés sur des garanties appropriées 1502, 1512, 1521, 1528, 1531, 2039, 2040
- Vérification de la conformité à posteriori 101

Révision totale de la LPD
- Consultation 1766
- Introduction 8
- Projet LPD révisée 1740, 1748

Robots
- Analyse de données 194
- Assurance obligatoire 321
- Autonomie 217, 301
- Biorobots 309, 313
- Charge de la preuve 330
- Commission européenne 261ss
- Délégations des décisions 323
- Développement responsable des robots intelligents 311
- Doctrine 318
- EMS 1915
- Interaction homme-machine 335
- Isaac Asimov 322
- Killer robots 313
- Objets connectés 336
- Personnalité juridique pour les robots 331, 334
- Régime de responsabilité strict 244
- Robots humanoïdes 309ss, 312
- Robots intelligents 297ss, 302, 304, 305, 307, 320, 324ss
- Statut juridique en droit européen 319
- Taxation 327, 328ss

S

Safe Harbor (accord)
- Accord Privacy Shield 158, 1466, 1467
- Clauses contractuelles 1518
- Décision d'adéquation 143
- Groupe de travail de l'art. 29 152
- Invalidation 139, 149
- Jurisprudence de la CJUE 143, 148, 582, 1488
- Préposé fédéral 153
- Programme d'adhésion volontaire 150, 151

Sanction
- Accord FATCA 2135
- Amende 852, 1193, 1320, 1876, 1953
- Aspect dissuasif 1903
- British Airways 2182
- Class action 1965, 2132
- Code pénal 1879
- Conformité au droit 2146
- Contrôle a posteriori 10, 1335

- Coopération des autorités de contrôle 561, 974, 1627 (guichet unique)
- Décision d'adéquation 1768
- Dédommagement financier 1901
- Délégué à la protection des données 1399, 1422
- Demandes d'accès 1031
- Devoirs des entreprises 33
- Directive (UE)2016/680 4
- Entreprises établies dans l'Union 1187
- Exécution des sanctions 990
- Garanties 946
- Gestion des risques 1333
- Injonction de l'autorité 819
- Mesures d'exécution 2159
- Notion 535ss, 1327ss
- Projet de LPD révisé 1847, 1860, 1871
- Préposé 1848, 1878, 1879, 1997
- Privacy Shield 154
- Public Enforcement 1907, 1988, 1994, 1996
- Rapport explicatif de la Convention 108 687, 688
- Reconnaissance de la sanction par les États tiers 2125
- Recours juridictionnel effectif 1725
- Respect de la personne humaine 79
- Responsabilité 1021, 1183, 1306, 1911
- Risque de double sanction (non bis in indem) 1880
- Risques de sécurité 1307
- RGPD 21, 66, 87, 975, 1309, 1881, 2158
- Safe Harbor 150
- Sanction administrative 1603, 1835, 1934, 1989, 2182
- Sanctions des comportements contraires au droit 1898
- Sanctions dissuasives 1197
- Sanctions pénales 1772, 1849, 1859
- Sanctions susceptibles de recours 1881
- Santé 201
- SIS 1000
- Vol de données Equifax 71

Schrems
- Accord Privacy Shield 1466
- Appel 143
- Autorité de surveillance irlandaise 140
- Avis du groupe de travail de l'art. 29 1452
- CJUE 79, 148, 1460, 1491
- Décision d'adéquation 1742
- Enjeux 1504
- Garanties appropriées 1516
- Invalidation de l'accord Safe Harbor 1488
- Validité des clauses contractuelles 1518

Secret professionnel / des affaires
- Avocat (Clouds) 891
- Confidentialité 1084, 1258, 1276
- Obligation 1415
- Secret des affaires 1059, 1078
- Violation du secret d'affaire 1137

Sécurité
- Algorithmes 211
- Approche fondée sur le risque 1238
- Art. 8 CEDH 507
- Assurances 256
- Blockchain 348, 364
- British Airways 1297
- Catégories de données 746
- Cloud 368, 371, 466
- Code de conduite 945
- Comité européen 1721
- Confiance dans la sécurité 135, 470
- Conv. 108 533
- Coopération 2159ss
- Cybersécurité 76, 77, 78, 185, 257, 284, 1087
- Décision d'adéquation 1440
- Deep Fake 285
- Délégation pour la sécurité du conseil fédéral 171

