Les Normes juridiques internationales applicables aux communications individuelles : les enjeux du " secret des correspondances " et des " données personnelles "

Sébastien-Yves Laurent, Maxime Kheloufi

ANR-14-CE28-0024-02

Programme « UTIC France-Europe »

UTIC
USAGES DES TECHNIQUES D'INTERCEPTION DE COMMUNICATIONS

Les normes juridiques internationales applicables aux communications individuelles : les enjeux du « secret des correspondances » et des « données personnelles »

IRM
Institut de recherche Montesquieu

université de BORDEAUX

Livrable n° 7
v. 10

Sébastien-Yves Laurent et Maxime Kheloufi
sebastien.laurent@u-bordeaux.fr / maxime.kheloufi@u-bordeaux.fr
Université de Bordeaux

28 février 2018

Sommaire

1 Synthèse et évaluation quantitative des textes juridiques (1948-2016) 4

2 Le « secret des correspondances » : un droit dérivé à portée très générale, dépassé par l'évolution technologique 5

3 L'abondance des textes innovants relatifs à la « protection des données personnelles » depuis 1973 12

4 L'apport considérable de la jurisprudence européenne sur les données 29

5 L'ambition du paquet « données » de 2016 40

6 Le contexte politique de l'adoption du RGPD dans la décennie 2010 44

7 Les innovations du RGPD en matière de protection des données 46

8 L'innovation fondamentale du RGPD en matière de responsabilisation des acteurs de la *data* 49

9 L'application géographique du RGPD européen, étendue au-delà de l'UE 53

10 L'application matérielle du règlement: la « sécurité nationale » en dehors du champ du RGPD 58

11 Conclusions (provisoires) 61

12 Annexes 62

13 Sources et bibliographie 91

Les échanges de communications individuelles qui sont au cœur du programme UTIC relèvent de deux grandes catégories de normes juridiques, le « secret des correspondances » (SC) et la protection des « données personnelles » (PDP). Ces deux ensembles sont au cœur de ce 7e livrable, l'intention étant de les étudier sur un plan quantitatif et qualitatif, selon le plan ci-dessous :

1. Synthèse et évaluation quantitative des textes juridiques (1948-2016)

2 Le « secret des correspondances » : un droit dérivé à portée très générale, dépassé par l'évolution technologique

3. L'abondance des textes innovants relatifs à la « protection des données personnelles » depuis 1973

4. L'apport considérable de la jurisprudence européenne sur les données

5. L'ambition du paquet « données » de 2016

6. Le contexte politique de l'adoption du RGPD dans la décennie 2010

7. Les innovations du RGPD en matière de protection des données

8. L'innovation fondamentale du RGPD en matière de responsabilisation des acteurs de la *data*

9. L'application géographique du RGPD européen, étendue au-delà de l'UE

10. L'application matérielle du règlement: la « sécurité nationale » en dehors du champ du RGPD

11. Conclusions (provisoires)

1 Synthèse et évaluation quantitative des textes juridiques (1948-2016)

On a relevé **21 textes** à portée internationale qui sont le résultat de quatre acteurs internationaux : les Nations Unies, l'OCDE, le Conseil de l'Europe et l'UE. Ils ont été rédigés entre 1948 et 2016. Le tableau récapitulatif suivant en donne une photographie :

Tableau 1 : évaluation numérique des textes relatifs au secret des correspondances (SC) et à la protection des données personnelles (PDP)

	SC		PDP		Tot.
	HL	**SL**	**HL**	**SL**	
UN	3	1	0	0	**4**
Council of Europe	1	0	2	2	**5**
EU	2	0	6	0	**8**
OECD	0	0	0	4	**4**
Total	**6**	**1**	**8**	**6**	21
Total général	**7**		**14**		**21**

Sur les **21 textes identifiés**, 7 touchent au secret des correspondances (SC, rédigés entre 1948 et 2002) et 14 à la protection des données personnelles (PDP, rédigés entre 1973 et 2016) :

Tableau 2 : évaluation numérique des textes de *hard law* et de *soft law*

	Hard Law (HL)		Soft Law (SL)		Tot.
	SC	**PPD**	**SC**	**PPD**	
UN	3	0	1	0	**4**
Council of Europe	1	2	0	2	**5**
EU	2	6	0	0	**8**
OECD	0	0	0	4	**4**
Total	**6**	**8**	**1**	**6**	
Total général	**14**		**7**		**21**

Sur les 21 textes identifiés, 14 sont de *hard law* (rédigés entre 1948 et 2016) et 7 de *soft law* (rédigés entre 1973 et 2013). On peut relever qu'en matière de SC la plupart des textes sont de *hard law*, mais on veillera à ne pas en tirer de conclusions hâtives (cf. 2e partie *infra*). Pour ce qui concerne le PDP, il y a un équilibre entre *hard law* et *soft law* : là aussi, il ne faut pas en tirer de conclusion trop rapide (cf. 3e partie *infra*). On peut également constater que la plupart des textes (*soft* ou *hard*) sur le PDP (10 sur 14) sont européens (UE et Conseil de l'Europe). Ceci s'inscrit bien dans le contexte de ce que Z. Laïdi a appelé la « préférence pour la norme »[1] en Europe. On verra que la singularité européenne n'est pas seulement une distinction par le principe de régulation par la norme, mais aussi par le fait qu'il y a un contenu bien spécifique pour la norme, en l'occurrence en matière de données personnelles (cf. 4e, 7e et 8e parties *infra*).

[1]. Cf. Zaki Laïdi, *La Norme sans la force*, Paris, Presses de Sciences-Po, 2013, 304 p.

2 Le « secret des correspondances » : un droit dérivé à portée très générale, dépassé par l'évolution technologique

En 201_, on peut constater qu'entre 1948 et 2002, 7 textes internationaux ont été adoptés sur le « secret des correspondances ». Ils figurent dans le tableau synthétique ci-dessous :

Tableau 3 : tableau synthétique des textes juridiques de droit supra-national sur le « secret des correspondances »

	Date	**Intitulé**	**OIT**
1.	10 décembre 1948	Déclaration universelle des droits de l'homme (DUDH)	ONU
2.	4 novembre 1950	Convention de sauvegarde des droits de l'homme et des libertés fondamentales	ONU
3.	19 décembre 1966	« Pacte international relatif aux droits civils et politiques » (PIDCP)	Conseil de l'Europe
4.	20 novembre 1989	Convention internationale des droits de l'enfant	ONU
5.	20 décembre 1992	Constitution de l'Union internationale des télécommunications (UIT)	ONU
6.	15 décembre 1997	Directive n° 97/66/CE « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications »	UE
7.	12 juillet 2002	Directive n°2002/58/CE « concernant la protection de la vie privée dans le secteur des télécommunications électroniques »	UE

En matière juridique, les approximations n'ont pas - théoriquement, leur place - il est essentiel de regarder en détail ce que disent les textes du secret des correspondances. Le tableau synoptique suivant est l'outil le plus commode pour ce faire.

Tableau 4 : tableau synoptique détaillé des textes juridiques de droit supra-national sur le « secret des correspondances »

Nature de norme		Date	Intitulé du texte	OIT	Principes dominants[2]	Nbre pays ayant ratifié
HL	**1.**	**10 déc. 1948**	**Déclaration universelle des droits de l'homme (DUDH)**	**Nations Unies**		
			- art. 12 : « Nul ne sera l'objet d'immixtions arbitraires dans [….] sa correspondance […] Toute personne a droit à la protection de la loi contre de telles immixtions […] ».		interdiction de l'« immixtion » dans la « correspondance »	
			- art. 19 : « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit »		droit individuel de faire circuler les « informations » et les « idées »	
HL	**2.**	**4 nov. 1950**	**« Convention de sauvegarde des droits de l'homme et des libertés fondamentales »/ « Convention européenne des droits de l'homme » (CEDH)**	**Conseil de l'Europe**		**47**[3]
			- art. 8 al. 1 : « Toute personne a droit au respect de sa vie privée et […] de sa correspondance »		« respect » de la « correspondance »	
			- art. 8 al. 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 […] est nécessaire à la sécurité nationale, à la sécurité publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »		« ingérence » dans la correspondance sous condition de légalité et de nécessité	
HL	**3.**	**19 déc. 1966**	**« Pacte international relatif aux droits civils et politiques » (PIDCP)**	**Nations Unies**		**168**

2 . Les guillemets signalent les extraits du texte original.

3 . http://www.coe.int/fr/web/conventions/search-on-treaties/-/conventions/treaty/005/signatures?p_auth=Yjnj91md

			- art. 17, alinéa 1 : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans […] sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ».		interdiction de l'« immixtion » dans la « correspondance »	
HL	**4.**	**20 nov. 1989**	**Convention internationale des droits de l'enfant**	**Nations Unies**		**192**[4]
			- art. 16, al. 1 : « Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa […] correspondance »		interdiction de l'« immixtion » dans la « correspondance » de l'enfant	
			- art. 16, al. 2 : « L'enfant a droit à la protection de la loi contre de telles immixtions [...] »			
SL	**5.**	**20 déc. 1992**	**Constitution de l'Union internationale des télécommunications (UIT)**	**Nations Unies**		**193**
			-art. 33 : " Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference"		« droit » individuel de correspondre	
			- art. 34 : **«** Member States reserve the right to stop, in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or any part thereof, except when such notification may appear dangerous to the security of the State"		« droit » des États d'interrompre l'acheminement d'un télégramme sous condition	
HL	**6.**	**15 décembre 1997**	**directive n° 97/66/CE « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications »**	**UE**		**28**

[4]. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&clang=_fr

			- art. 5 : « 1. Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, paragraphe 1 »		États doivent garantir la « confidentialité des communications »	
			- art. 14 : « 1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 5 et 6 et à l'article 8 paragraphes 1 à 4 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de télécommunications, comme le prévoit l'article 13 paragraphe 1 de la directive 95/46/CE ».		Droit des États de « limiter » la confidentialité sous condition de légalité et de nécessité	
HL	**7.**	**12 juillet 2002**	**directive n°2002/58/CE « concernant la protection de la vie privée dans le secteur des télécommunications électroniques »**	**UE**		**28**
			art. 5 : « 1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public […] En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1 »		États doivent garantir la « confidentialité des communications »	

			- art. 15 : « 1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE »		Droit des États de limiter la confidentialité sous condition de légalité, nécessité et proportionnalité	

Sur les 7 textes relatifs au SC, la grande majorité (6) est de *hard law,* un seulement relève du *soft law*. L'ancienneté des textes est également manifeste, en comparaison avec ceux relatifs aux données (cf. 3e partie *infra*). Ces deux caractéristiques induisent l'idée d'un corps de doctrine juridique ancien et comme tel appliqué.

La réalité est en fait bien différente. Les organisations internationales qui ont porté ces textes, notamment les Nations Unies, n'ont pas pu ou voulu pour autant mettre en place des cadres juridictionnels permettant d'en assurer le respect à l'échelle internationale. Qui plus est, la forme juridique prise par le SC indiquée dans le tableau est très spécifique. Il apparaît en effet nettement que, depuis le texte fondateur de 1948 la notion de SC n'a pas été enrichie - à la différence de celle touchant aux données, ainsi qu'on le verra plus loin. Les textes postérieurs à la DUDH de 1948 se sont contentés d'en rappeler la portée pour une catégorie particulière de population (enfants, 1989), d'en rappeler le principe pour un espace juridique particulier (Conseil de l'Europe, 1950) ou d'en dire l'appartenance à la catégorie des droits humains (PIDCP-NU, 1966). Pour chaque texte postérieur, les termes sont identiques ou très analogues sans qu'il y ait d'innovation. Ceci s'explique en fait par la nature et le développement historique du SC. Le « secret des correspondances » est en effet une innovation juridique des XVIIIe et XIXe siècles. C'est à cette époque qu'il est devenu l'un des piliers des ordres juridiques nouveaux établis dans les régimes libéraux ou en voie de libéralisation, en entrant dans les déclarations des droits ou les *bill of rights*. Le SC a alors été utilisé comme une revendication contre l'arbitraire des pratiques étatiques violant ce qui n'était pas encore appelé la « vie privée ». Le tableau 4 indique nettement à notre sens le caractère très général du SC. Ceci est lié au fait **qu'il doit être rapproché des droits fondamentaux, tels que la liberté d'opinion et de pensée dont il est** en fait **un des moyens d'expression**. Le SC est un **outil de mise en œuvre** de libertés fondamentales qui ont été au cœur de la révolution libérale. Le SC est d'ailleurs un « droit à », en l'occurrence un droit au respect du secret de ses correspondances.

Il faut aussi relever que les textes postérieurs à la déclaration fondatrice de 1948 qui faisait entrer le SC dans le droit international public ont veillé à affirmer le **droit des États à limiter** ce SC qui n'est dès lors qu'un **droit** individuel **relatif** mis en concurrence avec des impératifs d'État lui permettant de s'ingérer dans le SC (ou de l'interrompre) sous condition de légalité et de nécessité. Relevons au passage que cette disposition de « mise en balance » des droits est très classique en droit interne dans les démocraties libérales. Du point de vue du droit international qui nous intéresse exclusivement dans ce livrable, il faut relever que les textes du Conseil de l'Europe (1950), des Nations-Unies/UIT (1992) et de l'Union européenne (1997) ne définissent pas les cas de nécessité, ce qui témoigne – sans surprise – du respect par les organisations internationales d'**une disposition cardinale de la souveraineté de l'État qui est de fixer les limites de sa propre limitation.**

En fait le SC mis en avant par les organisations internationales après 1945 est **un droit dérivé lié à un principe fondamental très ancien qui perd en applicabilité ce qu'il a gagné par sa formulation très généra**le. Il faut enfin relever que le SC a été pensé dans un contexte des technologies de l'information stable où la « correspondance » renvoyait uniquement aux communications par voie postale. Le SC a été appliqué aux découvertes postérieures, au XIXe siècle, du télégraphe (1837) et du téléphone (1876). Mais l'entrée dans l'ère des communications individuelles hertziennes (téléphone mobile) puis numériques (courriels, VOD) a rendu rapidement obsolète la notion de « correspondance ». Ceci a été constaté par exemple en France où la loi de 1991 sur les interceptions de sécurité a été à l'origine d'ambiguïtés – constatées par des juridictions – sur le fait qu'elle couvrait ou non les communications hertziennes (discussion autour de l'article 20). La loi dite « renseignement » de 2015 a d'ailleurs veillé à adapter le droit aux technologies nouvelles. Il est fortement improbable qu'un nouveau texte international sur le SC voie le jour. Enfin, on relèvera que le principe du secret des correspondances est absent du texte du RGDP (2016) européen - y compris dans la longue liste des 173 considérants.

On relèvera enfin que les Nations Unies n'ont pas adopté de texte fondamental sur les

données personnelles, ce qui peut soit refléter les intenses divergences sur le sujet entre les membres de la communauté internationale, soit le fait que c'est à un organisme subordonné, l'Internet Governance Forum (IGF) que cette tâche ait été confiée. Nous reviendrons sur ce point dans le cadre du livrable 8.

3 L'abondance des textes innovants relatifs à la « protection des données personnelles » depuis 1973

Le RGPD adopté en mai 2016 sera le fondement du droit des données dans l'ensemble des 28 pays membres de l'UE à partir de mai 2018. Il s'appliquera également au-delà de l'UE (cf. 6e partie). Cependant **l'état du droit actuel est une sédimentation de textes anciens et entièrement nés en dehors de l'UE**. Cette recherche montre par ailleurs nettement qu'**une grande partie du droit des données actuel date du début des années 1970** et qu'**il n'y a eu qu'une innovation relative par la suite**.

Ainsi les premiers textes constituant la base du droit des données personnelles datent de **1973** et ont été élaborés dans la cadre du **Conseil de l'Europe**, institution née en 1949 avec pour objectif la protection des libertés fondamentales et de la démocratie. Une grande partie des principes fondamentaux entièrement validés par le nouveau RGPD de 2016-2018 datent en effet de 1973 : principe de finalité, catégories de données sensibles, droit d'accès des personnes…etc. L'OCDE a ensuite prolongé à partir de 1980 les principes fondamentaux du Conseil de l'Europe et les a développé, notamment en matière de « flux de données transfrontières ». L'Europe, alors « Communauté européenne » n'a adopté un premier texte relatif aux données personnelles qu'en 1995, un texte largement sous influence de ceux produits par les organes qui l'avaient devancé.

A titre de bilan, on peut relever l'existence de **14 textes qui ont créé le droit des « données personnelles » entre 1973 et 2016**. Il est possible de synthétiser ces strates temporelles et la diversité des institutions partie prenante dans le tableau 10 *infra*.

3.1 Le rôle fondateur sur la définition des « données » du Conseil de l'Europe en 1973-1974

Il est important de relever que c'est une assemblée européenne distincte de l'UE et de la CEE qui est à l'origine à la fin des années 1960 des premières initiatives en matière de droit des données personnelles dont le résultat est l'adoption en 1981 (convention 108) du texte de *hard law* le plus protecteur au monde pour les données. Depuis et jusqu'en 2016 (RPGD) l'Europe (en l'occurrence l'UE) a conservé cette avancée dans le monde.

C'est l'assemblée parlementaire du Conseil de l'Europe qui a demandé en 1968 au comité des ministres de déterminer si la convention de 1950 (cf. 2e partie supra) suffisait à protéger le droit à la vie privée face à la « science moderne », ceci devant s'entendre comme les progrès de l'informatique et des bases de données, principal enjeu ayant favorisé l'objectivation de l'enjeu informatique dans les sociétés européennes[5]. Cinq années plus tard, le comité des ministres du Conseil de l'Europe adoptait deux résolutions relatives à la protection de la vie privée des personnes physiques vis-à-vis des « banques de données électroniques » (*i.e* : base de données) respectivement dans le secteur privé (résolution n° 73-22 du 26 septembre 1973)[6] et dans le secteur public (résolution n° 74-29 du 20 septembre 1974).

Ces deux textes de *soft law* ont établi tous les principes fondamentaux en matière de protection des données, repris ensuite soit dans le droit national - notamment dans les lois fondatrices suédoises (1973), allemandes (1976), françaises (1978) et luxembourgeoises (1979)

5. Au début de l'année 1978, Simon Nora et Alain Minc publiaient : *L'informatisation de la Société. Rapport à M. le Président de la République*, Paris, La Documentation française, 1978, devenu ensuite un best-seller. Cf. André Vitalis, *Informatique, pouvoir et libertés*, Paris, Economica, « Politique comparée », 1981, 212 p., issu d'une thèse soutenue en 1979.

6. Résolution n° 73-22 du Comité des ministres du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé », p. 73-74

– **soit dans le droit supra-national/international**, ainsi qu'on va le voir *infra***.**

La résolution n° 73-22 s'achevait par la formulation de **« bonnes pratiques » avant l'heure** sous forme de 10 recommandations adressées aux gouvernements des pays membres du Conseil de l'Europe, détaillées dans le tableau ci-dessous.

Tableau 5 : les « bonnes pratiques » du Conseil de l'Europe en 1973 en matière de données

NB : dans la première colonne figure le n° de recommandation tel qu'il apparaît dans le texte originel. Nous laissons de côté les recommandations qui n'ont pas de relation directe ou indirecte avec les normes développées par la suite. Les passages en gras sont de nous, soulignant la précocité des principes fondamentaux dégagés par le Conseil de l'Europe.

1.	« Les informations enregistrées doivent être **exactes** et **tenues à jour**. Les informations concernant **l'intimité** des personnes ou celles pouvant être à la **source** de **discrimination ne doivent pas**, en règle générale, **être enregistrées**, ou du moins **diffusées** »
2.	« Les informations doivent être **adéquates** et **pertinentes** par rapport à la **finalité recherchée** »
3.	« Les informations **ne** doivent **pas être obtenues** par des moyens frauduleux et **déloyaux** »
5.	« Les **informations** ne **peuvent**, sans autorisation appropriée, **être utilisées** à **d'autres fins que celles pour lesquelles elles ont été enregistrées**, ni communiquées à des tiers »
6.	« En règle générale, la **personne** concernée a le **droit de connaître les informations** enregistrées sur elle, la fin pour laquelle les informations ont été stockées et les communications effectuées »
7.	« Toute diligence doit être faite pour **corriger** les **informations inexactes** et pour **effacer** les informations **périmées** ou obtenues de façon **illicite** »
10.	« Les **données** d'ordre **statistique** ne pourront être **diffusées que sous une forme agrégée** et de manière qu'il soit **impossible** de les **attribuer** à une **personne** déterminée »

On remarquera que les expressions de « traitement de données » ou de « données » ne figuraient pas encore dans le texte de 1973 malgré le terme de « banque de données » employé dans le titre. A l'époque c'est le terme, non spécifique, « d'informations » qui en tenait lieu. Il est aussi nécessaire de relever qu'aucune exception ou réserve à ces principes pour des motifs tels que la sécurité nationale ou l'ordre public ne figurait dans la résolution.

La résolution complémentaire n° 74-29 du 20 septembre 1974[7] avait pour objet la même matière, les « informations » sur des personnes privées collectées par des « banques de données » publiques cette fois. Elle s'achevait par 8 recommandations aux gouvernements. Les recommandations 2 à 5 étaient directement issues du texte adopté l'année précédente, avec une formulation partiellement nouvelle qui fut reprise dans tous les textes postérieurs.

7. Résolution n° 74-29 du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public », p. 87-88.

Encadré 1 : les « bonnes pratiques » du Conseil de l'Europe en 1974 en matière de données

NB : Les passages en gras sont de nous.

« 2. Les informations enregistrées doivent être[8] :
a. **obtenues** par des **moyens licites** et **loyaux**,
b. **exactes** et **tenues à jour**,
c. **adéquates** et **pertinentes par rapport** à la **finalité recherchée**
toute **diligence** doit être faite **pour corriger** les informations **inexactes** et pour **effacer** les informations **inadéquates**, **non pertinentes** ou **périmées**
3. Particulièrement lorsque des banques de données électroniques traitent des informations concernant l'intimité de la vie privée des personnes, ou lorsque le traitement des informations peut être à l'origine de discriminations,
a. leur **création** doit être **prévue par la loi** ou par une réglementation spéciale ou leur **existence** doit **être rendue publique** dans une déclaration ou un document, en conformité avec le système juridique de chaque État membre ;
b. ces lois, réglementation, déclaration ou document doivent **préciser** la **finalité** de **l'enregistrement** et de l'utilisation de telles informations ainsi que les conditions dans lesquelles elles peuvent être communiquées
c. les **informations** enregistrées ne doivent **pas** être **utilisées** à **d'autres fins que celles qui ont été définies**, à moins qu'une dérogation ne soit expressément autorisée par la loi ou accordée par une autorité compétente ou que les règles régissant l'utilisation de la banque de données électroniques ne soient modifiées
4. Des **règles** doivent être **établies** pour déterminer le **délai au-delà** duquel **certaines catégories d'informations ne pourront plus être conservées ou utilisées**
5. Chaque **personne** a le **droit de connaître** les **informations** enregistrées **sur elle** »

Il suffit de comparer les recommandations des textes de 1973 et 1974 avec le cœur de la convention 108 adoptée le 28 janvier 1981 par le Conseil de l'Europe pour prendre la mesure que les premiers ont été la matrice de la seconde et ce faisant de tout le droit des données par la suite.

Encadré 5 : les « principes de bases » de la convention du Conseil de l'Europe de 1981 en matière de données

Chapitre II – Principes de base pour la protection des données
[...]
« Article 5 – Qualité des données
Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:
a obtenues et traitées loyalement et licitement;
b enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;
c adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;
d exactes et si nécessaire mises à jour;
e 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. »

L'importance du texte du 21 janvier 1981 – dont l'appellation complète est : « Convention

[8]. *Ibid.*, p. 88.

européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », souvent résumée en « convention 108 » - tient au fait que ce n'était plus du *soft law* mais une « convention » de portée internationale supposant une ratification nationale et contraignante pour les États. Ce texte ramassé de 27 articles portant exclusivement sur ce qui était désigné comme « données » est **le premier texte de droit international sur la protection des données personnelles, élaboré dans le cadre du continent européen** mais aujourd'hui ratifié au-delà. En 2018, 51 États (dont la Russie) l'ont ratifié et 3 États africains (Tunisie, Sénégal et Maurice).

La « convention 108 » a été complétée par un « protocole additionnel » du Conseil de l'Europe le 13 novembre 2001 comprenant trois dispositions nouvelles importantes :

- la nécessité de création d'une autorité nationale de contrôle en matière de données,
- l'interdiction des flux transfrontières de données dans un pays n'assurant pas le même niveau de protection[9],
- et une disposition très importante, le fait d'accepter des exceptions aux principes fondamentaux « lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants »

Tableau 6 : tableau synthétique des textes du Conseil de l'Europe sur la protection des données

	Date	OIT	Intitulé	Nature du texte
1.	26 sept. 1973	Comité des ministres - Conseil de l'Europe	Résolutions 73-22 « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques respectivement dans le secteur privé »	SL
2.	20 sept. 1974	Comité des ministres - Conseil de l'Europe	Résolutions 74-29 « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques respectivement dans le secteur public »	SL
3.	28 janv. 1981	Conseil de l'Europe	« Convention 108 » : « Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »	HL
4.	13 nov. 2001	Conseil de l'Europe	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	HL

On constate donc que le *soft law* a été déterminant pour la création des grands principes du droit des données. Tout ce qui vient d'être abordé plus haut pour la période allant jusqu'en 1981 était relatif aux données, indépendamment de la question de leur mobilité.

[9]. Principe faussement nouveau car situé dans le droit fil des Lignes directrices de l'OCDE de 1980, cf. *infra.*

3.2 Les grands principes des « flux » de données fixés par l'OCDE en 1980

L'enjeu des flux de données d'un pays à un autre a été abordé pour la première fois dans le cadre de l'OCDE et c'est dans ce cadre que les principes fondamentaux en la matière ont été adoptés au début des années 1980. Sur ce point encore le *soft law* a été dominant. Dans le cadre de cette organisation - dont la finalité est exclusivement économique – ce sont des groupes d'experts et non pas des élus ou des commissaires, ni fonctionnaires nationaux dotés d'une mission qui ont défini les fondements ce qui a été appelé à l'époque les « flux transfrontières ».

Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel* ont été adoptées par l'OCDE le 23 septembre 1980. Elles comprennent 4 recommandations puis en annexe des « lignes directrices », comprenant elles-mêmes 8 « principes fondamentaux » au plan national et 4 « principes fondamentaux » au plan international. On retrouve dans ces principes l'apport initial des textes du Conseil de l'Europe de 1973 et 1974 (cf. *supra*), mais pas seulement. En l'état des rares travaux historiques existant sur le sujet il apparaît que ce sont les États-Unis qui ont pris l'initiative au sein de l'OCDE en 1979 pour que soit discutée la question des flux transfrontières[10] dans le cadre d'un groupe de travail qui avait été créée au début de l'année 1978. Le groupe d'experts, s'appuyant très manifestement sur le travail antérieur du Conseil de l'Europe (cf. tableau 7 *infra*), a remis son texte rapidement (juillet 1979)[11]. Il semble cependant que les tensions aient été très vives au sein du groupe entre la vision des États-Unis et celle des experts européens. Les *Lignes directrices* de 1980 qui en furent issues étaient bâties autour de la volonté de concilier la protection de la vie privée dans l'esprit des textes européens et la libre circulation des données s'inscrivant dans une démarche économiquement libérale. Les États-Unis percevaient le droit des données européen embryonnaire, mais nous l'avons vu très complet, comme un obstacle protectionniste au « free flow of information » risquant d'entraver la conquête de futurs marchés pour leur industrie informatique très dominante. La vision des États-Unis transparait dans le 4e et dernier principe fondamental figurant dans le tableau 7 *infra*.

Il est nécessaire de relever aussi que c'est dans ce même texte OCDE que l'on voit la première formulation d'exceptions pour les États aux règles de protection des données pour des motifs précis, « souveraineté nationale, la sécurité nationale et l'ordre public » (p. 10), ces exceptions devant être « aussi peu nombreuses que possible » et « portées à la connaissance du public ».

10. Arthe Van Laer, « Transmission électronique des données : la Communauté européenne face au Big Brother américain (1976-1981) », in: Patrick Fridenson et Pascal Griset (dir.), *Entreprise de haute technologie, État et souveraineté depuis 1945*, Paris, Comité pour l'histoire économique et financière de la France, 2010, p. 308.
11. *ibid*, p. 309.

Tableau 7 : les principes fondamentaux des « flux transfrontières de données » selon l'OCDE en 1980

Principes fondamentaux nationaux	
1.	« principe de la limitation en matière de collecte »
2.	« principe de la qualité des données »
3.	« principe de la spécification des finalités »
4.	« principe de la limitation de l'utilisation »
5.	« principe des garanties de sécurité »
6.	« principe de la transparence »
7.	« principe de la participation individuelle »
8.	« principe de la responsabilité »
Principes fondamentaux internationaux	
1.	réexportation des données
2.	« libre circulation sans interruption et en toute sécurité »
3.	motifs de limitation : 1. si la réexportation des données permet de contourner la législation sur la protection de la vie privée et des libertés individuelles. 2. s'il n'y a pas de protection équivalente à celle du pays étranger
4.	pays membres doivent éviter d'édicter des lois qui sous couvert de protection de la vie privée créeraient des obstacles à la circulation des données

Les textes postérieurs de *soft law* de l'OCDE (1985, 1998 et 2013) se sont inscrits dans la lignée de l'hyper-texte de 1980 sans nouveauté véritable.

Tableau 8 : tableau synthétique des textes de l'OCDE sur la protection des données

	Date	**Intitulé**	**Nature du texte**
1.	23 sept. 1980	Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel,	SL
2.	11 avril 1985	Déclaration sur les flux transfrontières de données	SL
3.	1998	Déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux, DSTI-ICCP-REG(98)10-FINAL-FRE	SL
4.	2013	Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data	SL

3.3. Le suivisme de l'UE : la directive de 1995

Tableau 8 : tableau synthétique des textes de l'UE sur la protection des données

	Date	Intitulé du texte	Nature
1.	24 octobre 1995	Directive UE 95/46/CE « 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 »	HL
2.	7 décembre 2000	Charte des droits fondamentaux de l'Union européenne	HL
3.	12 juillet 2002	Directive n°2002/58/CE « concernant la protection de la vie privée dans le secteur des télécommunications électroniques » (« directive vie privée et communications électroniques »	HL
4.	27 avril 2016	Règlement 2016/679 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 (« RGPD »)	HL
5.	27 avril 2016	Directive 2016/680 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 détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénale la libre circulation de ces données	HL
6.	27 avril 2016	Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes grav criminalité, ainsi que pour les enquêtes et les poursuites en la matière	HL

Le premier texte adopté par l'UE en matière de données a été la directive UE 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 ». Cette directive s'est bien évidemment appuyée très largement sur l'ample réflexion antérieure du Conseil de l'Europe et de l'OCDE (abordée *supra*). Le caractère très tardif de l'adoption de la directive doit être expliqué. En effet, en juin 1976 – alors que plusieurs États Membres s'étaient dotées de lois en matière d'informatique (avec une composante sur les données) ou étaient en train de le faire – la commission européenne avait réuni un groupe d'experts « informatique et protection des libertés » au sein duquel Louis Joinet représente la France. Le groupe de travail acheva rapidement ses travaux en janvier 1977 sans conclure, la commission estimant que le Traité de Rome (1957) ne lui donnait pas assez de pouvoirs pour adopter une directive sur le sujet[12]. Le parlement européen prit une initiative quelques années plus tard, en adoptant en mai 1979 un rapport « sur l'informatique et les droits de la personne » contenant une résolution sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique » totalement inspirés des textes de *soft law* du Conseil de l'Europe.

La directive 95/46 a été le premier texte de l'UE, un texte de *hard law* qui plus est, supposant l'obligation pour les États Membres de le transférer dans leur droit national. Ce texte assez bref (72 considérants, 32 articles) s'appuyait très largement sur la convention 108 (1981) du Conseil de l'Europe et ce explicitement dans son 11e considérant[13]. Disposition centrale de la directive, **l'article 6 définissant les données reprenait quasiment mot pour mot l'article 5 de la convention 108**. Finalement, la seule innovation tenait au fait que la directive rappelait – avec dix ans d'avance sur l'article 4 du traité de Lisbonne[14] - que les États pouvaient déroger aux

12. *Ibid*, p. 300.

13. (11e) « considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel; »

14. « L'union respecte l'égalité des États membres devant les traités ainsi que leur identité nationale, inhérentes à leurs structures fondamentales politiques et constitutionnelles, y compris en ce qui concerne l'autonomie locale et régionale. Elle respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre ». C'est nous qui soulignons.

dispositions très protectrices du texte en cas « d'intérêt public important » (*sic*), de sauvegarde de la « sûreté de l'État », de la « défense » et de la « sécurité publique » (articles 8 et 13). Ces clauses d'exception avaient fait leur apparition dans les *Lignes directrices* de l'OCDE de 1980 (cf. *supra*) : elles étaient pour la première fois transposées dans le droit européen. La directive 2002/58/CE « vie privée et communications électroniques » adoptée par la suite (en 2002) rappela l'équilibre entre protection des données et le droit des États de la limiter dans une terminologie qui est demeurée ensuite très stable **« lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée »**[15]**.**

Néanmoins, si ces dispositions témoignaient de la limitation de l'auto-contrainte des États Membres, la perspective dominante de l'UE était clairement libérale en matière de données. La « Charte des droits fondamentaux » de l'UE adoptée en 2000 était très claire à cet égard : en son article 8 elle synthétisait le « droit » individuel à la protection de ses données et en rappelait la portée (loyauté, respect des finalités, consentement, droit d'accès), **sans mentionner la possibilité de les limiter**. Avec ce texte l'UE s'est dotée d'une déclaration des droits adaptée au monde numérique sans plus dépendre sur le plan des grands principes de la convention 108 du Conseil de l'Europe (qui demeurait toutefois beaucoup plus précise).

15. Sur ce point, cf. le tableau 12 *infra*.

Tableau 10 : tableau synoptique détaillé des textes de droit international sur la protection des données

Type de norme		Date	Intitulé du texte	OIT	Principes dominants[16]	Appellation contemporaine des principes	Nbre pays ayant ratifié
SL	**1.**	**26 septembre 1973**	**Résolution n° 73-22 du Comité des ministres du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé**	**Conseil de l'Europe**			**47 Etats membres**
			recommandations aux gouvernements :				
					« informations […] doivent être exactes et tenues à jour »	Responsabilité de l'exactitude et de la mise à jour des informations	
					« informations concernant l'intimité des personnes » ne doivent pas être enregistrés ou diffusées		
					pas de recours à des « moyens frauduleux et déloyaux » pour obtenir des informations	Loyauté de la collecte	
					informations doivent être « utilisées » pour les fins pour lesquelles elles ont été enregistrées	respects de finalités de collecte par l'utilisateur	
					informations ne doivent pas être communiquées à des tiers	Principe de confidentialité	
					personne « a le droit de connaître les informations » le concernant « en règle générale »	Droit d'accès	
					informations inexactes doivent être corrigées avec « diligence »		
					informations « périmées » doivent être « effacées »		
					informations « obtenues de façon illicite » doivent être « effacées »		

16. Les guillemets signalent les extraits du texte original.

					« Des règles doivent être établies pour déterminer le délai au-delà duquel certaines catégories d'informations ne pourront plus être conservées ou utilisées »		
					« Chaque personne a le droit de connaître les informations enregistrées sur elle »		
SL	**2.**	**20 septembre 1974**	**Résolution n° 74-29 du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public »**	**Conseil de l'Europe**			**47 Etats membres**
			recommandations aux gouvernements :				
					informations doivent être « obtenues par des moyens licites et loyaux, exactes et tenues à jour, adéquates et pertinentes par rapport à la finalité recherchée »	Licéité et loyauté de la collecte	
					« diligence doit être faite pour corriger les informations inexactes et pour effacer les informations inadéquates, non pertinentes ou périmées »		
					lorsque l'intimité est concernée la création du traitement doit être « prévue par la loi ou par une réglementation spéciale » et rendue publique. La « finalité » doit être précisée ainsi que les conditions de communications		
					« informations enregistrées ne doivent pas être utilisées à d'autres fins que celles qui ont été définies, à moins qu'une dérogation ne soit expressément autorisée »	Respect par l'utilisateur de la finalité du traitement	
SL	**3.**	**23 septembre 1980**	**Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel**	**OCDE**			**34 Etats membres**

			définition des « flux transfrontières de données »				
			fixation de 8 « principes fondamentaux » au plan national et 4 au plan international				
			8 « principes fondamentaux » au plan national » :	1. « principe de la limitation en matière de collecte » : « obtenue par des moyens licites et loyaux »			
					2. « principe de la qualité des données »		
					3. « principe de la spécification des finalités »		
					4. « principe de la limitation de l'utilisation »		
					5. « principe des garanties de sécurité »		
					6. « principe de la transparence »		
					7. « principe de la participation individuelle »	= droit d'accès	
					8. « principe de la responsabilité »		
			4 « principes fondamentaux au plan international » :				
					« libre circulation » […] « sans interruption et en toute sécurité »		
					pays membre ne doit pas « limiter » les flux de données sauf si l'autre pays membre ne se conforme pas à crs lignes directrices		
					Pays membre peut imposer des « restrictions à l'égard de certaines données » s'il n'y a pas de « protection équivalente » à sa « législation interne » dans l'autre pays membre		
					pays membres doivent éviter d'édicter des lois qui, sous couvert de protection de la vie privée, créeraient des obstacles à la circulation des données		

HL	**4.**	**28 janvier 1981**	**Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel**	**Conseil de l'Europe**		= convention 108	**47**
			:		- art. 1er : « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou 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») ».		
			« principes de base pour la protection des données »	« Article 5 – Qualité des données Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:			
					« a : obtenues et traitées loyalement et licitement » ;	- loyauté et licéité de la collecte	
					« b : enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités » ;	- existence et légitimité des finalités	
					« c : adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » ;	- respect des finalités	
					« d : exactes et si nécessaire mises à jour »	- exactitude et mise à jour des données	

					« e : 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. »	- établissement d'un délai de conservation	
SL	**5.**	**11 avril 1985**	**Déclaration sur les flux transfrontières de données**	**OCDE**			**34 Etats membres**
			- La protection de la vie privée sur les réseaux a fait « d'importants progrès » - Encourage le développement des flux transfrontières à portée marchande afin de favoriser le développement du commerce international.				
SL	**6.**	**7-9 octobre 1998**	**Déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux**	**OCDE**			**34 Etats membres**
					« Considérant que pour accroître la confiance dans les réseaux mondiaux, les utilisateurs et consommateurs ont besoin d'avoir des assurances quant au caractère loyal de la collecte et du traitement des données personnelles les concernant [...] »	Loyauté de la collecte et du traitement	
					« Considérant que le recueil et la manipulation de données à caractère personnel devraient s'effectuer dans le dû respect de la vie privée »	Respect de la vie privée	
					« encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée »		
HL	**7.**	**7 décembre 2000**	**Charte des droits fondamentaux de l'Union européenne**	**UE**			**28**
					Art. 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ».		

					« 2. 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. »	- loyauté du traitement - consentement au traitement - droit d'accès - droit de rectification	
					« 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante »	- contrôle par une autorité indépendante	
HL	**8.**	**13 novembre 2001**	**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**	**Conseil de l'Europe**			**37**[17]
					- art. 1er : nécessité d'une autorité de contrôle en matière de données		
					- art. 2, al. 1 : « […] le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet État ou cette organisation assure un niveau de protection adéquat pour le transfert considéré »		
					- art. 2, al. 2 : exception possible « lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants »		

17 . https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=RoNkbHZg

SL	**9.**	**2013**	**Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data**	**OCDE**			**34 Etats membres**
					- art. 4 : exceptions aux guidelines pour « national sovereignty », « national security », « ordre public » (*sic*) doivent être limitées et connues du public		
					- art. 7 : « collection limitation principle »		
					- art. 8 : « data quality principle »		
					- art. 9 : « purpose specification principle »		
					- art. 10 : « use limitation principle »		
					- art. 11 : « security safeguards principle »		
					- art. 12 : « openness principle »		
					- art. 13 : « individual participation principle »	droit d'accès	
					- art. 14 et 15 : nécessité d'un data controller		
					- art. 17 : transborder flows of data si pays offrent des garanties suffisantes pour les données		
HL	**10.**	**27 avril 2016**	**Règlement (UE) 2016/679 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**	**UE**			**28**
			abroge la directive 95/46/CE				
HL	**11.**	**27 avril 2016**	**Directive 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**	**UE**			**28**

			abroge la décision-cadre 2008/977/JAI du Conseil				
HL	**12.**	**27 avril 2016**	**Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière**	**UE**			**28**

Tableau 11 : tableau de synthèse des textes de droit international relatifs à la protection des données personnelles (PDP)

	Date	Intitulé du texte	OIT
1.	26 septembre 1973	Résolution n° 73-22 du Comité des ministres du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques à-vis des banques de données électroniques dans le secteur privé	Conseil de l'Europe (1)
2.	20 septembre 1974	Résolution n° 74-29 du Conseil de l'Europe « relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public »	Conseil de l'Europe (2)
3.	23 septembre 1980	Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel	OCDE (1)
4.	28 janvier 1981	Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel	Conseil de l'Europe (3)
5.	11 avril 1985	Déclaration sur les flux transfrontières de données	OCDE (2)
6.	24 octobre 1995	Directive UE 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 »	UE (1)
7.	7-9 octobre 1998	Déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux	OCDE (3)
8.	7 décembre 2000	Charte des droits fondamentaux de l'Union européenne	UE (2)
9.	13 novembre 2001	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	Conseil de l'Europe (4)
10.	12 juillet 2002	Directive n°2002/58/CE « concernant la protection de la vie privée dans le secteur des télécommunications électroniques » (« dire vie privée et communications électroniques »)	UE (3)
11.	2013	Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Dat	OCDE (4)
12.	27 avril 2016	Règlement (UE) 2016/679 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 - RGPD	UE (4)
13.	27 avril 2016	Directive 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 donn	UE (5)
14.	27 avril 2016	Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passa (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes e poursuites en la matière	UE (6)

4 L'apport considérable de la jurisprudence européenne sur les données

En **droit du Conseil de l'Europe**[18]**,** tout comme en **droit de l'Union européenne**[19] **(UE)**, les « données à caractère personnel » sont définies comme des **« informations concernant une personne physique identifiée ou identifiable »,** c'est-à-dire des informations sur une personne dont l'identité est manifestement claire ou peut au moins être établie par l'obtention d'informations complémentaires[20]. Si les deux principales organisations régionales du continent européen prennent en compte la question de la protection des données, qui plus est en se basant sur des définitions équivalentes, il faut néanmoins souligner trois difficultés qui structurent cette 4e partie :
- La première concerne l'appréhension de la question au niveau du Conseil de l'Europe. En effet, si ce dernier s'est doté d'une convention spéciale relative à la protection des données – la Convention 108 – il n'appartient pas à la Cour européenne des droits de l'Homme d'en connaitre le contentieux. La Cour de Strasbourg est en effet en charge de l'interprétation et de la résolution des différends autour de la Convention européenne des droits de l'Homme[21]. Or cette dernière ne consacre pas explicitement de droit à la protection des données à caractère personnel (à la différence du secret des correspondances, cf. 2e partie *supra*). C'est donc de façon prétorienne que le juge de la CEDH a dû assurer la protection de ce droit, aujourd'hui source d'une jurisprudence fournie[22] (cf. 4.1. *infra*).
- Une seconde difficulté est liée à la question de la protection des données au sein de l'UE. En effet, le droit à la protection des données à caractère personnel étant un **droit fondamental, il convient de l'articuler avec l'objectif premier de l'intégration communautaire, à savoir la réalisation d'un marché intérieur** (cf. 5e partie *infra*). Or l'argument de la protection des données pourrait être avancé comme un frein, une entrave à cette réalisation. Il s'agit là d'un défi classique pour l'UE, mais elle doit assurer un équilibre entre droits fondamentaux et libertés économiques fondamentales (cf. 4.2.).
- La troisième, plus classique, concerne l'articulation de ces deux protections en matière de données à caractère personnel. En effet, la CJUE et la CEDH opérant sur un même territoire pour 31[23] des 47 États concernés, il convient d'éviter tout conflit d'interprétation de ce droit (cf. 4.3.).

4.1 L'apport décisif de la jurisprudence de la Cour européenne des droits de l'Homme (CEDH)

Comme présenté ci-dessus, le droit à la protection des données à caractère personnel n'est pas explicitement consacré par la ConvEDH. Ceci s'explique par le contexte historique de la réalisation de ce texte. Bien naturellement, il n'était pas encore question d'enjeux numériques au sortir de la Seconde Guerre mondiale. Les auteurs du texte n'ont donc pas pu prévoir ce droit. C'est pourquoi une seconde convention, spéciale, a été rédigée en 1980. Une autre piste aurait pu être suivie : l'ajout d'un nouveau protocole relatif à la protection des données. Mais, par souci de flexibilité sans doute – la révision de la ConvEDH n'étant pas simple à mener à terme – il a été préféré la rédaction d'un nouveau texte.

Dès lors, la CEDH a pu voir en cette nouvelle Convention 108, une source d'inspiration pour sa jurisprudence. Mais encore fallait-il trouver un moyen de rattacher cette question de la protection des données à caractère personnel au texte de la ConvEDH, sans quoi, il aurait été contestable pour le

[18] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n° 108, signée à Strasbourg le 28 janvier 1981, (ci-après « Convention 108 »).
[19] 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), (ci-après « RGPD »).
[20] Pour la Convention 108 : Art. 2, point a) ; Pour le RGPD : Art. 4, 1).
[21] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, STCE n° 005, signée à Rome le 4 novembre 1950, (ci-après ConvEDH).
[22] Voir en annexe le tableau 13 de la jurisprudence de la CEDH en matière de protection des données.
[23] 28 États membres de l'UE auxquels viennent s'ajouter 3 États de l'Association européenne de libre-échange (AELE) membres de l'Espace Economique Européen (EEE) que sont la Norvège, l'Islande et le Liechtenstein (cf. 9e partie *infra*).

juge de Strasbourg de se l'approprier. C'est ainsi que la CEDH eut recours à une technique classique d'interprétation, celle du « droit vivant » dégagé dans son arrêt *Airey c. Irlande* en 1979[24] où le juge explique que la ConvEDH « doit se lire à la lumière des conditions de vie d'aujourd'hui ». Il s'agit encore une fois d'éviter les lourdeurs d'une révision par protocole additionnel et de faire en sorte que le texte de 1950 ne soit pas dépassé pour autant. Si cette technique permet au juge d'adopter une interprétation dynamique de la ConvEDH, il doit néanmoins justifier son audace, afin de ne pas froisser les États parties qui s'étaient engagés sur un texte d'origine bien particulier.