- Délégué à la protection des données 1381, 1390, 1394
- Directive PSD2 475
- Documentation 1182
- Droit à la protection des données 2066
- Enregistrement 1883
- Espace de liberté, de sécurité et de justice 2071
- Éthique appliquée 1230
- Extraterritorialité 2158
- Fournisseurs tiers 477
- Garanties 38, 161, 466, 1024, 1213
- Insécurité juridique 909, 927, 1133, 1492, 1622, 1780
- Juridique 15, 63, 80, 82
- Jurisprudence CJUE 595, 596, 636, 639, 806
- Liberté 284
- Libre circulation 2161
- LRens 167
- Mesures de sécurité 529, 1020, 1188, 1245, 1304ss, 1339
- Niveau de sécurité adapté aux risques art. 32, 1857 (adéquat)
- Niveau de sécurité approprié 943,
- Niveau élevé de sécurité 948
- Normes ISO 485ss
- Obligations de sécurité 950
- Objets connectés 184, 255
- Obligation de moyens renforcée 1209
- Principe d'universalité
- Privacy Shield 1470ss
- Projet LPD révisé 1772, 1835, 1841
- Pseudonymisation 762
- PwC 1758
- RGPD 910, 975, 1262, 1436
- Sécurité alimentaire 649
- Sécurité des données 282ss, 387, 389, 940
- Sécurité du traitement 1179
- Sécurité end-to-end 1203
- Sécurité juridique 242, 559, 571, 583, 664, 1005, 1103, 1727, 1795, 1881, 2105, 2108, 2155
- Sécurité nationale 156, 642, 693, 1131
- Sécurité routière 216, 218, 234, 241
- Sociale 63
- Sphère de sécurité européenne 137
- Standards 1003
- Test de proportionalité 527
- Transferts 1532
- Violation de données 810, 811, 1265, 1266, 1269, 1274, 1859

Sensibles (données)
- Analyse d'impact 2206
- CEPD 2017
- CIP-CE 1769
- CIP-CN 1872
- Classification 969
- Consentement exprès 1835, 1855
- Délégué à la protection des données 2190
- Données non sensibles 967
- Dispositif de Schengen et Dublin 1692
- Entreprise 1767
- Entreprises de moins de 250 personnes 1246
- Forum shopping 2017
- Garanties appropriées 1507
- LPD 1883
- Mineurs 1844, 2200
- Notion 960
- Protection juridictionnelle effective 2196
- Prise de décisions automatisées 1156
- Régime de responsabilité objective 1915
- Traitement 967
- Traitement à grande échelle 1353
- Traitement risqué (analyse d'impact) 1260

Séquençage d'ADN
- Données génétiques 824
- Séquençage d'ADN 1157
- Stockage des données 384

Soft Law
- Mécanismes de Soft Law 2080

- Normes de Soft Law 2078
- Suisse 1851

Sous-traitant
- Accessibilité du site internet 715
- Acteurs 1017
- Action civile 10, 1293ss, 1903, 1941, 1943, 1945, 1951 (charge de la preuve), 1965
- Action sur instructions 388ss
- Art. 3, al. 2 RGPD 704
- Amendes 1953
- Autorités de contrôle 490, 784, 841, 1597, 1603 (injonction), 1620ss, 1624, 1639, 1643, 1647, 1660
- CEPD 2017, 2020
- Certification 1235
- Champ d'application 689, 2027ss
- Clauses contractuelles types 2047, 2163
- Codes de conduite 1303, 1528
- 1759
- Comité européen 1720
- Contrats 1952
- Décision effective 737
- Délégué à la protection des données 1338ss, 1396, 1399, 1400, 1407, 1409ss, 1418, 1420, 1423, 1353
- Dommages et intérêts 1332
- Établissement 703, 833 (établissement principal), 2008, 2009, 2016
- Extraterrittorialité 707, 709, 1374, 2023
- Géolocalisatioon en temps réel 1359
- Gestion des risques (de sécurité) 1307, 1333
- Groupe de travail de l'art. 29 1369ss
- Lien inextricable 1351
- Mise en oeuvre effective 2196
- Mesures techniques et organisationnelles appropriées 95, 1301, 1783, 1784, 1905
- Niveau de risques 1302
- Normes IFRS 851
- Notion 550, 770ss
- Nouvelles obligations du RGPD 1338
- Objection pertinente et motivée 846
- Privacy-by-Default / Privacy-by-Design 1196, 1208
- Privacy Shield 159
- Private Enforcement 1538, 1540
- Procédures coercitives 785
- Projet de LPD révisée 1747, 1785, 1793, 1795ss, 1805, 1835, 1836, 1859, 1871, 1874, 1876, 1900, 1901
- Recours juridictionnel effectif 21, 665, 668, 1723, 2107
- Registre des activités de traitement 1245
- RGPD 975, 1921
- Règles d'entreprises contraignantes 838
- Réparation du préjudice subi 2109
- Représentant 781, 1376, 1397, 2095, 2192, 2198
- Responsabilité 46, 664, 726, 850, 1019ss, 1164ss, 1306, 1310, 1311ss, 1780, 1911
- Situation du sous-traitant 729ss
- Suivi de comportement 2033
- Tiers 791ss
- Traitement à grande échelle 1344
- Traitements de données 36
- Traitement transfrontalier 1662, 1664, 1666, 1673ss, 1677
- Transferts transfrontalier 413, 843, 1427, 1432ss, 1502, 1512, 1514, 2039
- Visite médical coontraignante 1748