Concernant la protection des données à caractère personnel, la CEDH s'est basée sur une interprétation extensive, dynamique, de l'article 8 de la ConvEDH, celui relatif au respect de la vie privée et familiale[25]. Cet article a fait l'objet d'une interprétation particulièrement large par le juge de Strasbourg dans plusieurs domaines. A titre d'exemple, on peut citer le « droit pour un individu de nouer et de développer des relations avec ses semblables »[26], le droit à l'image[27] ou encore le droit de disposer de son corps et d'entretenir des relations sexuelles[28].

C'est aussi sur cet article que s'est fondée la CEDH pour assurer la protection des données à caractère personnel. Si les correspondances étaient déjà protégées par la ConvEDH et pouvaient comporter, au-delà de leurs contenus, des données personnelles, ce n'était pas le cas pour nombre de ces données, à l'image des données médicales par exemple. Pour justifier cette interprétation extensive, la Cour a donc pris le soin de rattacher la protection des données à caractère personnel à l'article 8 de la ConvEDH et a également souvent fait référence de façon explicite aux dispositions de la Convention 108[29].

La voie étant sécurisée pour le juge, celui-ci a pu expliciter sa vision de la protection des données dans l'affaire *Leander c. Suède* en 1987[30].

> « 48. Le registre secret de la police renfermait sans contredit des données relatives à la vie privée de M. Leander.
>
> Tant leur mémorisation que leur communication, assorties du refus d'accorder à M. Leander la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée, garanti par l'article 8 par. 1. »

Ce paragraphe ayant été généralisé sous la forme suivante en 2008 :

> « Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. »[31]

On notera que le juge de Strasbourg évoque la question de « données relatives à la vie privée » mais n'utilise pas le terme de « données à caractère personnel », lequel n'apparait explicitement qu'en 2008 dans l'arrêt de grande chambre *S. et Marper c. Royaume-Uni*[32] :

> « **Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. Peu importe que les informations mémorisées soient ou non utilisées par la suite**. Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée précités, la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés »

Depuis 1987, la jurisprudence en matière de protection des données a connu un essor particulièrement marqué. La Cour s'est intéressée à la question de l'accès aux données à caractère

---

[24] CEDH, *Airey c. Irlande*, 9 octobre 1979, n°6289/73.
[25] Art. 8 § 1er : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».
[26] CEDH, *Niemietz c. Allemagne*, 16 décembre 1992, n°13710/88.
[27] CEDH, *Von Hannover c. Allemagne*, 24 juin 2004, n°59320/00.
[28] CEDH, K.*A. et A.D. c. Belgique*, 17 février 2005, n°42758/98 et 15558/99.
[29] CEDH, grande chambre, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, n°30562/04 et 30566/04, § 41, 66 et 79.
[30] CEDH, *Leander c. Suède*, 26 mars 1987, n°9248/81.
[31] *S. et Marper c. Royaume-Uni*, précité, § 67.
[32] *Ibid.* § 66, 68, 69, 75, 76, 81, 103, 104, 120 et 121.

personnel notamment en matière de renseignement[33] ou de filiation[34], du droit à l'effacement[35], du droit de rectification[36], aux catégories sensibles de données[37] parmi lesquelles on retrouve notamment les données médicales[38].

- Au-delà de ces quelques thématiques, que nous détaillons en annexe, le juge de Strasbourg s'est également intéressé à la « qualité » des données traitées. C'est ainsi qu'il a pu affirmer les principes de transparence et d'accessibilité des données[39] sans oublier l'importance de la finalité des données traitées[40], c'est-à-dire que seules les données strictement nécessaires à l'objectif poursuivi peuvent être collectées. Le juge de Strasbourg a également posé un principe de limitation de la durée de conservation des données, c'est notamment le cas dans la célèbre affaire *S. et Marper c. Royaume-Uni* où la législation britannique entendait autoriser la collecte et la conservation d'empreintes digitales et profils ADN de façon indéfinie[41]. Ces éléments, avec le caractère sensible de certaines données[42], sont autant d'indices pris en compte par le juge lorsqu'il s'agit d'examiner s'il y a eu une ingérence dans un droit protégé par l'article 8 de la ConvEDH ou lorsqu'il s'agit d'apprécier la justification à cette ingérence.

En effet le droit au respect de la vie privée tel que prévu par l'article 8 de la ConvEDH ne fait pas partie des droits dits « absolus », à l'image de l'interdiction de la torture par exemple. Il s'agit d'un droit auquel il est possible de déroger (cf. 3e partie *supra*) sous conditions, lesquelles sont limitativement énumérés par le paragraphe 2 de l'article 8 :

> « 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 infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Ressortent ainsi **trois conditions cumulatives** devant être satisfaites **afin qu'une ingérence** dans le droit au respect de la vie privée **puisse être autorisée** :

- **Une base légale.**
- **Un but légitime.**
- **Une ingérence nécessaire dans une société démocratique.**

4.1.1 – Une base légale.

Si la CEDH adopte une position assez large de ce qu'il faut entendre par « base légale », et qui se justifie notamment par les différences de culture juridique entre les États parties à la ConvEDH, elle exige toutefois que la loi, qu'il s'agisse d'une règle écrite ou jurisprudentielle, soit suffisamment accessible et précise pour que les citoyens puissent disposer de renseignements suffisants afin de régler leur conduite[43]. Ceci s'inscrit dans l'idée de faire connaître le droit afin que chacun puisse en prendre connaissance et qu'il ne soit pas possible de porter atteinte à des libertés fondamentales de

[33] CEDH, *Turek c. Slovaquie*, 14 février 2006, n°57986/00.
[34] CEDH, grande chambre, *Odièvre c. France*, 13 février 2003, n°42326/98.
[35] CEDH, *Segerstedt-Wiberg et autres c. Suède*, 6 juin 2006, n°62332/00.
[36] CEDH, grande chambre, *Rotaru c. Royaume-Uni*, 4 mai 2000, n°28341/95.
[37] *S. et Marper c. Royaume-Uni*, précité.
[38] CEDH, *Avilkina et autres c. Russie*, 6 juin 2013, n°1585/09.
[39] *Rotaru c. Royaume-Uni*, précité.
[40] CEDH, *Peck c. Royaume-Uni*, 21 janvier 2003, n°44647/98.
[41] *S. et Marper c. Royaume-Uni*, précité.
[42] CEDH, *Armonas c. Lituanie et Biriuk c. Lituanie*, 25 novembre 2008, n°36919/02 et 23373/03.
[43] CEDH, *Sunday Times c. Royaume-Uni*, 26 avril 1979, n°6538/74, § 47 et 49.

façon pernicieuse ou déguisée. On peut prendre comme exemple l'arrêt *L.H. c. Lettonie*[44]. En l'espèce, des données médicales personnelles avaient été collectées par l'inspection du contrôle de la qualité des soins médicaux et de l'aptitude au travail (« MADEKKI »), un organisme d'État, sans le consentement de la requérante. La Cour avait conclu à la violation de l'article 8 de la ConvEDH en raison du fait que la loi lettone n'était pas assez précise sur cette collecte de données personnelles.

4.1.2 – Un but légitime.

Les buts légitimes, au nom desquels la CEDH accepte une ingérence dans le droit au respect de la vie privée, sont limitativement énumérés par l'article 8 lui-même. On y retrouve des justifications pouvant porter sur la protection de la sécurité nationale, de la sûreté publique et sur la prévention des infractions pénales[45]. On peut également citer la protection du bien-être économique du pays que l'on retrouve dans l'affaire *M.S. c. Suède* de 1997[46].

4.1.3 – Une ingérence nécessaire dans une société démocratique.

C'est l'appréciation de la « nécessité » qui est ici au cœur du travail du juge. Il s'agit d'opérer un contrôle de proportionnalité afin de vérifier notamment s'il n'était pas possible d'adopter une solution moins intrusive en termes d'atteinte au droit au respect de la vie privée. En matière de protection des données, la CEDH laisse une certaine marge de manœuvre aux États parties lorsqu'il s'agit notamment de collecte à des fins de renseignement ou pour des enquêtes pénales. C'est ainsi que la CEDH estime que dans une société démocratique, l'existence de services de renseignement et la conservation des informations peuvent s'avérer nécessaire et prévaloir sur l'intérêt des citoyens, à condition de poursuivre des buts légitimes[47].

Le contrôle de proportionnalité opéré par le juge ne se limite pas toujours à l'appréciation de la nécessité de la mesure adoptée. Il implique parfois de concilier plusieurs intérêts en présence, notamment de concilier différents droits fondamentaux en conflits. A propos de la protection des données personnelles, cela peut, par exemple, être le cas avec la liberté d'expression consacrée par l'article 10 de la ConvEDH. En effet, au nom de la liberté d'expression, on peut tout à fait imaginer qu'un individu, qu'une organisation décide de divulguer un certain nombre de données personnelles pouvant alors porter atteinte au respect de la vie privée des personnes dont les données sont rendues publiques. C'est ainsi que dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* de 2017[48], les autorités finlandaises ont fait interdiction à deux sociétés de données fiscales à caractère personnel, relatives à 1,2 millions de personnes, de rendre publiques les données en leur possession, ceci au nom des lois en matière de protection des données. Etaient alors en balance deux droits fondamentaux : la liberté d'expression, sur laquelle le recours devant la CEDH était formulé, et la protection de la vie privée à travers la question de la protection des données personnelles. Les juges de Strasbourg ont ici conclu que la non-publication n'entrainait pas de violation de la liberté d'expression. En effet, il a été reconnu que la législation finlandaise visait à assurer la protection de la vie privée des individus et qu'elle assurait un juste équilibre entre l'exercice de la liberté d'expression et la protection des individus.

C'est donc en se référant à la Convention 108 et par une interprétation dynamique de l'article 8 de la ConvEDH, relatif au respect de la vie privée et familiale, que la CEDH a pu appréhender la question de la protection des données à caractère personnel, là où le texte de 1950 était pourtant muet. Cette position que la ConvEDH reste un texte adapté à son temps et le juge de Strasbourg, par sa jurisprudence, semble avoir su moderniser la lettre du traité initial. Malgré la difficulté de voir

[44] CEDH, *L.H. c. Lettonie*, 29 avril 2014, n°52019/07, § 59.
[45] CEDH, *Uzun c. Allemagne*, 02 octobre 2010, n°35623/05.
[46] CEDH, *M.S. c. Suède*, 27 août, 1997, n°20837/92.
[47] *Leander c. Suède*, précité, §59.
[48] CEDH, grande chambre, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, 27 juin 2017, n°931/13.

aboutir un protocole additionnel, une évolution du texte de la ConvEDH par la prise en compte de divers droits liés au numérique serait souhaitable, mais en attendant, le juge a démontré toutes ses capacités d'adaptation.

4.2 L'apport de la jurisprudence de la Cour de Justice de l'Union européenne (CJUE)

Contrairement à la CEDH, la CJUE n'a pas vraiment eu à se préoccuper de l'existence de dispositions relatives à la protection des données personnelles. Il y a deux explications à cela. D'une part, comme pour la protection de tout droit fondamental, il ne s'agissait pas d'un objectif prioritaire pour l'UE puisque ce travail était originellement envisagé comme devant être celui du Conseil de l'Europe et de la ConvEDH. D'autre part, parce que rapidement, l'UE s'est dotée de ses propres textes relatifs à la protection des données à caractère personnel, évitant ainsi à la CJUE d'avoir à recourir à des logiques prétoriennes afin d'en assurer la protection.

De façon très classique, **la principale mission de l'intégration communautaire devait être la réalisation d'un marché intérieur, ceci impliquant que soient assurées les 4 libertés économiques fondamentales prévues par les traités : libre circulation des marchandises, des personnes, des capitaux et des services**. Mais sous la menace de la Cour Constitutionnelle fédérale allemande[49] de ne plus reconnaître la primauté du droit de l'Union si l'UE n'assurait pas une protection des droits fondamentaux, et avec le risque que l'argument de la protection des droits fondamentaux ne soit avancé comme entrave à la réalisation du marché intérieur, la CJUE s'est résignée à assurer la protection des droits fondamentaux. Dans un premier temps, cela fut souvent à travers l'utilisation de principes généraux du droit, création prétorienne du juge. Toutefois, ceci ne fut pas nécessaire en matière de protection des données puisque dès 1995 (cf. 3e partie *infra*), une directive relative à la protection des données fut adoptée[50], laquelle fut complété par un article dédié dans la Charte des droits fondamentaux de l'UE (ci-après « la Charte ») en 2000[51] :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
> 2. 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. »

La directive 95/46 a aujourd'hui été remplacée par le RGPD (cf. 3e partie *infra*). Si le droit de l'UE offre une bonne lisibilité à la CJUE dans son travail d'interprétation, il ne permet toutefois pas un contrôle transversal de la protection des données aussi poussé que celui qu'opère la CEDH. En effet, si cette dernière peut notamment assurer une protection poussée en matière de protection des données dans le cadre de la surveillance d'État – même si elle reconnait une marge de manœuvre importantes aux Hautes Parties contractantes – il n'en est pas de même pour la CJUE. Ce n'est en tout cas pas son objectif principal. Pour comprendre cela, il faut en revenir à l'intitulé exacte de l'ancienne directive 95/46 et du RGPD : « 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 »**.

Les textes de l'UE envisagent avant tout l'exigence de protection des données à caractère personnel afin de pouvoir en permettre la libre circulation. L'idée pour l'UE est de ne pas soustraire l'économie des données personnelles du marché intérieur. Pour assurer une libre circulation des données personnelles en amont, il est nécessaire d'en assurer la bonne protection. Ceci offre le double avantage de rassurer le consommateur européen quant à la fiabilité de la protection entourant les données personnelles qu'il pourrait être amené à communiquer, et d'éviter que les États membres ne

[49] Cour Constitutionnelle fédérale Allemande, affaire dite « Solange I », du 29 mai 1974.
[50] 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, (ci-après « Directive 95/46 »).
[51] Charte des droits fondamentaux de l'Union européenne, signée à Nice, 7 décembre 2000, article 8.

puissent avancer l'argument d'un risque pesant sur la protection de ces données pour empêcher qu'elles puissent circuler dans d'autres États de l'UE. On comprend donc que **l'ancienne directive 95/46 et le RGPD visent moins l'encadrement de la surveillance étatique que la protection des données afin de permettre leur libre circulation**. Il s'agira donc davantage de s'assurer, par exemple, qu'une entreprise respecte les garanties suffisantes en matière de traitement de données à caractère personnel de ses clients, que de vérifier les conditions dans lesquelles un État souhaite mettre en place un programme de surveillance.

Le droit de l'UE n'est pas pour autant démuni en matière de protection des données collectées par les États membres et liées à matière de pénale. En effet, le paquet « données » de 2016 (cf. 5e et 10e parties *infra*) a vu l'adoption de la directive 2013/680[52] abrogeant l'ancienne décision cadre 2008/977[53]. Mais une limite de taille, classique au demeurant, vient atténuer la portée de ce texte : elle ne peut être mobilisée en dehors du champ d'application du droit de l'Union (et donc lorsque le droit national s'applique), notamment en matière sécuritaire[54]. On comprend donc, par exemple, que les hypothèses de collectes de données à des fins de renseignement n'ont que peu de chance de tomber sous le coup de cette directive et donc que la CJUE n'interviendra que rarement dans ce domaine.

Mais la structure particulière du droit de l'UE n'a pas pour autant empêché toute intervention du juge de Luxembourg en matière de protection des données à caractère personnel. Deux célèbres affaires doivent être particulièrement soulignées : *Digital Rights Ireland*[55] en 2014 et *Maximillian Schrems*[56] en 2015 :

- dans la première affaire, le requérant, Digital Rights, propriétaire d'un téléphone portable avait remis en cause la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques. Ces mesures nationales se fondant sur la directive 2006/24/CE[57], Digital Rights en demandait l'annulation[58]. Selon la CJUE, en visant tous les moyens de communication électronique et en couvrant tous les abonnés et utilisateurs inscrits, la directive comporte une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne[59] sans qu'une telle ingérence ne soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire[60] et sans prévoir de garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données[61]. Le juge de Luxembourg prononça donc l'invalidation de la directive.

- dans la seconde affaire, le requérant, un ressortissant autrichien, était un utilisateur de Facebook. Pour ce faire, il avait conclu un contrat avec Facebook Ireland, comme tout utilisateur européen. Mais il contestait le fait que Facebook Ireland transfère ses données à caractère personnel à Facebook Inc.

---

[52] 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, (ci-après « Directive 2016/680 »).

[53] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, (ci-après « Décision-cadre 2008/977 »).

[54] Directive 2016/680, Art. 2, §3, a).

[55] CJUE, grande chambre, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, 08 avril 2014, Aff. C-293/12 et C-594/12.

[56] CJUE, grande chambre, *Maximillian Schrems contre Data Protection Commissioner*, 06 octobre 2015, Aff. C-262/14.

[57] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 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, (ci-après « directive 2006/24 »).

[58] *Digital Rights Ireland*, précité, § 17.

[59] *Digital Rights Ireland*, précité, § 56.

[60] *Digital Rights Ireland*, précité, § 65.

[61] *Digital Rights Ireland*, précité, § 66.

c'est-à-dire aux États-Unis en expliquant que la législation américaine ne garantissait pas un niveau de protection suffisant des données transférées contre des activités de surveillance à l'image de celles opérées par la National Security Agency (NSA)[62]. Ce transfert se fondait sur la décision 2000/520[63] de la Commission reconnaissant aux États-Unis un niveau suffisant en matière de protection des données et autorisant donc le transfert de données à caractère personnel de l'UE vers un pays tiers, les États-Unis. La CJUE expliqua alors que la décision 2000/520 rendait possible des ingérences, fondées sur des exigences relatives à la sécurité nationale et à l'intérêt public ou sur la législation interne des États-Unis, dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis. Plus encore, le juge a retenu que la décision 2000/520 ne faisait pas état de l'existence d'une protection juridique efficace contre des ingérences de cette nature aux États-Unis et qu'il ne pouvait donc pas être considéré que cet État fournissait un niveau de protection suffisant. La CJUE prononça donc l'invalidation de la décision 2000/520.

La jurisprudence de la CJUE joue donc un rôle fondamental dans l'élaboration du cadre juridique de l'UE en matière de protection des données[64]. Elle a démontré sa capacité à dépasser le simple cadre de protection offert par la directive 95/46, visant *in fine* à assurer une libre circulation des données, pour faire effectivement valoir le droit de toute personne à la protection des données à caractère personnel la concernant, prévu par l'article 8 de la Charte. Le juge de Luxembourg est intervenu afin d'assurer le respect d'importants principes relatifs à la protection des données tels que la mention de finalités précises, l'exigence d'une conservation limitée, ou encore la nécessité d'encadrer les conditions dans lesquelles les autorités peuvent mettre en place un traitement de données.

L'UE a su opérer une véritable articulation entre protection des 4 libertés économiques fondamentales du marché intérieur et les droits fondamentaux en permettant, grâce à l'ancienne directive 95/46, remplacée par le RGPD, une libre circulation des données à caractère personnel et en assurant le droit fondamental à la protection des données à caractère personnel, grâce à l'article 8 de la Charte des droits fondamentaux de l'UE.

4.3 Articulation entre les jurisprudences de la CJUE et de la CEDH en matière de protection des données à caractère personnel.

La CJUE et la CEDH assurant toutes deux, en partie sur un même territoire, un droit à la protection des données à caractère personnel, le principal risque réside en un conflit lié à l'interprétation de la dimension à donner à ce droit. Il s'agit d'une problématique tout à fait classique en matière droit européen des droits de l'Homme. La réponse à cette problématique est donc tout aussi classique.

4.3.1 – Une interprétation de la Charte par la CJUE équivalente à celle de la ConvEDH par la CEDH.

Pour cela il convient de se référer à l'intitulé de la Charte, laquelle prévoit à son article 52, §3 que :

> « Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des

[62] *Maximillian Schrems*, précité, § 26 à 28.

[63] Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, (ci-après « décision 2000/520 »).

[64]. Cf. en annexe le tableau 14.

libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ».

Naturellement, les dispositions de l'article 52 invitent à se détacher que texte même de la ConvEDH. Il s'agit de s'intéresser à « leur sens et leur portée ». Ainsi, bien que le libellé de l'article 8 de la ConvEDH ne consacre pas de protection des données à caractère personnel, nous avons vu qu'il n'en allait pas de même concernant la jurisprudence du juge de Strasbourg. La mention de cette nécessité de rapprochement des interprétations était notamment prévue par l'article 4[65] de la directive 2006/24, invalidée par la CJUE :

> « […] La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme ».

La directive 95/46 faisait également référence à la ConvEDH dans trois considérants 1[66], 10[67] et 37[68]. Le nouveau RGPD ne déroge pas à la tradition avec le considérant 73 :

> « Des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données, au droit à la portabilité des données, au droit d'opposition, aux décisions fondées sur le profilage, ainsi qu'à la communication d'une violation de données à caractère personnel à une personne concernée et à certaines obligations connexes des responsables du traitement peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ou de manquements à la déontologie des professions réglementées, et pour garantir d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés pour des motifs d'intérêt public général, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires. Il y a lieu que ces limitations respectent les exigences énoncées par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. »

On notera que la formule employée par le considérant, relative à l'autorisation d'ingérences dans le droit à la protection des données, reprend la même construction que celle de l'article 8 de la ConvEDH relatif au respect de la vie privée.

---

[65] Relatif à l'accès aux données.

[66] « Considérant que les objectifs de la Communauté, énoncés dans le traité, tel que modifié par le traité sur l'Union européenne, consistent […] à promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et les lois des États membres, ainsi que dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; »

[67] « Considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales […] ; »

[68] « Considérant que le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire […] doit bénéficier de dérogations ou de limitations de certaines dispositions de la présente directive dans la mesure où elles sont nécessaires à la conciliation des droits fondamentaux de la personne avec la liberté d'expression […] telle que garantie notamment à l'article 10 de la convention européenne de sauvegarde des droits de l' homme et des libertés fondamentales ; »

Tableau 12 : les définitions convergentes des « ingérences » et des « limitations » de 1950 à 2016

	Article 8 de la ConvEDH (1950)	**Article 52 de la Charte (2000)**	**Considérant 73 RGPD (2016)**
Base légale	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 …	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.	Des limitations à certains principes spécifiques […] peuvent être imposées par le droit de l'Union ou le droit d'un État membre
Ingérence nécessaire dans une société démocratique	… et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire …	Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires …	, dans la mesure nécessaire et proportionnée dans une société démocratique
But légitime	… 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 infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.	…et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.	démocratique pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces […]

Ces trois étapes, déjà détaillées pour la CEDH au point 4.1., sont non seulement affirmées par le droit primaire et le droit dérivé de l'UE, mais se retrouvent également dans le raisonnement de la CJUE. C'est ainsi que dans l'affaire *Digital Rights Ireland*, le juge de Luxembourg rappelle que toute limitation

de l'exercice des droits et des libertés consacrés par la Charte doit être prévue par la loi[69], ce qui est le cas avec la directive 2006/24. La Cour s'intéresse donc à la question de savoir si l'ingérence poursuivait un but légitime. Elle note qu'en l'espèce, le Conseil « Justice et affaires intérieures » a considéré que les données relatives à l'utilisation des communications électroniques étaient particulièrement importantes et constituaient un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée, et que ceci constituait bien un objectif d'intérêt général[70]. Restait donc à opérer un contrôle de proportionnalité. La CJUE procède ici en deux temps. Elle vérifie, d'une part, si la mesure en cause est apte à satisfaire l'objectif poursuivi, ce qui est le cas à ses yeux en l'espèce[71]. Elle vérifie, d'autre part, si la mesure ne dépasse pas les limites de ce qui est approprié et nécessaire à la réalisation des objectifs poursuivis[72]. La Cour note alors, après avoir largement fait référence à la ConvEDH et la jurisprudence de la CEDH[73], que la directive s'applique même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. Et qu'en outre, la directive ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel[74]. Partant, la CJUE estime que la directive excède les limites qu'impose le principe de proportionnalité[75].

Le raisonnement en trois étapes opéré par la CJUE s'approche donc de celui opéré par la CEDH.

4.3.2 – La reconnaissance commune d'un droit à un recours effectif en matière de protection des données à caractère personnel.

Un autre exemple significatif du rapprochement entre CJUE et CEDH en matière de protection des données à caractère personnel concerne la reconnaissance par les deux cours d'un droit à un recours effectif. Si la CEDH avait condamné la Suède pour ne pas avoir prévu de recours judiciaire direct pour obtenir de la part des services de renseignement la suppression des données concernant les requérants[76], la CJUE reprend les mêmes exigences. C'est ainsi que dans l'affaire *Maximillian Schrems*, le juge explique que la législation américaine, reconnue comme assurant une protection suffisante des données par la décision 2000/520, ne prévoyait 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. Le juge de Luxembourg en a donc conclu au fait

---

69 *Digital Rights Ireland*, précité, § 38.

70 *Digital Rights Ireland*, précité, § 42 à 44.

71 *Digital Rights Ireland*, précité, § 49 : […] eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales […].

72 *Digital Rights Ireland*, précité, § 46.

73 *Digital Rights Ireland*, précité, § 54 et 55 : Ainsi, la réglementation de l'Union en cause doit 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 tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, *Liberty et autres c. Royaume-Uni*, nº 58243/00, § 62 et 63, du 1er juillet 2008; *Rotaru c. Roumanie*, précité, § 57 à 59, ainsi que *S et Marper c. Royaume-Uni*, précité, § 99). La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit 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 (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, S et *Marper c. Royaume-Uni*, précité, § 103, ainsi que *M. K. c. France*, nº 19522/09, § 35, du 18 avril 2013).

74 *Digital Rights Ireland*, précité, § 58.

75 *Digital Rights Ireland*, précité, § 69.

76 *Segerstedt-Wiberg et autres c. Suède*, précité, § 122.

qu'une telle législation ne peut être entendue comme respectant le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte.

4.3.3 – Une référence commune à la Convention 108.

Dans le sens d'un rapprochement entre droit de l'UE et droit du Conseil de l'Europe, on peut également rappeler que la Convention 108 du Conseil de l'Europe reste un texte de référence commun lorsqu'il s'agit de faire référence aux principes directeurs en matière de protection des données. Il est assez fréquent de voir la CEDH s'y référer à l'image de l'affaire *S. et Marper c. Royaume-Uni*[77]. La CJUE est plus discrète mais plusieurs textes de droit dérivé mentionnent la convention de 1981[78]. Référence commune ne vaut pas interprétation commune, mais on peut toutefois noter que les mêmes principes directeurs sont source d'inspiration pour la CEDH et le droit de l'UE.

En réunissant tous ces éléments et en insistant notamment sur le fait que le juge de Luxembourg se réfère à la ConvEDH et à la jurisprudence du juge de Strasbourg pour la résolution du litige qui lui est soumis, on note **qu'il existe des techniques permettant d'assurer une certaine homogénéité entre l'interprétation par la CEDH de la ConvEDH et l'interprétation par la CJUE du droit de l'UE**. Ceci semble fonctionner convenablement pour ce qui concerne l'interprétation à donner au respect des données à caractère personnel.

[77] *S. et Marper c. Royaume-Uni*, précité, § 66.
[78] Directive 95/46, considérant 11. RGPD, considérant 105.

5 L'ambition du paquet « données » de 2016.

Il se compose de 3 textes, un règlement (le RGPD) et deux directives :

1. Le règlement 2016/679 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. C'est ce texte, élément central du paquet législatif « données à caractère personnel », qui est couramment appelé RGPD pour règlement général sur la protection des données ».

Il remplace la directive 95/46 de 1995.

2. La directive 2016/680 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.

Cette directive remplace la décision-cadre 2008/977/JAI du Conseil.

3. La directive 2016/681 relative à l'utilisation des données des dossiers passagers[79] (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

Il s'agit de la directive « PNR », souvent évoquée.

5.1 Contexte général de l'adoption du paquet « données »

5.1.1 – Contexte général de l'adoption du RGPD.

Dès le milieu de la décennie 2000, la question de l'adaptation de la directive de 1995 a été posée. La critique de ce texte, ayant pourtant posé les bases essentielles de la protection des données personnelles dans l'UE, est sans appel. Le législateur de 2016 s'accorde un droit d'inventaire évoqué très directement dans les premiers considérants du RGPD :

> « Si elle demeure satisfaisante en ce qui concerne ses objectifs et ses principes, la directive 95/46/CE n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique ou le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne »[80].

Et il ajoute :

> « Ces différences dans le niveau de protection résultent de l'existence de divergences dans la mise en œuvre et l'application de la directive 95/46/CE ».[81]

La question du choix de l'instrument juridique s'impose au centre des préoccupations. Ceci trouvera en l'utilisation d'un règlement plutôt que d'une directive une réponse très concrète. Nous reviendrons sur l'avantage de cet instrument[82].

---

[79] Les données Passenger Name Record (PNR) sont des « informations non vérifiées collectées par les compagnies aériennes auprès de leurs voyageurs et conservées dans leur système de réservation » (voir : PEYROU (S.), « Le rejet de la proposition de directive "PNR" par la Commission des libertés civiles du Parlement européen : l'impossible alchimie entre lutte contre le terrorisme et protection des droits fondamentaux ? », *Réseau Universitaire européen Droit de l'Espace de liberté, sécurité et justice* [en ligne], 5 mai 2013. Disponible sur **:** http://www.gdr-elsj.eu/2013/05/05/cooperation-policiere/le-rejet-de-la-proposition-de-directive-pnr-par-la-commission-des-libertes-civiles-du-parlement-europeen-limpossible-alchimie-entre-lutte-contre-le-terrorisme-et-protection-de/, [page consultée le 20 novembre juillet 2017].

[80] RGPD, considérant n°9.

[81] *Ibid.*

[82] Voir 5.2 *infra.*

5.1.2 – Le contexte général de l'adoption de la directive PNR.

En parallèle des discussions sur le RGPD, celles relatives à la directive PNR ne sont guère plus simples. Les fichiers PNR sont apparus aux États-Unis, en Australie, au Canada et au Royaume-Uni en réaction aux attentats du 11 septembre 2001[83]. En France, c'est la loi de 2006 relative à la lutte contre le terrorisme[84] qui a introduit cette possibilité. Aujourd'hui, il faut se référer à l'article 17 de la loi de programmation militaire de 2013 qui prévoit la possibilité de mettre en place de tels fichiers PNR[85]. A noter que les données dites « sensibles » telles que l'origine raciale, les convictions politiques, philosophiques ou religieuses, en sont exclues.

Ainsi, plusieurs États membres de l'Union ont pu développer leur propre législation en matière de fichiers PNR. Cette situation conduisait à ce que de nombreux citoyens de l'UE fassent l'objet d'une collecte de leurs données par leur propre État lorsqu'ils voyageaient à l'étranger en dehors de l'UE – la France par exemple ne collectant pas de données pour des vols purement domestiques en métropole[86] - ou par leur propre État et un État tiers si celui-ci disposait lui aussi d'une législation PNR, sans que de telles données ne soient collectées pour des vols intra-communautaires. C'est pour cette raison et afin d'éviter une fragmentation trop importante de la législation, que la Commission européenne avait souhaité la mise en place d'une directive « PNR » au niveau de l'UE[87]. Ce texte prévoyait de permettre l'exploitation de 19 types de données à des fins répressives de manière réactive, en temps réel et de manière proactive. Toutefois, le projet de texte fut rejeté par la commission des libertés civiles du Parlement européen le 24 avril 2013, marquant ainsi un coup d'arrêt au projet. Ce n'est qu'avec les divers attentats ayant frappé l'UE, notamment Paris et Bruxelles (2015), qu'un compromis fut trouvé avec les parlementaires européens. En substance, il s'agissait d'accepter un nouveau projet de directive PNR en l'échanger d'un renforcement de la protection des données à caractère personnel dans l'Union et donc l'adoption simultanée du RGPD. Ce fut chose faite le 27 avril 2016.

5.2 Le choix européen d'un règlement pour remplacer la directive 95/46

Comme nous avons pu commencer à l'aborder, le choix de recourir à l'instrument juridique du règlement plutôt que d'une directive s'inscrit dans une volonté d'une meilleure homogénéité du droit de l'UE en matière de protection des données à caractère personnel[88].

L'intérêt de recourir à un règlement plutôt qu'à une directive se comprend très bien du point de vue de l'unicité du droit. En effet, comme l'explique l'article 288 du traité sur le fonctionnement de l'UE (ci-après TFUE), une directive « lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens » alors que le règlement « est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre ». Ainsi, en ne fixant qu'un simple objectif à atteindre, la directive ouvre la voie à une fragmentation des législations nationales car si ces dernières tendront bien au même objectif, elles pourront utiliser des voies et des dispositions différentes d'un État à l'autre. Le règlement en revanche ne connait pas ce problème, en tout cas, pas dans les mêmes proportions. Il convient en effet de

[83] Pour les États- Unis, voir : US Aviation and Transportation Security Act, *Public Law* 107-71, 19 novembre 2001, Sec.115 (3).

[84] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, Art. 7.

[85] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, Art. 17, codifié à l'article L232-7 du *code de la sécurité intérieure*.

[86] Article L232-7, II du *code de la sécurité intérieure*.

[87] Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, COM(2011) 32 final.

[88] RGPD, considérant n°9.

souligner que les règlements ont « une portée générale »[89]. C'est-à-dire qu'ils posent un certain nombre de principes généraux mais laissent bien souvent la possibilité aux États membres d'ajuster le curseur au sein du cadre défini par le règlement. Le RGPD l'illustre parfaitement :

> « En ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, 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, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées « données sensibles »). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite ».

Concernant la licéité du traitement, les États membres peuvent donc « maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) [à propos des traitements nécessaires au respect d'obligations légales] et e) [à propos des traitements nécessaires à l'exécution d'une mission d'intérêt public], en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal ».[90]

Autre exemple, en ce qui concerne « la majorité numérique » c'est-à-dire le traitement de données relatives à un enfant dans le cadre de la fourniture de services de la société d'information. Le RGPD envisage qu'un traitement de données doit est licite si les mineurs de 16 ans et plus y ont consenti, protégeant ainsi les mineurs de moins de 16 ans[91]. Mais le RGPD offre la possibilité aux États membres de « prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans »[92]. Ici, un État membre peut donc aller moins loin dans la protection des données que celle envisagée par défaut par le RGPD.

Mais il est aussi des cas où le RGPD autorise les États membres à aller plus loin que la protection prévue par défaut. Si l'on s'intéresse aux catégories sensibles de données, désormais appelées catégories « particulières de données »[93] par le RGPD, on constate qu'ici aussi « les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé ».

C'est dans ce contexte que la France en décembre 2017 a vu l'adoption par l'Assemblée Nationale en première lecture[94] du projet de loi sur la protection des données personnelles. Ce texte vise à préparer le droit français à l'entrée en vigueur du RGPD. C'est aussi l'occasion d'y fixer les éléments pour lesquels le RGPD laisse une certaine marge d'appréciation aux États

---

[89] Art.288 du TFUE.
[90] RGPD, Art.6 §2.
[91] RGPD, Art.8 §1, al.1er.
[92] RGPD, Art.8 §1, al.2.
[93] L'art.9 §1 du RGPD prévoit qu'il s'agit de l'origine raciale ou ethnique, des opinions politiques, des convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
[94] 505 « pour », 18 « contre » et 24 « abstentions ».

membres à l'image de la « majorité numérique » fixée à 15 ans par le législateur français[95], là où le RGPD laissait la possibilité de choisir entre 13 et 16 ans. On constate donc que si le règlement permet indéniablement une meilleure uniformité du droit que ce qui était rendu possible par la directive précédente, uniformité ne signifie pas pour autant unicité sur tous les points.

[95] Age correspondant à l'entrée au lycée. DEBES (F.), *Les Echos*, « RGPD : le texte européen soumis à l'examen du Parlement français », 18 février 2018, [disponible en ligne] https://www.lesechos.fr/tech-medias/hightech/0301303412667-rgpd-le-texte-europeen-soumis-a-lexamen-du-parlement-francais-2154562.php, [consulté le 19 février 2018].

6 Le contexte politique de l'adoption du RGPD dans la décennie 2010

Dès le milieu de la décennie 2010, sous le double effet de la mondialisation accentuée des flux économiques et informationnels, la question de l'adaptation de la directive UE de 1995 (cf. 3e partie *supra*) a été posée. Dans le même temps les évolutions de l'intégration européenne ont déplacé l'enjeu d'une directive vers un règlement, norme d'application directe.

Cependant sur ce sujet aussi bien technique que juridique et économique les discussions ont été longues. C'est en janvier 2012 seulement que la Commission européenne a publié des propositions en vue de l'adoption d'un règlement. Et c'est au cours de la période 2012-2014 que les « révélations » d'Edward Snowden en juin 2013 ont fait connaître à l'opinion mondiale l'intensité des pratiques d'espionnage (étatsuniennes) portant sur les données au travers des pratiques dites de « bulk access ». La mobilisation de la commission libertés civiles, de la justice et des affaires intérieures (« Libe ») du Parlement européen et du Conseil de l'Europe a été très vive et a pesé fortement sur les échanges. Après 3 lectures, le Parlement européen a modifié la proposition de la commission et a adopté une version finale en mars 2014. Puis les 3 autorités constituant le « trilogue » (Parlement, Commission et Conseil) ont repris les discussions. En juin 2015, le Conseil a adopté une orientation générale en vue du futur règlement et en décembre 2015, la commission « Libe » du Parlement européen du Parlement a fait sienne la version qui est devenue le RGPD en avril 2016. Entretemps le 6 mars 2015, la Commission avait publié sa stratégie pour le « Marché Unique Numérique » (MUN) comportant 16 propositions et reposant sur trois piliers :

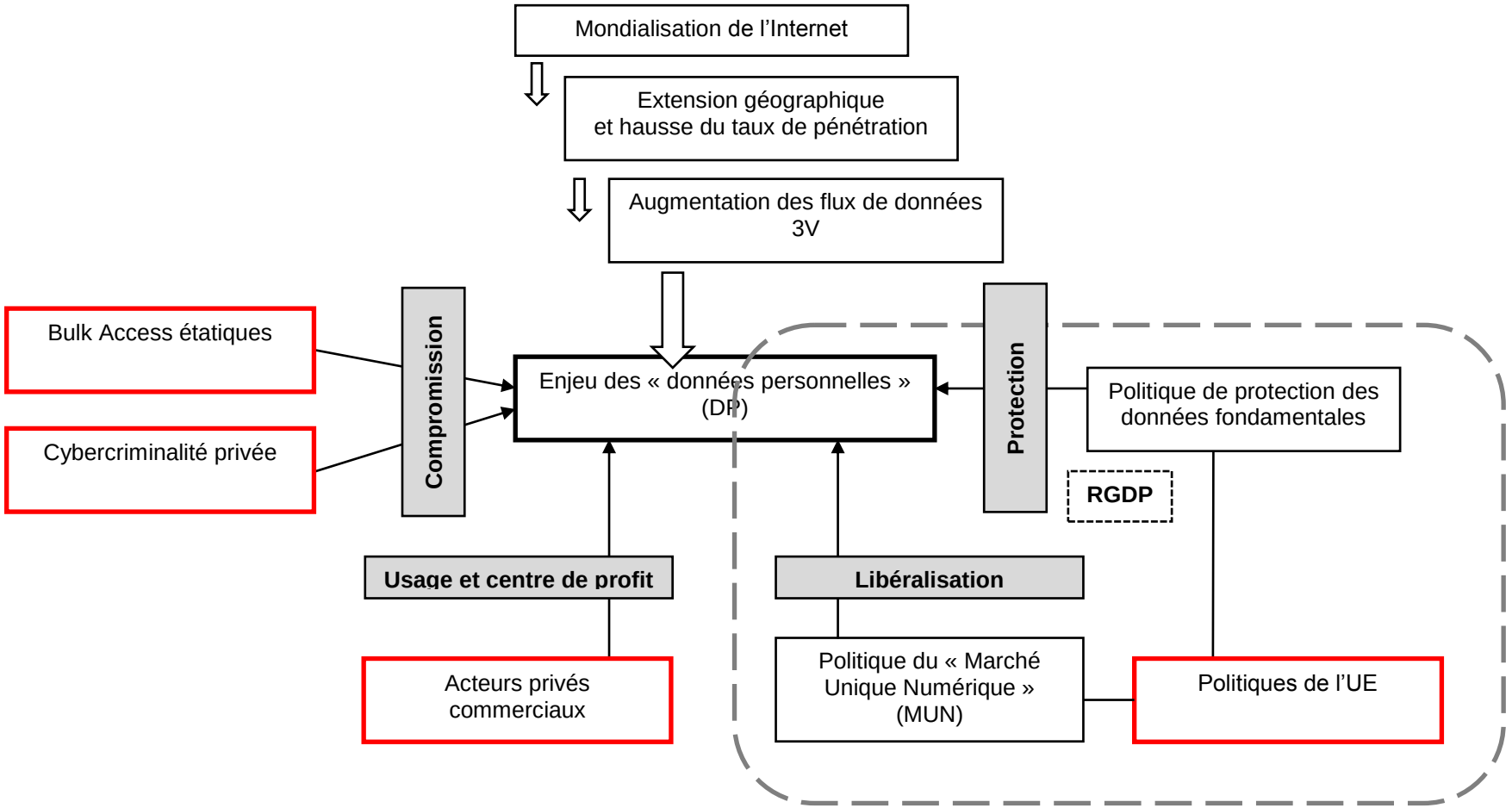
(1) amélioration de l'accès aux biens et services numériques pour les consommateurs et les entreprises,

(2) offrir un « environnement propice » au développement du numérique et

(3) garantir une maximisation du potentiel de croissance de l'économie numérique européenne.

Le nouveau règlement est le résultat hybride d'une politique de protection des données personnelles et d'une politique de libéralisation des données favorables aux acteurs économiques. Indépendamment des questions d'espionnage étatique, les acteurs européens ont voulu faire évoluer avec le RGPD les principes et les pratiques de la protection des données personnelles après l'explosion des flux de données (les « 3V »), résultat de l'expansion de l'Internet commercial dans le monde entier, un Internet qui était seulement embryonnaire sous cette forme en 1995. Le contexte de modification de la directive de 1995 est donc particulièrement dense et parfois contradictoire. Le résultat qu'est le RGPD peut être figuré dans le schéma suivant :

Figure 1 : Paramètres et contexte de production du RGPD



7 Les innovations du RGPD en matière de protection des données

Le texte du RGPD, voté et adopté par le Parlement européen et par le Conseil a été promulgué le 27 avril 2016 : selon son dernier article il doit entrer en vigueur le 25 mai 2018. Le règlement est « 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 », c'est-à-dire exactement la même dénomination que la directive de 1995. Ce texte d'application directe dans les 28 pays de l'UE succède à et supprime cette directive « 95/46/CE » du 24 octobre 1955 et qui avait dû être transposée en son temps dans chacun des droits nationaux.

Le nouveau RGPD comprend 173 considérants qui rappellent les principes fondamentaux et les acquis de la doctrine de l'UE en matière de données personnelles et 99 articles qui constituent le nouveau règlement. La structuration interne dit clairement la portée du texte :

- chapitre I : « dispositions générales »
- chapitre II : « principes »
- chapitre III : « droits de la personne concernée »
- chapitre IV : « responsable du traitement et sous-traitant »
- chapitre V : « transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales »
- chapitre VI : « autorités de contrôles indépendantes »
- chapitre VII : « coopération et cohérence »
- chapitre VIII : « voies de recours, responsabilité et sanctions »
- chapitre IX : « dispositions relatives à des situations particulières de traitement »
- chapitre X : « actes délégués et actes d'exécution »

Le RGPD de 2016-18 est un texte presque quatre fois plus long (173 considérants, 99 articles) que la directive de 1995 (72 considérants, 32 articles) et sa structuration est assez nettement différente. Le RGPD est un **texte relatif aux données des personnes physiques** dans l'espace de l'Union Européenne (UE) à l'égard des **l'utilisation qui peut en être faite** en stock (traitement de données) comme en flux (transfert de données) **par des personnes morales.**

En substance le RGPD est nettement plus protecteur que la directive de 1995 (transposée entretemps dans tous les pays) **et plus contraignants pour les personnes morales utilisant des données** et constituant pour ce faire des traitements de données.

A l'image de ce que nous avons pu évoquer concernant son champ d'application territorial, le RGPD réaffirme les grands principes posés par la directive 95/46. C'est notamment le cas du consentement (7.1). Mais le RGPD va plus loin en prévoyant également de nouveaux droits pour les personnes physiques (7.2).

7.1 La réaffirmation de la place centrale du consentement.

Le consentement demeure le principal moyen permettant à un traitement de données d'être considéré comme licite[96]. Le RGPD reprend la même définition du consentement que celle posée par la directive 95/46. Il s'agit de « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif

[96] RGPD, Art.6, §1, a) « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; […] »

clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[97]. Aux termes de l'article 7, la preuve de ce consentement doit être rapportée par le responsable du traitement[98]. Toute personne est également libre de retirer son consentement, sans que cela n'ait d'effet rétroactif[99]. Il s'agit ici de concilier le droit qu'a chacun de retirer son consentement, sans pour autant remettre en cause le traitement réalisé lorsque le consentement était encore accordé. Cet article 7, exclusivement consacré au consentement, est une innovation du RGPD. La directive 95/46 n'était pas aussi précise à ce sujet.

7.2 La consécration de nouveaux droits.

a) « La majorité numérique ».

Nous avons déjà évoqué plus haut la question de la « majorité numérique »[100] visant à protéger les mineurs contre le traitement de leurs données à caractère personnel (cf. 6.2. *supra*).

b) Le droit à la portabilité des données.

Ce droit permet à chaque individu, dont les données personnelles font l'objet d'un traitement, d'en obtenir le contenu. Il est également précisé que ce contenu doit être transmis dans un « format structuré, couramment utilisé et lisible par machine »[101]. Toutefois, cette possibilité n'est offerte qu'à partir du moment où le traitement est le résultat d'un consentement de la personne concernée ou s'il s'agit d'un traitement opéré dans le cadre de l'exécution d'un contrat[102]. Mais ce droit ne se limite pas à l'obtention du détail des données collectées nous concernant. Il prévoit également, dans les mêmes conditions, que l'individu ayant exercé son droit à la portabilité puisse transmettre cette liste à un autre responsable de traitement de données à caractère personnel, et même que cette transmission se fasse directement entre les deux responsables de traitements lorsque cela est possible[103].

c) La reconnaissance d'actions collectives.