Snowden Edouard 83, 88, 132, 133ss, 148, 156

T

Tableau de bord de santé personnalisée 202

Taxation des robots 327

Technologie FinTech 183, 345, 356, 459, 461, 472

Test de la balance des intérêts 915

Tiers
- Autorité nationale 1613
- Communication à des tiers 1998
- Droit de rectification auprès des tiers 1759
- Destinataire 787
- Directive PSD2 474, 476, 477
- Domaine médical 191
- Droit à l'auto-détermination informationnelle 338
- Droit d'accès 1981
- États tiers 1692, 1829, 2002, 2005ss, 2006, 2039ss, 2040, 2041, 2080ss, 2102, 2103, 2106, 2108, 2114, 2129, 2131, 2163, 2165, 2166, 2167, 2170, 2192, 2196
- Google 212
- Infractioon 1884
- Intérêt des tiers 1614
- LPD 1982
- Niveau de protection adéquat 147, 1826
- Normes ISO 488
- Pays tiers 143, 144
- Personnes décédées 1798
- Présomption d'atteinte 1836
- Privacy Shield 159
- Résolution de conflits 2091, 2098
- Robots 320
- Tiers de confiance 404
- Tiers non autorisés 184
- Transfert 159, 2047ss, 2069, 2085
- Vente de données 469
- Conv. 108 537
- LPD 652, 656, 659
- Pays tiers 671
- RGPD 695
- Langue 715
- Transferts 739, 740ss, 845, 890, 975, 1079, 1171, 1427, 1429, 1430, 1439ss, 1493, 1494, 1512, 1525, 1532
- Décision d'adéquation 1436ss, 1462ss
- Principe de réciprocité 1171
- Principe du droit à réparation 1312
- Demandes des tiers 1393
- Collecte auprès d'un tiers 1081
- Droit à la portabilité des données 1097
- Effacement 1033, 1054 (notification des tiers), 1060, 1063
- Droit à l'information 1075
- Droit à l'oubli 1038
- Avocat 891
- Licéité 906
- Helsana 754
- Tribunal administratif fédéral 754
- Tiers de confiance 764
- Tiers 791

Traçabilité
- Blockchain 353, 742
- Industrie alimentaire 455
- Traçabilité des données 1394
- Traitement 1109
- RGPD 2155

Traité sur le fonctionnement de l'UE 105, 498, 555, 1516

Traitement transfrontalier
- Mécanisme du guichet unique 1627, 1653 (exceptions)
- Notion 842, 1662ss

Transhumanisme 440, 446

Transparence
- Action de groupe 1326
- Analyse d'impact 619
- Arrêt Google 1187
- Cloud 369, 491
- Comité européen 1701
- Confiance 1133
- Délégué à la protection des données 1394
- Garanties 916
- Industrie alimentaire 456
- Innovations 554
- Normes IFRS 1011
- Obligations des parties 1318

- Principe 269, 494, 755, 816, 853, 892, 954, 957ss, 1203, 1232ss
- PSD2 Directive 473, 477
- Préposé 656, 754
- Publication des avis de l'autorité de contrôle 1612
- Registre des activités de traitement 1244
- Responsabilité 242, 1691
- RGPD 560, 664,
- Transparence des algorithmes 1137, 1144, 1146, 1149, 1150
- Tribunal fédéral 1564

V

Valeur juridique contraignante
- Charte des droits fondamentaux 3
- RGPD 500, 585, 848
- Conv. 108 521, 538, 1005, 2062

Véhicules autonomes
- Action civile 265
- Assurance robotique 259
- Boíte noire 237
- Blockchain 357
- Building Trust in Human-Centric Articial Intelligence 258
- Class action 1968
- Considérations éthiques 287
- Cybersecurity Act 257
- Détermination de l'auteur d'un accident 232
- Développement de véhicules autonomes 224
- Droit de conduire 292, 294
- État du Californie 238
- État du Nevada 235ss
- Exemple de système autonome 219ss
- Garantie 1138
- Impact environnemental 291
- Interactions avec l'environnement 239
- Niveaux d'autonomie 228ss
- Normes de sûreté 226, 234
- Objets connectés 190
- Proposition de résolution du Parlement européen 223
- Protection des données 262ss, 267, 270ss, 273ss, 279, 280.
- Répercussions juridiques 241
- Responsabilité 242ss, 280
- Robots 301, 307
- Sécurité routière 216, 218
- Sécurité 255
- Self-drive act 226
- Tests 254

Violations de données
- Amende 1286
- Autorités compétentes européennes 1271, 1272, 1309
- British Airways 1187
- Déclaration 554
- Définition 741ss
- Délai de notification 1268, 1275
- Département fédéral du commerce américain 226
- Détection automatisée des violations 821
- Documentation 1283
- Droit à la réparation du préjudice 665
- Information de la personne concernée 1263, 1268, 1269, 1271, 1277, 1988, 2201
- Mesures appropriées 941, 1284
- Mesures d'urgence 1285
- Nombre 76
- Notification 105, 1835, 1988
- Notification forcée par l'autorité de contrôle 818
- Notion 810ss, 1263ss, 1265ss
- Obligation de double notification 1277
- Pseudonymisation 762
- Procédure en cas de violation de données 2201, 2202
- Responsabilité 767
- Responsabilité solidaire du responsable du traitement et du sous-traitant 1019
- Risque pour les droits et libertés 1269
- Violation de l'obligation d'annonce 819