Le RGPD envisage le fait que toute personne ayant fait l'objet d'un traitement de données non conforme puisse intenter une action collective :

> « 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, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77 [droit d'introduire une réclamation auprès d'une autorité de contrôle], 78 [droit à un recours juridictionnel effectif contre une autorité de contrôle] et 79 [droit

---

97 RGPD, Art.4, 11).

98 RGPD, Art.7, §1er : « Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant ».

99 RGPD, Art.7, §3 : « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement ».

100 Voir point 5.2.

101 RGPD, Art.20, §1er.

102 *Ibid.*

103 RGPD, Art.20, §2.

à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant] et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit ».

d) Droit à la réparation des dommages matériel et moral.

Si la directive 95/46 restait relativement évasive sur la question, en prévoyant simplement que « toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi »[104], le RGPD, ici encore, permet de gagner en précision. Désormais, « toute personne ayant subi un dommage **matériel ou moral** du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi »[105].

Le RGPD présente ainsi un certain nombre de droits nouveaux. Mais au-delà de leur consécration, l'enjeu réside au niveau de leur effectivité. A l'image de la « majorité numérique », comment contraindre en pratique un mineur de moins de 16 ans de ne pas utiliser un réseau social ?

[104] Directive 95/46, Art.23.
[105] RGPD, Art.82, §1er.

8 L'innovation fondamentale du RGPD en matière de responsabilisation des acteurs de la *data*

S'il est une innovation centrale du RGPD, c'est peut-être celle de la responsabilisation des acteurs de traitement de données. La directive 95/46 et le RGPD changent de paradigme à ce sujet. Si la directive commandait aux autorités de protection de démontrer une violation du texte par les responsables du traitement, le RGPD commande aux responsables de traitement et aux sous-traitants, de démontrer qu'ils sont en conformité avec le texte. A l'aube de l'entrée en vigueur du RGPD, ce **renversement de la charge de la preuve** inquiète les entreprises, lesquelles travaillent sans cesse de façon plus étroite avec les données personnelles.

On touche ici au paradoxe de ce règlement : alors qu'il doit favoriser la libre circulation des données personnelles au sein de l'UE afin de parachever la réalisation du marché intérieur, ce qui représente une véritable manne financière pour de nombreuses entreprises, l'entrée en vigueur du RGPD constitue pour ces dernières un vrai risque juridique.

La directive 95/46 conditionnait la mise en œuvre d'un traitement de données à un régime de déclaration préalable[106]. Ceci n'est pas repris pas le RGPD. Mais en contrepartie, de nombreux garde-fous et autres mécanismes de certifications sont envisagés afin que les responsables de traitements puissent démontrer le bon respect du RGPD.

8.1 La tenue d'un registre des activités de traitement.

Ceci est prévu par l'article 30 du RGPD :

> « Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité ».

Ce registre doit intégrer un certain nombre d'informations relatives au traitement telles que le nom et les coordonnées du responsable du traitement[107], les finalités du traitement[108] ou encore les catégories de personnes et de données à caractère personnel visées par le traitement[109].

8.2 La notification à l'autorité de contrôle d'une violation de données à caractère personnel

Cette mesure est prévue par l'article 33 du RGPD :

> « En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais ».

Si la terminologie « meilleurs délais » reste vague, le RGPD prévoit tout de même que, lorsque la violation est susceptible d'engendrer un risque pour les droits fondamentaux des individus, il est souhaitable que le responsable du traitement informe l'autorité de contrôle dans les 72h. A noter également que le sous-traitant n'est pas exempt de toutes obligations. S'il n'est pas contraint de notifier une violation directement à l'autorité de contrôle, il doit tout de même en référer « dans les meilleurs délais après en avoir pris connaissance » au responsable du traitement[110].

8.3 La réalisation d'analyse d'impact relative à la protection des données

---

[106] Directive 95/46, Art.18, §1er – Obligation de notification à l'autorité de contrôle – « Les États membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées ».

[107] RGPD, Art. 30, §1, a).

[108] RGPD, Art. 30, §1, b).

[109] RGPD, Art. 30, §1, c).

[110] RGPD, Art. 33, § 2.

Il s'agit une nouvelle fois d'un instrument visant à assurer au responsable du traitement, que les données qu'il est sur le point de traiter ne constitueront pas une violation du RGPD. La réalisation d'une telle analyse d'impact est imposée par le RGPD pour les traitements les plus intrusifs en matière de protection des données et respect de la vie privée des personnes concernées. L'article 35, §3 prévoit que :

> « L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :
> a) l'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 ;
> b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou
> c) la surveillance systématique à grande échelle d'une zone accessible au public. »

Il convient de noter que l'article utilise le terme « en particulier » ce qui implique que la série d'hypothèses prévue par le RGPD n'est pas exhaustive. Ici, l'éclairage par les autorités de protection[111], ou mieux, des lignes directrices communes de la part du Comité seront les bienvenues. Cette liste pourra également être enrichie par la jurisprudence future de la CJUE.

Le RGPD fournit une liste des éléments devant figurer à minima dans l'analyse d'impact. Il s'agit :

- D'une « description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement »[112].
- D'une « une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités »[113].
- D'une « évaluation des risques pour les droits et libertés des personnes concernées »[114] ; et
- Des « mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement »[115].

Lorsque l'analyse d'impact révèle que le traitement fait peser un risque élevé sur les droits des individus concernés, l'autorité de contrôle doit être consultée de façon préalable par le responsable du traitement[116]. Avec cet outil, il s'agit d'éviter qu'un responsable de traitement ne mette en danger les droits fondamentaux des individus et de faire en sorte que le responsable de traitement, lui-même, soit protégé face à un risque de violation, par son fait, du RGPD.

8.4 La désignation d'un délégué à la protection des données.

Le délégué à la protection des données (ci-après « DPO » pour data protection officer) est un organe ayant pour missions d'informer, conseiller[117] et contrôler[118] le responsable du

---

[111] A ce sujet, la Cnil a publié une série de 3 documents en juin 2015 et juin 2012 relative aux études d'impact sur la vie privée. Voir Cnil, *PIA : la méthode ; PIA : les outils ; Mesures pour traiter les risques sur les libertés et la vie privée.* [Disponible en ligne] https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil, [consulté le 13 janvier 2018].
[112] RGPD, Art.35, §7, a).
[113] RGPD, Art.35, §7, b).
[114] RGPD, Art.35, §7, c).
[115] RGPD, Art.35, §7, d).
[116] RGPD, Art. 36.
[117] RGPD, Art. 39, §1, a).

traitement, mais aussi les éventuels sous-traitants et les employés vis-à-vis de la règlementation, européenne ou nationale, en matière de protection des données. C'est aussi le DPO qui assure le lien entre l'organisme pour lequel il travaille (entreprise, association, …) et l'autorité de contrôle, c'est-à-dire la Cnil pour le cas français. Il est le véritable interlocuteur, le « point de contact »[119] avec lequel que l'autorité de contrôle sera amenée à « coopérer »[120] sur tout point relatif à la protection des données à caractère personnel concernant l'organisme pour lequel le DPO travaille.

Le RGPD impose la désignation d'un tel délégué dans 3 situations :

- Tout d'abord, lorsque « le traitement est effectué par une autorité publique ou un organisme public »[121]. Ne sont bien sûr pas visées les juridictions à partir du moment où elles agissent dans l'exercice de leurs fonctions juridictionnelles.
- Ensuite lorsque « 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 leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées »[122].
- Enfin, lorsque « les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données[123] […] et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 »[124].

En dehors de ces situations obligatoires, tout organisme peut, bien entendu, désigner un DPO. Ce DPO est donc avant tout un facilitateur des relations entre autorité de protection et responsable du traitement, ainsi qu'un organe visant à faire en sorte que la réglementation en matière de protection des données à caractère personnel puisse être respectée la mieux possible au quotidien et au plus près des acteurs de la *data*.

8.5 L'élaboration de codes de conduite

Ce mécanisme est envisagé par l'article 40 du RGPD :

> « 1. Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises.
> 2. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement ».

Une fois élaboré, tout code de conduite doit être soumis à l'autorité de contrôle pour validation[125]. Pour la France, il s'agit de la CNIL. Les codes de conduite approuvés sont ensuite publiés[126] et les responsables de traitement peuvent alors s'y référer. A noter que les codes de conduite sont également soumis à approbation des autorités de contrôle lorsqu'ils sont modifiés

---

118 RGPD, Art. 39, §1, b).
119 RGPD, Art. 39, §1, e).
120 RGPD, Art. 39, §1, d).
121 RGPD, Art. 37, §1, a).
122 RGPD, Art. 37, §1, b).
123 D'après l'article 9 du RGPD : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identification d'une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
124 RGPD, Art. 37, §1, c).
125 RGPD, Art. 40, §5.
126 RGPD, Art. 40, §6.

ou prorogés.

Le RGPD prévoit également la mise en place possible de code de conduite communs à plusieurs États membres. Ces codes doivent alors être soumis par les autorités de contrôle au Comité[127] – réunion des différentes autorités de contrôle nationales – puis, en cas d'adoption, sont également soumis à approbation de la Commission européenne[128] qui, en cas d'adoption, sera en charge de leur publication[129].

8.6 La mise en place de mécanismes de certification.

Ceci est prévu par l'article 42 du RGPD :

> « Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement ».

L'accession des responsables de traitements à ces mécanismes de certification est basée sur le volontariat[130] et ne diminue aucunement leur responsabilité[131]. Il s'agit plutôt d'un élément allant dans le sens de la reconnaissance que le responsable du traitement a fait preuve de diligence. Cela ne le soustrait pas à ses responsabilités mais constitue une preuve de la bonne du responsable du traitement quant au respect du RGPD. Les certifications peuvent être délivrées directement par l'autorité de contrôle, selon ses propres critères ou ceux du Comité, ou par des organismes de certification agrées par les autorités de contrôle[132].

8.7 Les nouvelles prérogatives des autorités de contrôle nationales.

La place des autorités de contrôle est réaffirmée par le RGPD. Elle est même renforcée sur certains points. C'est par exemple le cas concernant les codes de conduites. En effet, « en cas de violation du code par un responsable du traitement ou un sous-traitant, [l'autorité de protection] peut notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code »[133]. Mais c'est aussi, et de façon plus spectaculaire, au niveau des amendes administratives pouvant être infligées en cas de violation du RGPD que l'on peut apprécier à quel point les autorités de protections sont confortées dans leurs missions. Ainsi, aux termes de l'article 83, elles peuvent adresser des amendes administratives pouvant s'élever dans certains cas jusqu'à 10 000 000.€ ou 2% du chiffre d'affaire mondial annuel d'une entreprise[134]. Le plafond est constitué par la somme la plus élevée des deux. Pour les violations les plus graves[135], les montants peuvent même s'élever jusqu'à 20 000 000 € ou 4% du chiffre d'affaire mondial annuel d'une entreprise[136].

---

127 RGPD, Art. 40, §7.
128 RGPD, Art. 40, §8.
129 RGPD, Art. 40, §10.
130 RGPD, Art.42, §3.
131 RGPD, Art.42, §4.
132 RGPD, Art.42, §5 et Art. 43.
133 RGPD, Art.41, §4.
134 RGPD, Art.83, §4.
135 Violation des principes liés au consentement, aux droits des personnes concernées par le traitement (accès, effacement, rectification, …), …
136 RGPD, Art.83, §5.

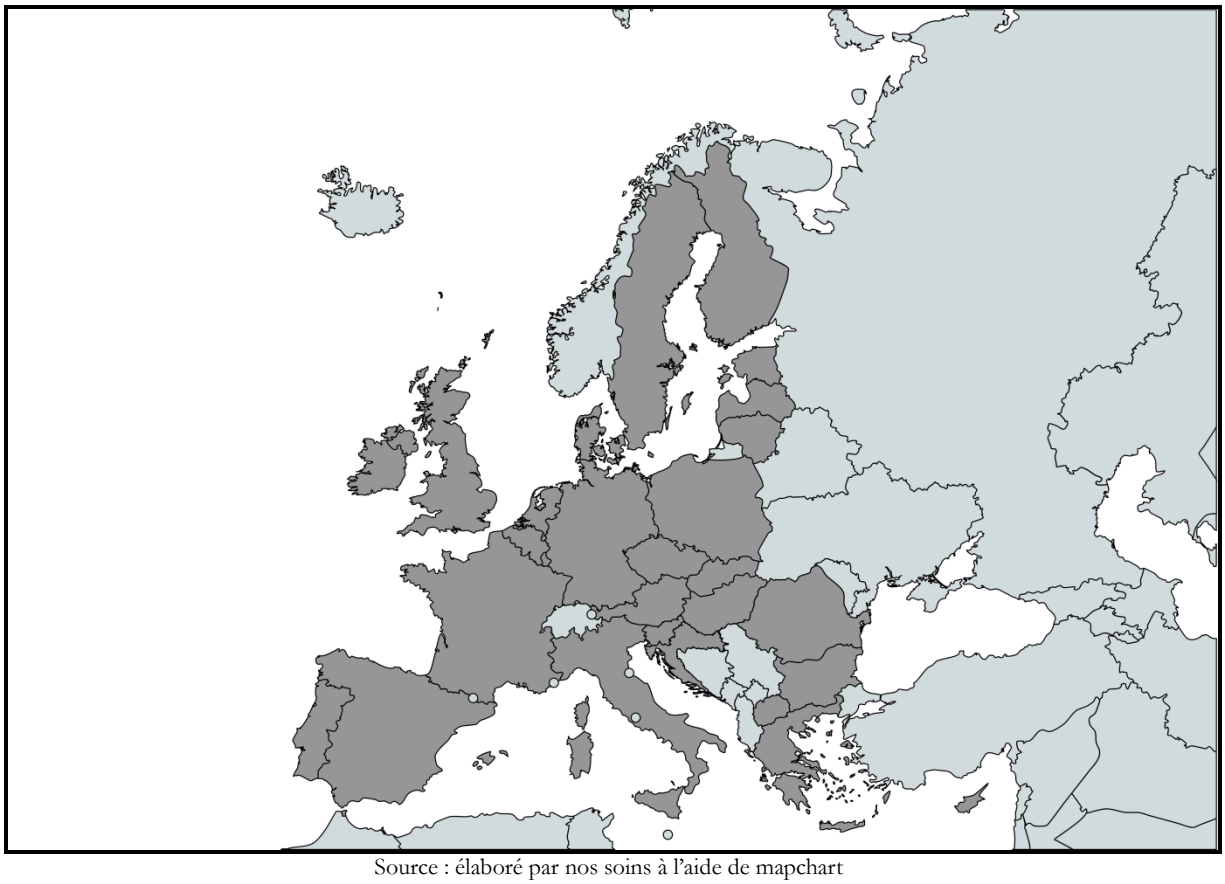
9 L'application géographique du RGPD européen, étendue au-delà de l'UE

* Le RGPD sera appliqué dans 4 espaces[137] :

- (1) le territoire de l'UE
- (2) dans trois pays européens non-membres de l'UE
- (3) et quasiment intégralement dans les pays considérés comme « adéquats » par l'UE
- (4) enfin, au-delà de l'UE à certaines conditions en raison du principe nouveau d'extra-territorialité

- (1) Le RGPD concerne d'abord et principalement un ensemble de **28 pays**, soit plus d'**un demi-milliard de personnes**.

Carte 1 : la zone d'application du RGPD : l'UE des 28

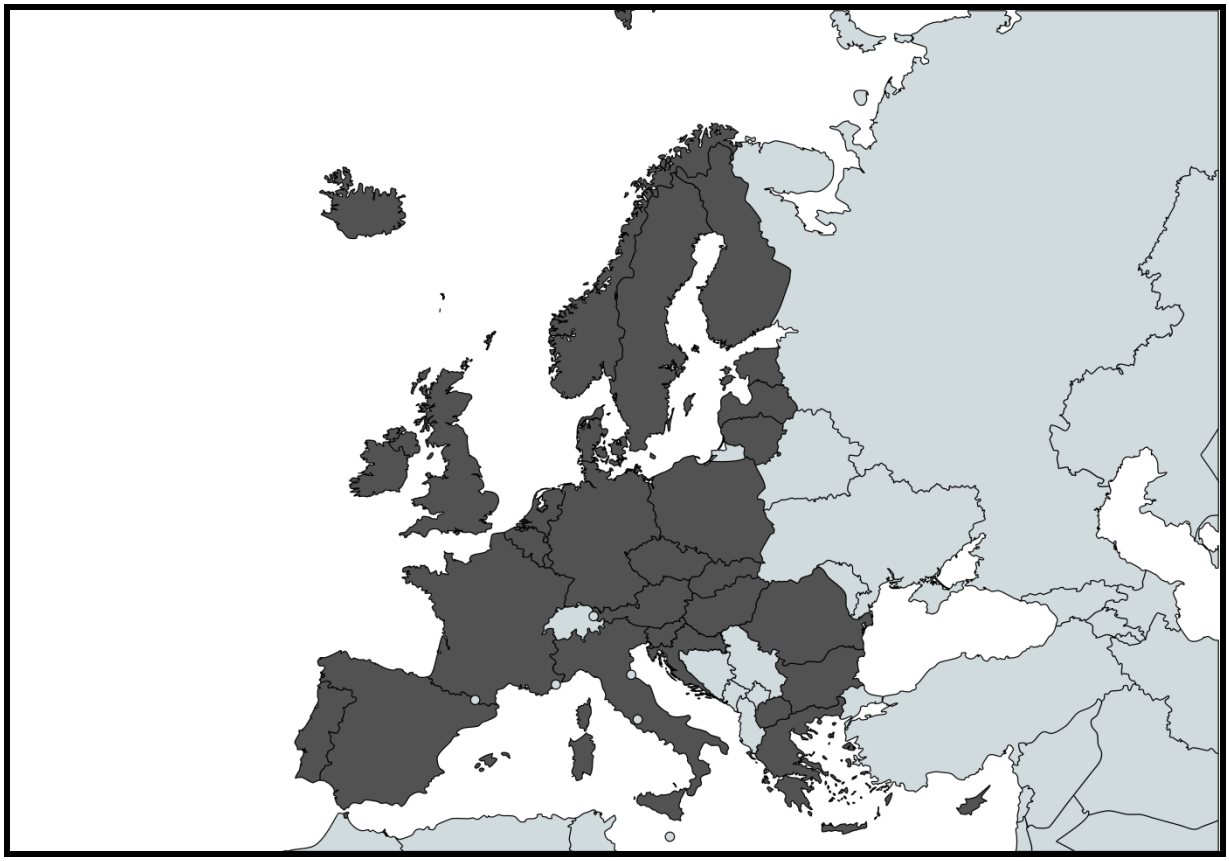


Source : élaboré par nos soins à l'aide de mapchart

[137]. La cartographie présente dans ce document est plus précise que celle publiée par la CNIL (https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde)

- (2) Il faut ajouter qu'il existe des pays européens non membres de l'UE comme l'Islande, le Liechtenstein et la Norvège mais qui **verront s'appliquer le RGPD** dans le cadre de leur appartenance à l'Espace Economique Européen (EEE).

Carte 2 : la zone étendue d'application d'une législation de type RGPD



Source : élaboré par nos soins à l'aide de mapchart

- **(3)** Par ailleurs, selon la Commission européenne les **pays** avec lesquels il est possible d'assurer un transfert de données parce qu'ils **offrent un niveau** de **protection « adéquat »**[138] (à entendre comme conforme aux principes du droit des données dans l'UE sans pour autant être une copie du RGPD[139]) figurent sur la carte ci-dessous : **l'Uruguay, l'Argentine, la Suisse, Israël, la Nouvelle-Zélande et l'Andorre, les îles Féroé, Jersey et Guernesey, enfin l'île de Man**. Il faut noter que les décisions de la Commission dans le cas du Canada et des États-Unis sont des décisions de constats « d'adéquations partiels » seulement. Par ailleurs, des discussions sont en cours avec la Corée et le Japon. Le contenu détaillé des constats d'adéquations partiels n'est pas connu.

L'objectif pour l'UE a été double et ambitieux : ne pas marginaliser les flux de l'Europe et s'imposer comme productrice de normes exigeantes dans le monde. Il semble que cette attitude ne soit pas illusoire : selon Greenleaf, 76 pays avaient adopté des législations en matière de protection des données en 2011 et 120 en 2017[140]. Cependant le constat de Greenleaf paraît purement arithmétique, car au-delà du standard que constitue le fait d'avoir une législation spécifique le niveau de protection est en fait très inégal selon les pays. Il semble que la convention 108 sur les données personnelles du Conseil de l'Europe, ratifiée par 51 pays en 2017, puisse être considérée comme un plus petit dénominateur commun : elle est en tout cas le texte le plus protecteur pour les données[141]. Encore n'est-elle pas suffisante (en particulier elle est obsolète à certains égards car elle date de 1981) du point de vue d'une l'UE particulièrement exigeante car, comme on vient de le voir, rares sont les pays à être considérés comme « adéquats » par l'UE. Le RGPD a d'ailleurs ambitionné après la directive de 1995 de dépasser cette obsolescence.

---

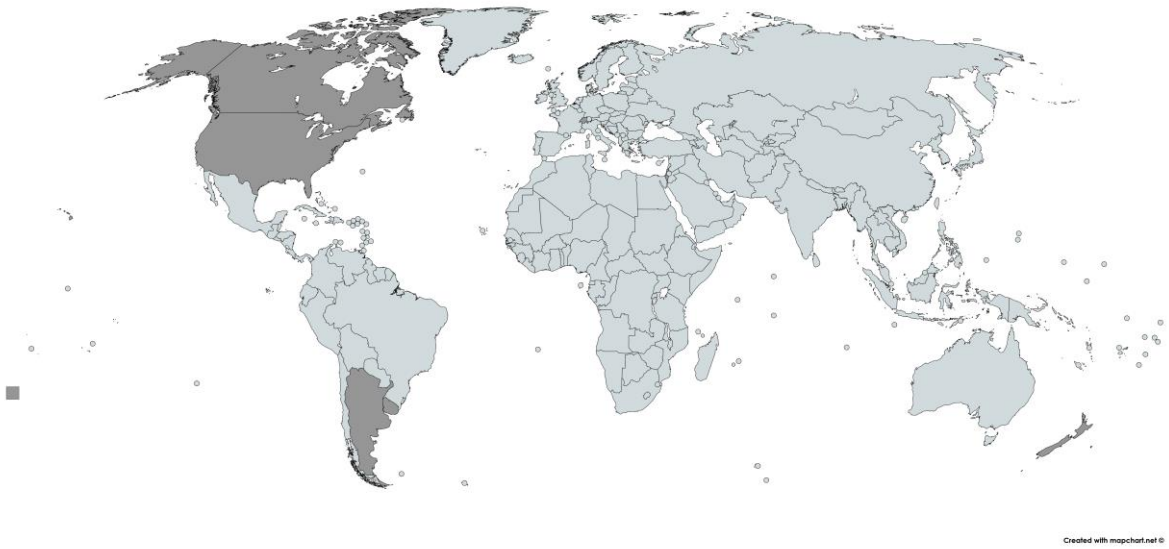
138. Commission européenne, Échange et protection de données à caractère personnel à l'ère de la mondialisation. *Communication de la commission au Parlement européen et au conseil*, 10 janvier 2017, 18 p. http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-7-F1-FR-MAIN-PART-1.PDF

139. *Ibid*., p. 7.

140. Graham Greenleaf, « Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey », (2017), 145 Privacy Laws & Business International Report, 10-13; UNSW Law Research Paper No. 45, available at SSRN: https://ssrn.com/abstract=2993035, 8 p.

141. UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, 2016, UNCTAD, p. 25.

Carte 3 : les pays considérés comme « adéquats » et « adéquats partiels » en protection des données pour l'UE selon la commission européenne



Source : élaboré par nos soins à l'aide de mapchart

- **(4) enfin au-delà de l'UE** à certaines conditions en raison du principe nouveau d'extra-territorialité.

De façon générale, il faut souligner qu'en matière de champ d'application territorial, le RGPD demeure dans la lignée de la directive 95/46 précédente, à savoir que le champ d'application est entendu de façon particulièrement large, ceci, dans le but de protéger le plus efficacement possible les individus. Le RGPD apporte cependant une nouveauté fondamentale en consacrant spécialement un article à la question de son champ d'application territorial, lequel entérine un principe d'application du droit au-delà des limites territoriales de l'UE, c'est-à-dire un **principe d'extraterritorialité**.

> Article 3 du RGPD – Champ d'application territorial.
> 1. 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.
> 2. Le présent règlement 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, lorsque les activités de traitement sont liées :
> 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.
> 3. Le présent règlement s'applique 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 ».

Le règlement prend en compte deux paramètres :

1. la localisation de l'établissement mettant en œuvre le traitement de données,
2. la localisation des personnes objets du traitement de données.

Il s'agit en fait de rendre applicable le RGPD à tout établissement présent dans l'UE mettant en œuvre un traitement de données « dans le cadre de ses activités » (quel que soit le lieu où est réalisé le traitement) et à tout établissement hors de l'UE mettant en œuvre un traitement à l'égard d'une personne résidant dans l'UE.

En synthèse, l'UE doit être une zone d'application du RGPD, que ce soit pour les créateurs du traitement de données ou pour ceux qui en sont l'objet, c'est-à-dire les personnes résidentes sur le territoire de l'UE (et non pas seulement les citoyens de l'UE).

Il convient par ailleurs de noter que la CJUE a pu adopter une conception particulièrement extensive de la directive 95/46 et de ce qu'il faut entendre par un traitement effectué « dans le cadre des activités » d'un établissement du responsable du traitement. Ceci ressort notamment de son arrêt *Google Spain* du 13 mai 2014[142]. Dans le cas considéré, Google Spain opérait pour Google Inc., situé aux États-Unis, afin de vendre des espaces publicitaires en Espagne en utilisant un traitement de données de Google Inc. La CJUE a considéré qu'il suffisait que le traitement de données soit **réalisé « dans le cadre des activités »** de Google Spain sans que ce traitement soit directement réalisé **« par »** Google Spain pour emporter l'application territoriale de la directive 95/46. Or, il ne semble pas que la CJUE ou le législateur européen n'aient laissé entendre un quelconque assouplissement de ce principe avec l'entrée en vigueur du RGPD.

[142] CJUE, grande chambre, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, 13 mai 2014, Aff. C-131/12

10 L'application matérielle du règlement: la « sécurité nationale » en dehors du champ du RGPD

De prime abord, le RGPD semble envisager un champ d'application matériel particulièrement large (10.1.). Il convient toutefois d'être vigilent aux nombreuses exceptions qu'il pose (10.2.).

10.1. Cas matériels d'application du RGPD.

Cette question est réglée par l'article 2 par. 1er du RGPD :

> « Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

On note immédiatement que le RGPD ne précise pas si le traitement de données à caractère personnel, automatisé en tout ou partie ou non, doit être effectué par le responsable du traitement, le sous-traitant, ou les deux, le cas échéant. Ce silence tend à laisser penser que la qualité de responsable de traitement ou de sous-traitant n'entre pas en jeu dans l'identification du champ d'application matériel du RGPD. Ce qui importe est le fait de savoir s'il y a traitement de données à caractère personnel. Pour ce faire, il convient de se référer à la définition apportée par l'article 4, par. 2) du RGPD. On y apprend que constitue un traitement de données à caractère personnel :

> « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la 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, la limitation, l'effacement ou la destruction ».

Cette liste particulièrement large l'est d'autant plus par son caractère non exhaustif, souligné par le terme « telles que ». Les 19 « opérations » citées, ne le sont donc qu'à titre d'illustration, d'exemple. D'autres hypothèses pourront ainsi se voir précisées par les autorités de contrôle, les lignes directrices du Comité, ou encore la jurisprudence, aussi bien par les juridictions nationales, que par la position unificatrice de la CJUE.

Pour autant, l'aspect extensif permis par cette liste ne doit pas nous conduire à ignorer les hypothèses dérogatoires d'application matérielle du RGPD, lesquelles ne sont pas négligeables.

10.2. Exceptions au champ d'application matériel du RGPD.

Les exceptions au champ d'application matériel du RGPD sont prévues aux paragraphes 2 et 3 de l'article 2.

10.2.1 – Les exceptions de l'article 2, paragraphe 2.

Les exceptions de l'article 2, paragraphe 2 sont au nombre de 4 :

a) Une activité ne relevant pas du champ d'application du droit de l'Union[143].

Il s'agit là d'une exception tout à fait classique mais qui, par souci de précision, était néanmoins nécessaire à rappeler. Bien évidemment, d'un point de vue matériel, le RGPD ne peut

[143] RGPD, Art. 2, § 2, a).

s'appliquer pour les cas où les Etats membres n'ont pas entendu transmettre leurs compétences à l'Union par l'intermédiaire des traités. C'est en particulier le cas des activités relatives à la sécurité nationale[144]. Cette matière relevant d'une dimension purement interne aux Etats membres, il s'agit donc d'une hypothèse ne pouvant être considérée comme incluse dans le champ d'application du droit de l'Union. A noter que cet exemple de la **sécurité nationale**, fourni par le considérant n° 16 du RGPD n'est donné qu'à titre d'illustration, ainsi que nous renseigne le terme « telles que ». Une nouvelle fois, ceci signifie que les autorités de contrôle, le Comité ou les juges – nationaux ou de l'Union – pourront, dans leur interprétation du RGPD, préciser les matières qu'ils entendent comme ne relevant pas du droit de l'Union, même si sur ce point, la jurisprudence de la CJUE apporte déjà une lisibilité satisfaisante[145].

Notons que la directive 2016/680 du paquet « données », prévoit, elle aussi, des cas d'exclusion de son application matérielle, lorsqu'est en cause une activité ne relevant pas du champ d'application du droit de l'Union[146]. Les considérants de la directive, outre la **sécurité nationale**, précisent que doivent également être exclues « les **activités des agences ou des services responsables des questions de sécurité nationale** »[147], permettant d'obtenir davantage d'éléments pour qualifier ce qui ne relève pas du champ d'application du droit de l'Union, en matière de traitement de données à caractère personnel.

b) Un traitement opéré par les Etats membres au titre de la politique étrangère et de sécurité commune (PESC)[148].

Comme souvent, le caractère particulier de la PESC, notamment la sensibilité politique de cette matière éminemment régalienne, conduit le législateur de l'Union à l'envisager comme une hypothèse devant faire l'objet d'une exception.

A l'image de ce que nous avons pu voir au point précédent, concernant les activités ne relevant pas du champ d'application du droit de l'Union, cette exception est, elle aussi, réaffirmée par la directive 2016/680. Le considérant n° 14 de cette dernière explique que « le traitement de données à caractère personnel par les Etats membres dans le cadre d'activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne »[149], c'est-à-dire, relevant de la PESC, ne sont « pas considérées comme des activités relevant du champ d'application de la présente directive »[150].

c) Traitement réalisé par une personne physique dans le cadre d'une activité strictement personnelle ou domestique[151].

Cette exception, pragmatique et limpide, n'appelle pas de commentaires particuliers. A titre d'exemple, on imagine mal devoir imposer à un individu, effectuant, pour son propre compte, des recherches généalogiques sur sa famille, dans un cadre strictement personnel, devoir s'embarrasser des contraintes du RGPD.

d) Traitement réalisé 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, y compris la protection contre des menaces pour la sécurité publique et

144 RGPD, considérant n° 16.
145 CJUE, *Procédure pénale c. Bodil Lindqvist*, 06 novembre 2003, Aff. C-101/01, § 38. CJUE, grande chambre, *Huber c. Bundesrepublik Deutschland*, Aff. C-524/06, § 44 et 45.
146 Directive 2016/680, Art. 2, § 3, a).
147 Directive 2016/680, considérant n° 14.
148 RGPD, Art. 2, § 2, b).
149 Directive 2016/680, considérant n° 14.
150 *Ibid.*
151 RGPD, Art. 2, § 2, c).

la prévention de telles menaces.

Cette importante catégorie, autorisant l'exclusion de l'application du RGPD, est très directement liée au champ d'application matériel de la directive 2016/680 du paquet « données ». Cette matière n'est donc pas prise en compte par le RGPD car elle est traitée par cette directive tout particulièrement.

> « La présente directive établit des règles relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[152].

A noter que si la directive 2016/680 reprend, pour l'essentiel, les principes liés à la protection des données à caractère personnel[153], posés par le RGPD, elle laisse toutefois une marge de manœuvre relativement large aux Etats membres, quant à leur application[154].

10.2.2 – Les exceptions de l'article 2, paragraphe 3.

Les exceptions visées par l'article 2, paragraphe 3 du RGPD, concernent les cas de traitement de données à caractère personnel relevant d'une situation purement interne aux institutions de l'Union. Ces hypothèses dérogent au RGPD en raison du fait qu'elles sont régies par un autre texte, à savoir le règlement (CE) n° 45/2001[155].

[152] Directive 2016/680, Art. 1er, § 1 et Art. 2, § 1.

[153] Notamment les droits de la personne concernée par le traitement de données à caractère personnel.

[154] Voir : Directive 2016/680, Art. 13, § 3 et 4, concernant la limitation des informations à mettre à la disposition de la personne concernée ou à lui fournir ; Art. 15 concernant la limitation du droit d'accès de la personne concernée à ses données à caractère personnel ; Art. 16 § 4, concernant la limitation de l'information auprès de la personne concernée quant au refus d'une demande de rectification ou d'effacement de données à caractère personnel.

[155] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil 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.

11 Conclusions (provisoires)

Le principe du « secret des correspondances », s'il est historiquement fondateur, est une norme aussi ancienne que démonétisée juridiquement. La notion de protection des « données personnelles » qui tient compte de la numérisation des communications, l'a remplacée. L'Europe est la partie du monde où l'activité de protection des données personnelles est certainement la plus ancienne et la plus poussée. L'arsenal de normes en la matière est né très tôt, dès le début des années 1970, dans le cadre du Conseil de l'Europe et de l'OCDE. L'UE a ensuite effectué un travail d'intégration de ces normes dans son droit propre par la directive 95/46 de 1995, puis par le RGPD. Si le RGPD offre d'indéniables progrès par l'unicité du droit qu'il permet, par le degré de précision atteint par le texte et par les garanties qu'il offre, il faudra observer avec soin l'effectivité concrète des droits consacrés. Il s'agira notamment d'être vigilant sur le décalage pouvant exister entre principes juridiques et réalités numériques. On peut d'ores et déjà relever que ce qui a trait à la sécurité nationale ne s'inscrit pas dans le champ d'application matériel du règlement, mais renvoie à la directive 2016/680 du paquet « données » avec des contraintes très atténuées pour ceux qui ordonnent (les Etats) et ceux qui opèrent (les sociétés) les traitements de données. De ce point de vue, le paquet « données » de 2016 montre que les Etats n'ont pas atténué leur droit à exercer de la surveillance numérique.

12 Annexes

Tableau 13 : tableau de synthèse des principaux arrêts de la CEDH en matière de protection des données à caractère personnel

Juridiction	Date	Arrêt	Thème	Droit concerné	Violation	Source de l'ingérence	Motifs
CEDH	06/09/1978	Klass et autres c. **Allemagne**	Interception des correspondances.	Art.8 – Respect de la vie privée et du secret des correspondances.	Non	Surveillance des correspondances et des communications téléphoniques.	Nécessaire dans une société démocratique à la sécurité nationale, la défense de l'ordre et la prévention d'infractions pénales.
CEDH	02/08/1984	Malone c. **Royaume-Uni**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Délit de recel de biens volés : interception des communications postales et téléphoniques. Comptage du téléphone.	Surveillance non prévue par la loi.
CEDH	23/03/1987	Leander c. **Suède**	Conservation et exploitation de données personnelles. Accès aux données personnelles.	Art.8 – Respect de la vie privée.[156]	Non	Sur l'utilisation d'un fichier secret de police faisant mention du passé syndical du requérant pour refuser son embauche.	Système suédois de contrôle du personnel présentant suffisamment de garanties. Protection de la sécurité nationale prévalant sur les intérêts individuels du requérant.
CEDH	07/07/1989	Gaskin c. **Royaume-Uni**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur un individu pris en charge par les services sociaux lors de son	Méconnaissance de l'intérêt que pouvait avoir le requérant à

[156] En substance, les débats reviennent sur de nombreux principes consacrés par la Convention 108 de 1981 pour la protection des personnes à l'égard du traitement automatisé des **données à caractère personnel**, mais la Suède ne ratifie ce texte que le 29 septembre 1982, là où les faits de l'affaire se déroulent durant l'été 1979. La CEDH ne fait donc pas référence à la Convention 108 contrairement à d'autres affaires qui suivront.

						enfance et cherchant à connaître son passé mais dont l'accès à son dossier lui fut refusé.	recevoir les renseignements nécessaires pour comprendre son enfance
CEDH	24/04/1990	Kruslin c. **France**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Instruction pour assassinat : écoutes téléphoniques ordonnées par un juge d'instruction.	Droit pas assez clair sur l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités en matière d'écoutes.
CEDH	24/04/1990	Huvig c. **France**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Instruction pour fraude fiscale : écoutes téléphoniques ordonnées par un juge d'instruction.	Droit pas assez clair sur l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités en matière d'écoutes.
CEDH	25/02/1997	Z c. **Finlande**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la protection des données confidentielles relatives à la santé : révélation de la séropositivité de la requérante au cours d'une procédure pénale dirigée contre son mari.	Divulgation non justifiée. Législation interne devant ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties de la Convention
CEDH	25/06/1997	Halford c. **Royaume-Uni**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Interception de conversations téléphoniques transmises par un système de télécommunications interne à la police et par le	Absence de règlementation en droit interne concernant l'interception de conversations téléphoniques.

						réseau public.	
CEDH	27/08/1997	M.S. c. **Suède**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée	Non	Sur la communication par un service de gynécologie à un organisme de sécurité sociale du dossier médical de la requérante.	Justifié au nom de la protection du bien-être économique du pays. Le service a pu transmettre le dossier afin que soient opérées les vérifications nécessaires relatives au versement d'indemnités.
CEDH	25/03/1998	Kopp c. **Suisse**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Mise sur écoute du téléphone d'un cabinet d'avocats par le procureur général de la Confédération.	Droit pas assez clair sur les modalités des écoutes.
CEDH /GC	16/02/2000	Amann c. **Suisse**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Etablissement d'une fiche par les services de renseignement suisses pour un appel passé au requérant par l'ambassade soviétique.	Ingérences non prévues par la loi et droit trop imprécis.
CEDH / GC	04/05/2000	Rotaru c. **Roumanie**	Droit à la rectification et à l'effacement de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Le requérant se plaignait de l'impossibilité de réfuter les données, selon lui contraires à la réalité, détenues dans un dossier à son sujet par le Service roumain des renseignements (SRI).	La Cour estime que la détention et l'utilisation par le SRI d'information sur la vie privée du requérant n'étaient pas prévues par la loi et que celle-ci ne fixe pas de limites quant à l'ancienneté des informations détenues et la durée de leur conservation.
CEDH	25/09/2001	PG et JH c. **Royaume-Uni**	Interception des correspondances.	Art.8 – Respect de la vie privée.	Oui	Ecoutes cachées menées par la police dans ses	Pas de système légal.

						locaux.	
			Collecte de données personnelles.		Oui	Sonorisation d'un appartement	Dispositif de sonorisation non prévu par la loi.
					Non	Obtention de renseignements relatifs à l'usage d'un téléphone dans le cadre d'une enquête et d'un procès portant sur une association de malfaiteurs en vue de perpétrer un vol qualifié.	Mesure nécessaire dans une société démocratique.
CEDH	22/10/2002	Taylor-Sabori c. **Royaume-Uni**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Interception par la police de messages sur messager de poche dans le cadre d'une opération de surveillance spéciale.	Pas de disposition légale. Ingérence non prévue par la loi.
CEDH	29/01/2003	Peck c. **Royaume-Uni**	Respect de la vie privée. Finalité de la collecte de données.	Art.8 – Respect de la vie privée.	Oui	Sur la divulgation dans les médias d'une séquence enregistrée dans la rue par une caméra de télévision en circuit fermé d'une mairie, montrant le requérant en train de se trancher les veines.	Divulgation de la séquence litigieuse par le conseil municipal non entourée de garanties suffisantes et ayant porté une atteinte disproportionnée et injustifiée à la vie privée du requérant.
CEDH / GC	13/02/2003	Odièvre c. **France**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Non	Sur le cas d'une requérante abandonnée à sa naissance aux services de l'Assistance publique par sa mère qui demanda le secret de son identité vis-à-vis de son enfant et ne pouvant obtenir d'éléments sur sa famille	La requérante a déjà eu accès à quelques éléments sur sa famille biologique. Par ailleurs, la législation français, avec la loi de 2002 tentait d'atteindre un équilibre et une proportionnalité

						biologique.	suffisante entre les intérêts en cause en facilitant les recherches des origines biologiques.
CEDH	17/07/2003	Perry c. **Royaume-Uni**	Exploitation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Surveillance vidéo secrète par la police à des fins d'identification d'un individu ayant commis une série de vols.	Ingérence non prévue par la loi.
CEDH	31/05/2005	Vetter c. **France**	Collecte de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sonorisation d'un appartement entrainant poursuite pour homicide	Droit pas assez clair
CEDH / GC	19/10/2005	Roche c. **Royaume-Uni**	Respect de la vie privée.	Art.8 – Respect de la vie privée.	Oui	A propos d'un requérant soutenant que ses problèmes de santé étaient le résultat de sa participation à des tests sur le gaz moutarde et sur un gaz neurotoxique effectués sous les auspices des forces armées britanniques et accusant cette dernière de ne pas lui avoir fourni toutes les informations nécessaires pour appréhender les risques liés à ces essais.	Le Royaume-Uni n'a pas satisfait l'obligation positive qui lui incombait d'offrir au requérant une procédure effective et accessible qui eût permis à l'intéressé d'avoir accès à l'ensemble des informations pertinentes et appropriées, et ainsi d'évaluer tout risque auquel il avait pu être exposé lors de sa participation aux tests.
CEDH	22/12/2005	Wisse c. **France**	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Enregistrement de conversations téléphoniques et au parloir d'individus en détention avec leurs proches	Droit pas assez clair sur les possibilités d'ingérence. Enregistrement systématique déniant toute utilité du parloir

							en matière de maintien de la vie privée.
CEDH	14/02/2006	Turek c. **Slovaquie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Le requérant alléguait que la conservation d'un dossier de l'ancien service de sécurité de l'ex-Tchécoslovaquie communiste dans lequel il était inscrit sur la liste des agents de ce service, le refus de lui délivrer un « certificat de sécurité », le fait de le débouter de son action en contestation de cette inscription et les conséquences que ces décisions avaient eues pour lui emportaient violation de son droit au respect de sa vie privée.	Absence de procédure par laquelle le requérant aurait pu obtenir la protection de son droit au respect de sa vie privée.
CEDH	06/06/ 2006	Segerstedt-Wiberg et autres c. **Suède**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Non	Accès aux données à caractère personnel détenus par des services de renseignement.	Marge d'appréciation laissée aux États concernant leur sécurité nationale et la lutte contre le terrorisme.
			Droit à l'effacement de données personnelles.	Art.13 – Droit à un recours effectif.	Oui	Demande de suppression.	Pas de recours judiciaire direct pour obtenir la suppression des données les concernant.
CEDH	29/06/2006	Panteleyenko c. **Ukraine**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la divulgation, lors d'une audience judiciaire, d'informations confidentielles concernant la santé mentale et le	Divulgation illégale au regard de la loi ukrainienne de 2000 sur l'assistance médicale psychiatrique.

						traitement psychiatrique du requérant.	
CEDH	10/10/2006	LL c. **France**	Exploitation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur l'utilisation de pièces médicales concernant le requérant, dans une procédure de divorce, sans son consentement.	Ingérence subie par le requérant dans sa vie privée non justifiée au vu du rôle fondamental joué par la protection des données à caractère personnel.
CEDH	01/07/2008	Liberty et autres c. **Royaume-Uni**	Interception des correspondances. Collecte et conservation de données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Sur l'interception, par le ministère britannique de la défense, de communications par téléphone, par télécopie et par courriel, dont certaines contenaient des informations juridiques couvertes par le secret professionnel et des renseignements confidentiels.	Droit interne applicable à l'époque des faits n'offrant pas une protection appropriée contre l'abus de pouvoir. Pas d'indication sur les durées de conservation ou la destruction des données.
CEDH	25/11/2008	Armonas c. **Lituanie** Biriuk c. **Lituanie**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la publication dans le plus grand quotidien lituanien de noms de personnes séropositives.	Condamnation de la Lituanie en raison des faibles indemnités accordées aux requérants par les tribunaux lors de la divulgation de leur séropositivité. Nécessité de garantir la confidentialité des requérants.
CEDH	02/12/2008	K.U. c. **Finlande**	Protection des données en ligne. Divulgation de	Art.8 – Respect de la vie privée.	Oui	A propos d'un mineur de 12 ans ayant vu nombre de ses données personnelles usurpées et	Obligation positive de l'État finlandais de protéger la vie privée jusque dans le relations

			données personnelles.			mises en lignes pour la réalisation d'une annonce de rencontre et sur le refus du fournisseur d'accès à internet d'identifier l'individu associé à l'adresse IP.	entre les individus.
CEDH / GC	04/12/2008	S et Marper c. **Royaume-Uni**	Conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Rétention indéfinie de données d'empreintes digitales et ADN après acquittement dans procédure pénale.	La conservation de données en cause s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique.
CEDH	28/04/2009	K.H. et autres c. **Slovaquie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	A propos de huit femmes d'origine rom, se retrouvant dans l'impossibilité de procréer après avoir été traitées dans les services gynécologiques de deux hôpitaux soupçonnant d'y avoir été stérilisées durant leur séjour et n'ayant pu avoir accès à leur dossier médical.	La Cour explique que les personnes qui souhaitent obtenir des photocopies de documents renfermant des informations à caractère personnel les concernant n'ont pas à devoir expliquer précisément pourquoi elles en ont besoin et que c'est, au contraire, aux autorités détentrices d'éléments de ce type qui ne souhaiteraient pas les produire de justifier leur refus par des

							motifs impérieux.
CEHD	27/10/2009	Haralambie c. **Roumanie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Accès aux données à caractère personnel détenues par des services de renseignement.	Difficultés d'accès excessives. Durée pour obtention d'informations trop longue.
CEDH	17/12/2009	BB c. **France** Gardel c. **France** MB c. **France**	Conservation de données personnelles.	Art.8 – Respect de la vie privée et protection des données à caractère personnel.	Non	Inscription d'agresseurs sexuels sur le fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS).	Traitement automatisé ayant pour finalité des objectifs de prévention, conservation limitée à 30 ans proportionnel aux objectifs poursuivis.
CEDH	18/05/2010	Kennedy c. **Royaume-Uni**	Interception de correspondances Collecte et conservation de données personnelles.	Art.8 – Respect de la vie privée.	Non	Soupçon d'interception de communications par la police – Procédure de vérification.	Justifié et législation suffisamment claire.
CEDH	02/09/2010	Uzun c. **Allemagne**	Collecte, conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée	Non	Surveillance données GPS. Soupçon de participation attentats à la bombe.	But légitime de protection de la sécurité nationale, de la sûreté publique, de la protection des victimes et de la prévention des infractions pénales. Mesure proportionnée.
CEDH	10/02/2011	Dimitrov-Kazakov c. **Bulgarie**	Conservation de données personnelles.	Art.8 – Respect de la vie privée et protection des do.nnées à caractère personnel	Oui	Inscription comme délinquant sur des registres de police après interrogatoire sans poursuite future.	Inscription au registre non prévue par la loi.
				Art. 13 – Droit à un recours effectif	Oui		Pas de recours prévu.
CEDH	24/05/2011	Association « 21 Décembre 1989 » et	Interception des correspondances.	Art.8 – Respect de la vie privée et respect du secret	Oui	Acteur des manifestations lors de la chute du régime	La Cour estime qu'il n'y a pas, dans la

		autres c. **Roumanie**		des correspondances.		communiste roumain, Teodor Mărieş estime faire l'objet, en tant que président de l'association requérante, de mesures de surveillance secrète, en particulier d'écoutes téléphoniques.	législation nationale, de garanties suffisantes, ce qui a conduit à ce que les informations recueillies en 1990 par les services de renseignement au sujet de M. Mărieş soient encore conservées par ceux-ci 16 ans plus tard, en 2006, et qui génère pour M. Mărieş un risque sérieux de voir ses communications téléphoniques mises sur écoute.
CEDH	21/06/2011	Shimovolos c. **Russie**	Conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Enregistrement d'un militant des droits de l'Homme dans une base de donnés relative aux surveillances secrètes et à ses déplacements.	Dispositions régies par un arrêté ministériel jamais publié. Donc droit pas assez clair.
CEDH	19/07/2011	Jarnea c. **Roumanie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Le requérant avait fait l'objet de surveillance par l'ancienne police politique roumaine (*Securitate*). Il souhaite avoir accès aux informations collectées à son sujet, ce qu'il obtient, mais soupçonne que le fichier qui lui a été soumis est incomplet.	La Cour estime que l'État n'a pas satisfait à l'obligation positive qui lui incombait d'offrir au requérant une procédure effective et accessible lui permettant d'avoir accès dans un délai raisonnable à l'ensemble des informations pertinentes le

							concernant qui avaient été recueillies par l'ancienne *Securitate* et qui se trouvaient encore en possession des autorités publiques.
CEDH	18/10/2011	Khelili c. **Suisse**	Conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la mémorisation de données erronées portant atteinte à la vie privée. Fichage d'une femme comme prostituée.	Mention dans un tel fichier non justifié dans une société démocratique. Ne justifie pas une telle ingérence dans le respect de la vie privée.
CEDH	25/09/2012	Godelli c. **Italie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur le secret de la naissance et l'impossibilité pour une personne abandonnée par sa mère d'obtenir des éléments non identifiants sur sa famille naturelle.	La Cour conclut à la violation estimant notamment qu'un juste équilibre n'avait pas été ménagé entre les intérêts en présence
CEDH	13/11/2012	MM c. **Royaume-Uni**	Conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Maintien du nom du requérant dans un fichier relatif à l'enlèvement d'enfants initialement pour 5 ans puis prolongé de façon illimitée.	Conditions de conservation et de divulgation des données non prévues par la loi.
CEDH	08/01/2013	Bucur et Toma c. **Roumanie**	Divulgation de données personnelles.	Art.10 – Liberté d'expression.	Oui	A propos d'un employé du service roumain de renseignements ayant été condamné pénalement à la suite de la divulgation d'informations classées « ultra-secrètes ».	Question particulièrement importante au regard de l'histoire roumaine, touchant directement la société civile et concernant les fondements de la démocratie roumaine. Affaire relevant d'un

							débat politique dans une société démocratique, dont l'opinion publique a un intérêt légitime à être informée.
CEDH	18/04/2013	MK c. **France**	Conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Conservation de données sur le requérant, à l'issue d'enquêtes pour vol, au fichier automatisé des empreintes digitales, même après avoir été innocenté.	Marge d'appréciation de l'État outrepassée en la matière, car ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Atteinte disproportionnée au droit du requérant au respect de sa vie privée ne pouvant passer pour nécessaire dans une société démocratique
CEDH	24/09/2013	Antoneta Tudor c. **Roumanie**	Accès aux données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur l'impossibilité, pour la requérante, d'obtenir l'accès à l'ensemble des fichiers et documents détenus par les anciens services secrets du régime communiste à propos de feu son père.	La Cour estime que l'État n'a pas satisfait à l'obligation positive qui lui incombait d'offrir à la requérante une procédure effective et accessible lui permettant d'avoir accès dans un délai raisonnable à l'ensemble des informations recueillies à propos de feu son père par l'ancienne *Securitate* et qui se

							trouvaient encore en possession des autorités publiques.
CEDH	29/04/2014	L.H. c. **Lettonie**	Collecte de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Collecte de données médicales personnelles sans le consentement de la personne concernée par un organisme d'État.	Imprécision des dispositions du droit interne autorisant l'accès d'un organisme public au dossier médical de la requérante.
CEDH	06/06/2013	Avilkina et autres c. **Russie**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la divulgation de dossiers médicaux de certains membres des Témoins de Jéhovah russes aux autorités de poursuite russes à la suite de leur refus de subir des transfusions sanguines durant leur séjour dans des hôpitaux publics et afin de pouvoir identifier cette communauté.	Les autorités n'ont pas cherché l'équilibre entre, d'une part, le droit des requérantes au respect de leur vie privée et, d'autre part, l'objectif de protection de la santé publique poursuivi par le procureur.
CEDH	15/04/2014	Radu c. **République de Moldova**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur la divulgation par un hôpital public des données médicales de la requérante à son employeur, lequel relaya les informations sur le lieu de travail aboutissant à une fausse couche de la requérante en raison du stress généré.	Condamnation en raison du fait qu'une telle ingérence n'était pas prévue par la loi.
CEDH	18/09/2014	Brunet c. **France**	Conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Inscription du requérant dans le fichier STIC (Système de traitement des infractions constatées)	État ayant outrepassé sa marge d'appréciation en la matière. Atteinte disproportionnée au

						malgré le classement sans suite de la procédure pénale engagée contre lui.	droit du requérant au respect de sa vie privée ne pouvant passer pour nécessaire dans une société démocratique
CEDH	15/01/2015	Dragojević c. **Croatie**	Interception des correspondances. Collecte et conservation de données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Surveillance secrète des communications en matière de stupéfiants.	Législation pas assez claire sur le pouvoir discrétionnaire donné aux autorités.
CEDH	03/09/2015	Sõro c. **Estonie**	Divulgation de données personnelles.	Art.8 – Respect de la vie privée	Oui	Divulgation de données à caractères personnel relatives à l'activité d'un individu en tant qu'ancien agent du KGB. Préjudice sur son droit au respect de la vie privée.	Mesures non proportionnées au but poursuivi.
CEDH	27/10/2015	RE c. **Royaume-Uni**	Interception des correspondances. Collecte, conservation et effacement de données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Surveillance secrète des consultations entre détenus et avocats.	Directives sur la collecte, le stockage et la destruction des communications surveillées, bien qu'existantes, n'étaient pas encore applicables au moment des faits.
					Non	Surveillance secrète des consultations entre détenus vulnérables (mineurs, personnes atteintes de troubles, …) et personnes appropriées (tuteurs, proches, expert).	Pas de protection du secret professionnel comme cela est le cas dans le cas d'une consultation juridique. Exigences moindres. Législation interne suffisamment protectrice.
CEDH /	04/12/2015	Roman Zakharov c.	Interception des	Art.8 – Respect de la vie	Oui	Interception secrète des	Législation ne

GC		**Russie**	communications. Collecte et conservation de données personnelles.	privée, respect du secret des correspondances.		communications de téléphonie mobile russe. En l'espèce, d'un rédacteur en chef d'une maison d'édition.	prévoyant pas les garanties adéquates contre toute ingérence arbitraire, ni contre toute conservation automatique des données interceptées.
CEDH	12/01/2016	Szabo et Vissy c. **Hongrie**	Interception des communications. Collecte, conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée, respect du secret des correspondances.	Oui	Opérations secrètes de surveillance antiterroriste.	Législation ne fournissant pas les garanties nécessaires pour prévenir les abus.
				Art.13 – Droit à un recours effectif.	Non	Absence de contrôle juridictionnel des opérations secrètes de surveillance antiterroristes.	L'article 13 ne peut être interprété comme exigeant un recours contre l'état du droit interne
CEDH	07/06/2016	Karabeyoğlu c. **Turquie**	Interception des correspondances. Collecte, conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Non	Procureur turc ayant fait l'objet de mesures de surveillances téléphoniques dans le cadre d'une enquête pénale d'une part, …	Ingérence nécessaire à la protection de la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales, prévue par la législation nationale - accessible et prévisible - et subordonnée à une série de conditions limitatives.
					Oui	… et d'une enquête disciplinaire d'autre part.	Utilisation des mêmes données non prévue par la loi en matière d'enquête disciplinaire.
CEDH	18/10/2016	Vukota-Bojic c. **Suisse**	Collecte, conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	A l'issue d'un accident de la route, mise sous surveillance de la	Assureur regardé comme une entité publique en droit

						requérante, par des détectives privés, sous instruction de son assureur afin d'obtenir des éléments justifiant une baisse de sa pension d'invalidité.	suisse. Mesure de surveillance non prévue par la loi car pas assez précises.
CEDH / GC	08/11/2016	Magyar Helsinki Bizottság c. **Hongrie**	Accès aux données personnelles. Mise en balance entre protection des données à caractère personnel et liberté d'expression.	Art.10 – Liberté d'expression.	Oui	Sur le refus des autorités de transmettre à une ONG des informations relatives aux avocats commis d'office, les autorités ayant qualifié ces informations de données à caractère personnel non soumises à divulgation selon le droit hongrois.	La Cour estime qu'il n'y a pas eu d'atteinte au droit au respect de la vie privée des avocats commis d'office car en tout état de cause, la demande d'information concernait des données à caractère personnel ne portant pas sur des informations relevant du domaine privé. Le refus ne se justifiait donc pas et a porté atteinte à l'article 10.
CEDH	08/11/2016	Figueiredo Teixeira c. **Andorre**	Collecte, conservation et exploitation de données personnelles.	Art.8 – Respect de la vie privée.	Non	Sur la conservation et la communication à l'autorité judiciaire des données d'appels téléphoniques du requérant suspecté de délit de trafic de stupéfiants.	Ingérence prévue par le droit andorran.
CEDH	22/06/2017	Aycaguer c. **France**	Collecte et conservation de données personnelles.	Art.8 – Respect de la vie privée.	Oui	Sur l'ordre fait au requérant de se soumettre à un prélèvement biologique destiné à un	Réserves, formulées par le Conseil Constitutionnel français relatives à la proportionnalité et à la

						enregistrement dans le fichier national automatisé des empreintes génétiques (FNAEG) et pour lequel son refus d'obtempérer avait donné lieu à une condamnation pénale.	durée de conservation des données du fichier, non suivies. Pas d'équilibre entre les intérêts publics et privés en jeu.
CEDH / GC	27/06/2017	Satakunnan Markkinapörssi Oy et Satamedia Oy c. **Finlande**	Divulgation de données personnelles. Mise en balance entre protection des données à caractère personnel et liberté d'expression.	Art.10 – Liberté d'expression.	Non	Sur l'interdiction de la publication par deux sociétés de données fiscales à caractère personnel relatives à 1,2 millions de personnes car illégal au regard des lois en matière de protection des données selon les autorités finlandaises.	Ingérence prévue par la loi, poursuivant un but légitime de protection de la vie privée d'individus et ménageant un juste équilibre entre le droit à la vie privée et le droit à la liberté d'expression.
CEDH	18/07/2017	Mustafa Sezgin Tanrıkulu c. **Turquie**	Interception des correspondances. Collecte et conservation de données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Interception des communications électroniques de tout personne se trouvait en Turquie.	Mandat d'interception des communications non prévu par la loi.
CEDH / GC	05/09/2017	Bărbulescu c. **Roumanie**	Interception des correspondances. Collecte et exploitation des données personnelles.	Art.8 – Respect de la vie privée et respect du secret des correspondances.	Oui	Décision d'une entreprise privée de mettre fin au contrat d'un de ses employés après avoir surveillé ses communications électroniques et avoir eu accès à leur contenu.	Autorités n'ayant pas protégé le droit au respect de la vie privée du requérant en n'ayant pas déterminé, premièrement, quelles raisons spécifiques avaient justifié la mise en place des mesures

							de surveillance, deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications avait été possible à son insu.

Tableau 14 : tableau de synthèse des principaux arrêts de la CJUE en matière de protection des données à caractère personnel

Juridiction	Date	Arrêt	Texte concerné	Faits et prétentions	Apport
CJUE	06/11/2003	Procédure pénale c. Bodil **Lindqvist**	**Directive 95/46/CE** Art. 3, 8 et 25. (champ d'application – catégories particulières de données – transfert de données vers pays tiers). **Art. 10 ConvEDH**	Mme Lindquivist a créé une page internet pour sa paroisse, sur laquelle figurait nombre de données personnelles, sans que ces dernières n'aient été obtenues avec le consentement des individus concernés. Le ministère public a donc engagé une procédure à son égard.	La CJUE a tout d'abord répondu que l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier (par leur nom, leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps), constitue un traitement de données à caractère personnel au sens de l'art. 3 de la directive 95/46. Concernant l'indication, sur la page internet, du fait qu'une personne s'est blessée au pied et est en congé maladie partiel, la CJUE explique que ceci constitue une donnée à caractère personnel relative à la santé, relevant des catégories particulières de données au sens de l'art. 8 de la directive 95/46. La CJUE considère également que le fait, pour une personne se trouvant dans un Etat membre, d'inscrire des données à caractère personnel sur une page internet stockée auprès d'un fournisseur de services d'hébergement dans le même Etat, les rendant ainsi accessibles à toute personne connectée à internet, ne constitue pas un transfert de données vers un pays tiers. Concernant l'article 10 de la ConvEDH relatif à la liberté d'expression, la CJUE estime que les dispositions de la directive 95/46 ne comportent pas une restriction contraire au principe général de la liberté d'expression. La CJUE rappelle la nécessité pour les Etats membres

					d'assurer un équilibre entre protection des données à caractère personnel et libre circulation de ces données.
CJUE / GC	29/01/2008	Productores de Música de España (**Promusicae**) c. Telefónica de España SAU	**Directive 2000/31/CE** Art. 15 § 2 et 18. **Directive 2001/29/CE** Art. 8 § 1 et 2. **Directive 2004/48/CE** Art. 8.	Promusicae, une association regroupant des producteurs et des éditeurs d'enregistrements musicaux a introduit une demande de mesures préliminaires devant le Tribunal de commerce n° 5 de Madrid contre Telefónica, société de fourniture de services d'accès à l'Internet. Elle a demandé qu'il soit ordonné à Telefónica de révéler l'identité et l'adresse physique de certaines personnes auxquelles cette dernière fournit un accès à l'Internet et dont l'adresse IP ainsi que la date et l'heure de connexion sont connues, au motif que ces personnes utiliseraient le programme d'échange d'archives « peer to peer », pour permettre l'accès, dans le répertoire partagé de leur ordinateur personnel, à des phonogrammes dont les droits d'exploitation appartiennent aux associés de Promusicae, méconnaissant ainsi les droits de propriété intellectuelle.	La CJUE explique ici que les directives visées dans cette affaire n'imposent pas aux États membres de prévoir, dans une situation telle que celle de l'affaire, l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile. Toutefois, le droit communautaire exige desdits États que, lors de la transposition de ces directives, ils veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. La CJUE explique que les juridictions des Etats membres, lorsqu'elles interprètent les directives visées en l'espèce, ne doivent pas entrer en conflit avec le principe général du droit communautaire de la proportionnalité.
CJUE / GC	16/12/2008	Tietosuojavaltuutettu c. Satakunnan **Markkinapörssi** Oy **et**	**Directive 95/46/CE** Art. 3 et 9. (champ d'application – traitement	La société Markkinapörssi collecte auprès des autorités fiscales finlandaises des	La CJUE explique qu'une telle activité de la part des sociétés Markkinapörssi et Satamedia constitue un traitement de données à caractère personnel au sens de

		Satamedia Oy[157].	de données à caractère personnel et liberté d'expression).	données fiscales publiques afin de les publier dans le journal Veropörssi. Les informations comprennent le nom et le prénom d'1,2 million de personnes physiques dont le revenu excède certains seuils ainsi que le montant de leurs revenus du capital et du travail et des indications concernant l'imposition de leur patrimoine. Markkinapörssi a cédé ces données sur CD-ROM à la société Satamedia qui compte les publier via SMS. Des particuliers se sont plaints devant l'autorité finlandaise de protection des données, laquelle a demandé l'interdiction de telles pratiques.	l'article 3 de la directive 95/46. Elle considère également que de telles activités doivent être considérées comme des activités de traitement de données à caractère personnel exercées « aux seules fins de journalisme » au sens de l'article 9 de la directive 95/46, à condition que lesdites activités aient pour seule finalité la divulgation au public, sous quelque moyen de transmission que ce soit, d'informations, d'opinions ou d'idées. La CJUE exclut que ces activités soient réservées aux entreprises de média, et estime qu'elles peuvent être liées à un but lucratif. Il s'agit ensuite aux juridictions nationales d'apprécier le caractère journalistique de l'activité en question.
CJUE / GC	16/12/2008	Heinz **Huber** c. Bundesrepublik Deutschland.	**Directive 95/46/CE** Art. 7, e). (traitement de données nécessaire à une mission d'intérêt public). **Art. 12 § 1, 17, 18, 43 § 1 du TCE.**	M. Huber, ressortissant autrichien, s'est installé en Allemagne en 1996 pour y exercer la profession d'agent d'assurance indépendant. Un certain nombre de données personnelles le concernant ont alors été collectées pour le registre central des étrangers (AZR). M. Huber estimait être discriminé.	La Cour estime qu'il est nécessaire, pour un État membre, de disposer des informations et des documents pertinents aux fins de vérifier, dans le cadre défini par la réglementation communautaire applicable, l'existence d'un droit de séjour sur son territoire dans le chef d'un ressortissant d'un autre État membre ainsi que l'absence de raisons justifiant une restriction à ce droit. De ce point de vue, le registre AZR est légitime. Mais il ne doit pas contenir d'autres données personnelles que celles nécessaire à cette fin et son caractère centralisé ne peut être justifié que pour des raisons d'efficacité de l'application de la règlementation

[157] Pour les suites de l'affaire, voir : CEDH, grande chambre, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, 27 juin 2017, n° 931/13.

					relative au droit de séjour. La Cour estime en revanche qu'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non-ressortissants de cet État membre dans l'objectif de lutter contre la criminalité serait contraire à l'article 12 § 1 CE relatif à l'interdiction des discriminations.
CJUE	07/05/2009	College van burgemeester en wethouders van Rotterdam c. M. E. E. **Rijkeboer**	**Directive 95/46/CE** Art. 12, a). (droit d'accès).	M. Rijkeboer souhaite savoir quelles informations le concernant et provenant de l'administration communale, ont été transmises à de tierces personnes. Le collège des bourgmestre et échevins de Rotterdam ne fait que partiellement droit à sa demande, ce qui génère le contentieux.	L'article 12, a), de la directive 95/46 impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement. Une réglementation limitant ce droit d'accès, ne saurait constituer un juste équilibre des intérêt et obligation en cause.
CJUE / GC	09/03/2010	**Commission européenne c. République fédérale d'Allemagne.**	**Directive 95/46/CE** Art. 28, (autorité nationale de contrôle).	Recours en manquement contre l'Allemagne en raison du manque d'indépendance des autorités de contrôle des Länder allemand en matière de protection des données en raison de la tutelle administrative fédérale exercée sur ces autorités.	Selon la CJUE, le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel prévues à l'article 28, paragraphe 1, de la directive 95/46, 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, suffit pour entraver l'exercice indépendant des missions de celles-ci. D'une part, il pourrait y avoir une « obéissance anticipée » de ces autorités eu égard à la pratique décisionnelle de l'autorité de tutelle. D'autre part, le rôle de gardiennes du droit à la vie privée qu'assument lesdites autorités de contrôle exige que

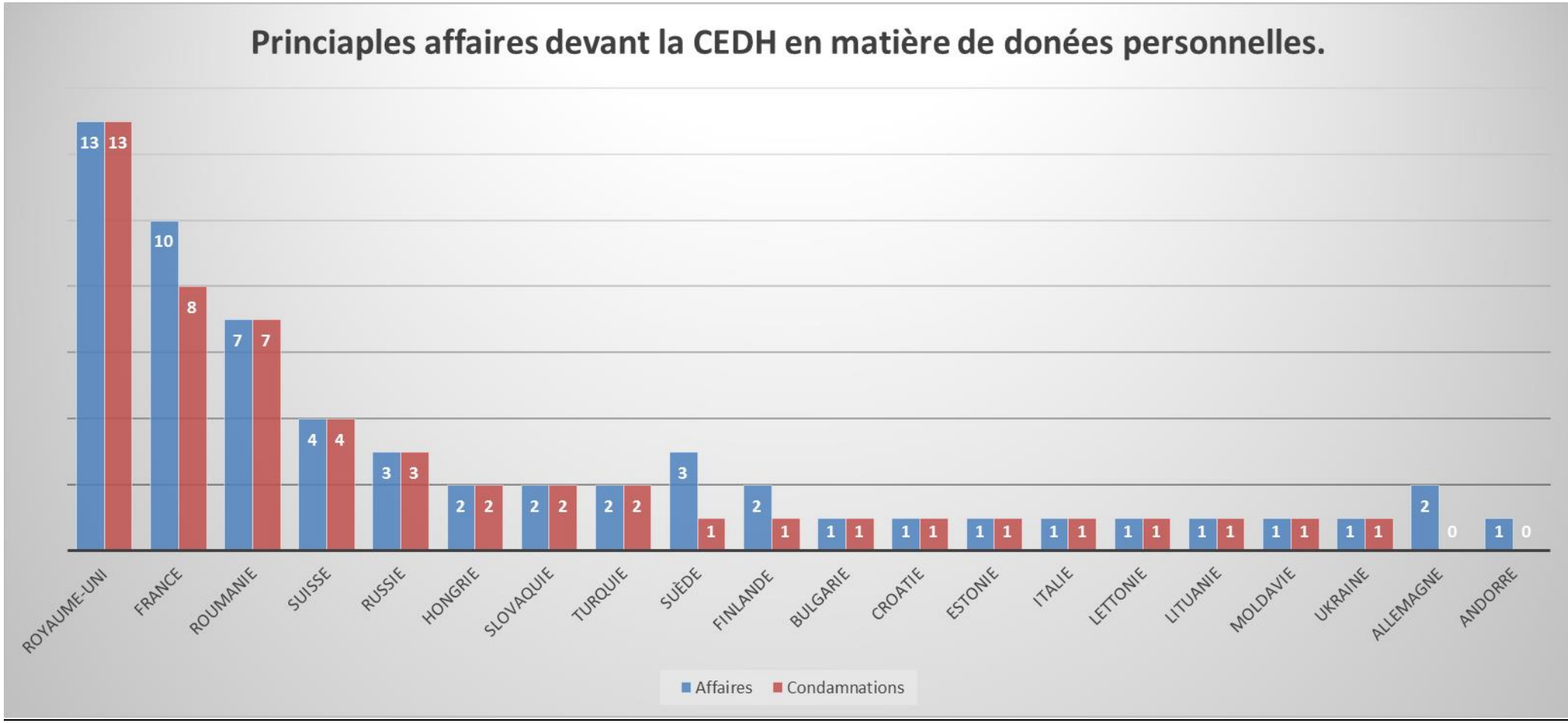
					leurs décisions, et donc elles-mêmes, soient au-dessus de tout soupçon de partialité. La tutelle de l'État exercée sur les autorités nationales de contrôle compétentes pour la surveillance du traitement des données à caractère personnel dans le secteur non public n'est donc pas compatible avec l'exigence d'indépendance. Manquement de l'Allemagne vis-à-vis de l'article 28 de la directive 95/46.
CJUE / GC	09/11/2010	**Volker** und Markus Schecke GbR et Hartmut Eifert **c. Land Hessen.**	**Règlement 1290/2005** modifié par **règlement 1437/2007** et **règlement 259/2008**. Art. 42, 8) et 44 bis. **Directive 95/46/CE** Art. 18 et 20. (déclaration préalable des traitements de données – contrôle des traitements à risque pour les droits des individus). **Art. 7 et 8 Charte**	Les requérants, une société agricole, d'une part, et un agriculteur, d'autre part, s'opposent à la publication par le Land Hessen des données relatives aux aides qu'ils perçoivent dans le cadre de certains fonds européen (FEAGA et Feader). Le Land estime que cette obligation découle des règlements 1290/2005 et 259/2008.	La Cour estime que rien n'indique que le Conseil et la Commission ont pris en considération, lors de l'adoption de l'article 44 bis du règlement n° 1290/2005 et du règlement n° 259/2008, des modalités de publication d'informations relatives aux bénéficiaires concernés qui seraient conformes à l'objectif d'une telle publication tout en étant moins attentatoires au droit de ces bénéficiaires à la protection de leurs données à caractère personnel. Les dispositions visées ne satisfont pas le contrôle de proportionnalité. Concernant les dispositions de la directive 95/46, la Cour estime qu'il n'était pas nécessaire en l'espèce, pour le détaché à la protection des données, de tenir un registre préalablement à la mise en œuvre du traitement, ce qui était prévu par les dispositions invalidées des règlements, ni de soumettre à contrôle préalable un tel traitement.
CJUE	16/02/2012	Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (**SABAM**) c. Netlog NV	**Directive 2000/31/CE** **Directive 2001/29/CE** **Directive 2004/48/CE** **Directive 95/46/CE**	L'origine du contentieux réside en ce que, SABAM, une société de gestion représentant des auteurs, compositeurs et éditeurs d'œuvres musicales, estime que le réseau social Netlog donne à tous ses utilisateurs la possibilité de	Le juge national souhait alors savoir s'il était possible de formuler l'injonction au réseau social de mettre en place un système de filtrage des informations stockées sur ses serveurs par les utilisateurs de ses services, qui s'applique à l'ensemble de ses utilisateurs, à titre préventif, à ses frais, et sans limitation dans le temps. La CJUE a estimé qu'un tel système ne satisferait pas

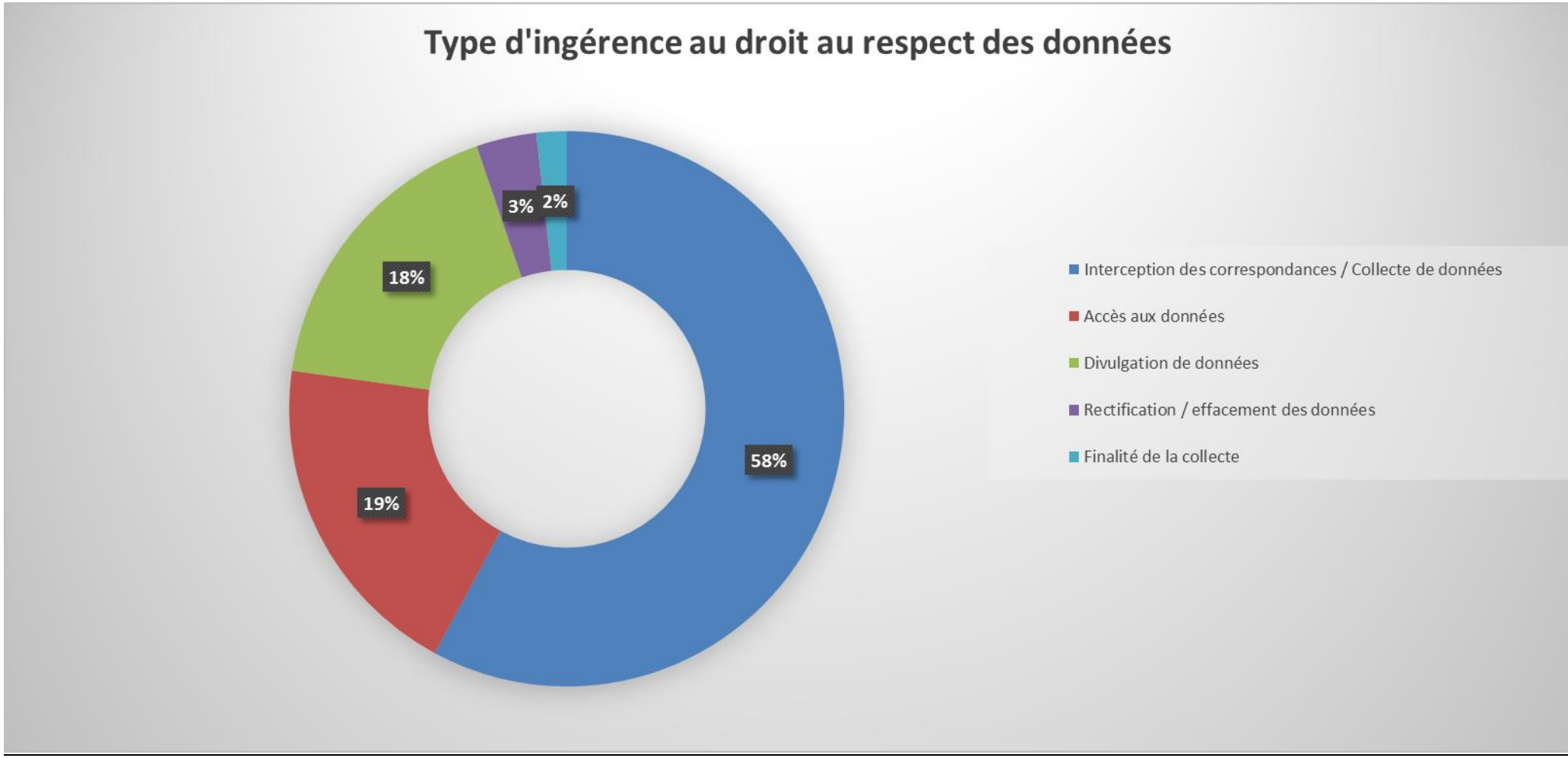
			Directive 2002/58/CE	faire usage des œuvres musicales et audiovisuelles du répertoire de SABAM en mettant ces œuvres à la disposition du public de telle manière que d'autres utilisateurs dudit réseau puissent y avoir accès, et ce sans l'autorisation de SABAM et sans que Netlog ne verse une redevance à ce titre.	un juste équilibre entre protection de la propriété intellectuelle et la liberté d'entreprise et qu'un tel système pourrait également faire peser un risque sur la liberté d'information.
CJUE / GC	16/10/2012	**Commission européenne c. République d'Autriche.**	**Directive 95/46/CE** Art. 28, (autorité nationale de contrôle).	Recours en manquement contre l'Autriche en raison du manque d'indépendance de l'autorité autrichienne de protection des données (DSK) vis-à-vis de la chancellerie fédérale autrichienne.	Aux yeux de la CJUE, en ne prenant pas toutes les dispositions nécessaires pour que la législation en vigueur en Autriche satisfasse au critère d'indépendance concernant la DSK, plus précisément, en instituant un cadre réglementaire en vertu duquel — le membre administrateur de la DSK est un fonctionnaire fédéral assujetti à une tutelle de service, — le bureau de la DSK est intégré aux services de la chancellerie fédérale, et — le chancelier fédéral dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de la DSK, l'Autriche a manqué aux obligations qui lui incombent en vertu de l'article 28, de la directive 95/46.
CJUE	17/10/2013	Michael **Schwarz** c. Stadt Bochum	**Règlement 2252/2004** Art. 1er, § 2). **Art. 7 et 8 Charte**	M. Schwarz a sollicité la délivrance d'un passeport auprès de la Stadt Bochum, tout en refusant que soient relevées, à cette occasion, ses empreintes digitales. La Stadt	La CJUE estime ici qu'il y a bien une atteinte au droit à la vie privée et à la protection des données et vérifie donc si elle est justifiée. La CJUE reconnait que le règlement respecte bien la règle du consentement pour obtenir la collecte des

				Bochum ayant rejeté sa demande, M. Schwarz a introduit un recours pour qu'il soit enjoint à cette ville de lui délivrer un passeport sans relever ses empreintes digitales. M. Schwarz conteste la validité du règlement 2252/2004 prévoyant le relevé des empreintes digitales.	empreintes digitales et que ce texte poursuit bien un but légitime, à savoir empêcher l'entrée illégale de personnes sur le territoire de l'UE. De telles limitations ne remettent donc pas en cause le contenu essentiel des droits prévus aux articles 7 et 8 de la Charte. La CJUE procède alors à la vérification de la proportionnalité de la mesure vis-à-vis du but poursuivi. La Cour reconnait que les mesures du règlement sont aptes à atteindre les buts qu'il poursuit. Reste à savoir si certaines mesures moins attentatoires ne pourraient pas être envisagées pour atteindre le même but. La mesure en question vise la collecte de l'empreinte de deux doigts aux côtés de la photo d'identité. La Cour explique que selon les éléments fournis, la seule mesure alternative équivalente serait la prise d'une photo de l'iris de l'œil, ce qui ne serait pas moins attentatoire aux droits fondamentaux. Elle note par ailleurs que les données des empreintes digitales ne sont conservées que dans le passeport lui-même, lequel reste constamment en la possession de son détenteur. La CJUE estime donc que la mesure satisfait le contrôle de proportionnalité et donc que les dispositions du règlement 2252/2004 ne sont pas contraires à la Charte.
CJUE / GC	08/04/2014	**Digital Rights** Ireland Ltd c. Minister for Communications, Marine	**Directive 2006/24/CE** **Art. 7 et 8 Charte**	Le requérant remet en cause la légalité de mesures législatives et administratives nationales	Selon la Cour, la directive vise tous les moyens de communication électronique et couvre tous les abonnés et utilisateurs inscrits. Elle comporte une

		and Natural Resources e.a. et Kärntner Landesregierung e.a.		concernant la conservation de données relatives à des communications électroniques et demande, notamment, à la juridiction de renvoi de constater la nullité de la directive 2006/24.	ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne sans qu'une telle ingérence ne soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire et sans prévoir de garanties suffisantes, telles que requises par l'article 8 de la charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. Invalidation de la directive 2006/24.
CJUE / GC	08/04/2014	**Commission européenne c. Hongrie.**	**Directive 95/46/CE** Art. 28, (autorité nationale de contrôle).	Recours en manquement contre la Hongrie en raison du manque d'indépendance de l'autorité hongroise de protection des données généré par la mise à terme de l'existence de ladite autorité, du mandat de son président (M. Jóri), et son remplacement par la création d'une nouvelle autorité avec à sa tête une nouvelle personne (M. Péterfalvi).	La Cour rappelle que les États membres sont libres d'adopter et de modifier le modèle institutionnel qu'ils estiment le plus adapté pour leurs autorités de contrôle. Toutefois, ils doivent dans ce cadre veiller à ne pas porter atteinte à l'indépendance de l'autorité de contrôle résultant de l'article 28 de la directive 95/46, laquelle implique l'obligation de respecter la durée du mandat de celle-ci. En effet, s'il était loisible à chaque État membre de mettre fin au mandat d'une autorité de contrôle avant le terme initialement prévu de celui-ci sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, la menace d'une telle cessation anticipée qui planerait alors sur cette autorité tout au long de l'exercice de son mandat pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec ladite exigence d'indépendance. Manquement de la Hongrie vis-à-vis de l'article 28 de la directive 95/46.
CJUE / GC	13/05/2014	**Google Spain** SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González.	**Directive 95/46/CE** Art. 2, 4, 12 et 14. (droit d'accès – droit d'opposition). Art. 7 et 8 CDFUE.	Individu demandant le déréférencement par Google de données le concernant et publiées par un quotidien espagnol.	Moteurs de recherches reconnus comme responsables de traitement de données et devant envisager les demandes de déréférencement, relatives à des données personnelles, formulées par les personnes concernées.

CJUE	01/10/2015	**Smaranda Bara** e.a. c. Președintele Casei Naționale de Asigurări de Sănătate e.a.	**Directive 95/46/CE** Art. 10, 11 et 13. (information de la personne concernée).	A propos de la légalité de la législation roumaine concernant la transmission de données fiscales du requérant d'une administration à une autre sans information ni consentement préalable.	Directive s'opposant à des mesures nationales permettant à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement.
CJUE / GC	06/10/2015	**Maximillian Schrems** c. Data Protection Commissioner	**Décision 2000/520/CE** **Directive 95/46/CE** Art. 25 et 28. (transfert de données vers pays tiers – autorité nationale de contrôle). **Art. 7, 8 et 47 Charte**	Le requérant demandait l'interdiction auprès du Commissaire à la protection des données d'interdire à Facebook Ireland de transférer, ses données personnelles à Facebook Inc aux Etats-Unis, transfert autorisé par la décision 2000/520/CE.	La décision 2000/520 rend possible des ingérences, fondées sur des exigences relatives à la sécurité nationale et à l'intérêt public ou sur la législation interne des États-Unis, dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis. A cela, s'ajoute le fait que la décision 2000/520 ne fait pas état de l'existence d'une protection juridique efficace contre des ingérences de cette nature. Invalidation de la décision 2000/520.


Princiaples affaires devant la CEDH en matière de donées personnelles.
13 13
10 8
7 7
4 4
3 3
2 2
2 2
2 2
3 1
2 1
1 1
1 1
1 1
1 1
1 1
1 1
1 1
2 0
1 0
ROYAUME-UNI
FRANCE
ROUMANIE
SUISSE
RUSSIE
HONGRIE
SLOVAQUIE
TURQUIE
SUÈDE
FINLANDE
BULGARIE
CROATIE
ESTONIE
ITALIE
LETTONIE
LITUANIE
MOLDAVIE
UKRAINE
ALLEMAGNE
ANDORRE
Affaires
Condamnations


Type d'ingérence au droit au respect des données
58%
19%
18%
3%
2%
Interception des correspondances / Collecte de données
Accès aux données
Divulgation de données
Rectification / effacement des données
Finalité de la collecte

13 Sources et bibliographie

(ordre chronologique)

I. Sources

- Ensemble des 21 textes cités et référencés à plusieurs reprises tout au long de l'étude

- BLUMANN (C.) et DUBOUIS (L.), *Droit institutionnel de l'Union européenne*, 5e éd., Paris : Lexis Nexis, coll. « Manuel », 2013, 864 p.
- ISAAC (G.) et BLANQUET (M.), *Droit général de l'Union européenne*, 10e édition, Paris : Sirey, coll. « Sirey université », 2012, 768 p.
- MARGUENAUD (J.-P.), La Cour européenne des droits de l'Homme, 7e éd., Paris : Dalloz, coll « Connaissance du droit », 2016, 212 p.
- SUDRE (F.), *Droit européen et international des droits de l'Homme*, 13e éd., Paris : PUF, coll « Droit fondamental », 2016, 1005 p.
- *Handbook on European data Protection Law*, Council of Europe-European Court of Human Rights, 2014, 210 p.
- SUDRE (F.) et *alii*, *Les grands arrêts de la Cour européenne des droits de l'Homme*, 8e éd., Paris : PUF, coll « Thémis droit », 2017, XII-967 p.

- CNIL, *Les transferts de données à caractère personnel hors Union européenne*, novembre 2012, 38 p.
- CNIL, « Etude d'impacts sur la vie privée : suivez la méthode de la CNIL », *CNIL*, [en ligne], 02 juillet 2015. Disponible sur : https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil, [page consultée le 13 janvier 2017].
- UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, 2016, UNCTAD, 125 p.
- CNIL, « Le « système API-PNR France », *CNIL*, [en ligne], 10 août 2016. Disponible sur : https://www.cnil.fr/fr/le-systeme-api-pnr-france, [page consultée le 10 janvier 2017].
- CNIL, « Règlement européen sur la protection des données : ce qui change pour les professionnels », *CNIL*, [en ligne], 15 juin 2016. Disponible sur : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels, [page consultée le 13 janvier 2017].
- Commission européenne, *Échange et protection de données à caractère personnel à l'ère de la mondialisation. Communication de la commission au Parlement européen et au conseil*, 10 janvier 2017, 18 p. (http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-7-F1-FR-MAIN-PART-1.PDF)

II. Bibliographie

- André VITALIS, *Informatique, pouvoir et libertés*, Paris, Economica, « Politique comparée », 1981, 212 p.
- Martin MARCUSSEN, « OECD Governance through Soft Law" dans : Ulrika Mörth (ed.), *Soft Law in Governance and Regulation. An Interdisciplinary Analysis*, Cheltenham, Edward Elgar, 2004, p. 103-126.
- Arthe VAN LAER, « Transmission électronique des données : la Communauté européenne face au Big Brother américain (1976-1981) », in: Patrick Fridenson et Pascal Griset (dir.), *Entreprise de haute technologie, État et souveraineté depuis 1945*, Paris, Comité pour l'histoire économique et financière de la France, 2010, p. 299-316.

- Zaki LAÏDI, *La Norme sans la force*, Paris, Presses de Sciences-Po, 2013, 304 p.
- PEYROU (S.), « Le rejet de la proposition de directive "PNR" par la Commission des libertés civiles du Parlement européen : l'impossible alchimie entre lutte contre le terrorisme et protection des droits fondamentaux ? », *Réseau Universitaire européen Droit de l'Espace de liberté, sécurité et justice* [en ligne], 5 mai 2013. Disponible sur : http://www.gdr-elsj.eu/2013/05/05/cooperation-policiere/le-rejet-de-la-proposition-de-directive-pnr-par-la-commission-des-libertes-civiles-du-parlement-europeen-limpossible-alchimie-entre-lutte-contre-le-terrorisme-et-protection-de/, [page consultée le 20 novembre 2017].
- Soraya SIDANI, « Les bonnes pratiques de la gouvernance. Résistance et déviance », in Asmara Klein *et alii* (dir.), *Les Bonnes pratiques des organisations internationales*, Paris, Presses de Sciences Po, « Relations internationales », 2015, p. 189-206.
- Anne-Thida NORODOM, « Le droit international après l' « affaire Snowden » : la recherche de nouveaux équilibres », *Annuaire français de droit international*, LX, 2014, p. 731-753.
- Samuel BEROUD et Thomas HAJDUK, « L'OCDE et les bonnes pratiques. Une histoire inséparable », in Asmara Klein *et alii* (dir.), *Les Bonnes pratiques des organisations internationales*, Paris, Presses de Sciences Po, « Relations internationales », 2015, p. 61-77.
- Jean-Philippe FOEGLE, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 30 mars 2016, consulté le 31 mai 2016. URL : http://revdh.revues.org/2074
- Graham GREENLEAF, « Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey », (2017), 145 Privacy Laws & Business International Report, 10-13; UNSW Law Research Paper No. 45, available at SSRN: https://ssrn.com/abstract=2993035, 8 p.

Table des matières

1 Synthèse et évaluation quantitative des textes juridiques (1948-2016) 4

Tableau 1 : évaluation numérique des textes relatifs au secret des correspondances (SC) et à la protection des données personnelles (PDP) 4

Tableau 2 : évaluation numérique des textes de *hard law* et de *soft law* 4

2 Le « secret des correspondances » : un droit dérivé à portée très générale, dépassé par l'évolution technologique 5

Tableau 3 : tableau synthétique des textes juridiques de droit supra-national sur le 5

« secret des correspondances » 5

Tableau 4 : tableau synoptique détaillé des textes juridiques de droit supra-national sur le « secret des correspondances » 6

3 L'abondance des textes innovants relatifs à la « protection des données personnelles » depuis 1973 12

3.1 Le rôle fondateur sur la définition des « données » du Conseil de l'Europe en 1973-1974 12

Tableau 5 : les « bonnes pratiques » du Conseil de l'Europe en 1973 en matière de données 13

Encadré 1 : les « bonnes pratiques » du Conseil de l'Europe en 1974 en matière de données 14

Encadré 5 : les « principes de bases » de la convention du Conseil de l'Europe de 1981 en matière de données 14

Tableau 6 : tableau synthétique des textes du Conseil de l'Europe sur la protection des données 15

3.2 Les grands principes des « flux » de données fixés par l'OCDE en 1980 16

Tableau 7 : les principes fondamentaux des « flux transfrontières de données » selon l'OCDE en 1980 17

Tableau 8 : tableau synthétique des textes de l'OCDE sur la protection des données 17

3.3. Le suivisme de l'UE : la directive de 1995 18

Tableau 8 : tableau synthétique des textes de l'UE sur la protection des données 18

Tableau 10 : tableau synoptique détaillé des textes de droit international sur la protection des données 20

Tableau 11 : tableau de synthèse des textes de droit international relatifs à la protection des données personnelles (PDP) 28

4 L'apport considérable de la jurisprudence européenne sur les données 29

4.1 L'apport décisif de la jurisprudence de la Cour européenne des droits de l'Homme (CEDH) 29

4.2 L'apport de la jurisprudence de la Cour de Justice de l'Union européenne (CJUE) 33

4.3 Articulation entre les jurisprudences de la CJUE et de la CEDH en matière de protection des données à caractère personnel. 35

Tableau 12 : les définitions convergentes des « ingérences » et des « limitations » de 1950 à 2016 37
5 L'ambition du paquet « données » de 2016. 40
5.1 Contexte général de l'adoption du paquet « données » 40
5.2 Le choix européen d'un règlement pour remplacer la directive 95/46 41
6 Le contexte politique de l'adoption du RGPD dans la décennie 2010 44
Figure 1 : Paramètres et contexte de production du RGPD 45
7 Les innovations du RGPD en matière de protection des données 46
7.1 La réaffirmation de la place centrale du consentement. 46
7.2 La consécration de nouveaux droits. 47
8 L'innovation fondamentale du RGPD en matière de responsabilisation des acteurs de la *data* 49
8.1 La tenue d'un registre des activités de traitement. 49
8.2 La notification à l'autorité de contrôle d'une violation de données à caractère personnel 49
8.3 La réalisation d'analyse d'impact relative à la protection des données 49
8.4 La désignation d'un délégué à la protection des données. 50
8.5 L'élaboration de codes de conduite 51
8.6 La mise en place de mécanismes de certification. 52
8.7 Les nouvelles prérogatives des autorités de contrôle nationales. 52
9 L'application géographique du RGPD européen, étendue au-delà de l'UE 53
Carte 1 : la zone d'application du RGPD : l'UE des 28 53
Carte 2 : la zone étendue d'application d'une législation de type RGPD 54
Carte 3 : les pays considérés comme « adéquats » et « adéquats partiels » en protection des données pour l'UE selon la commission européenne 56
10 L'application matérielle du règlement: la « sécurité nationale » en dehors du champ du RGPD 58
11 Conclusions (provisoires) 61
12 Annexes 62
Tableau 13 : tableau de synthèse des principaux arrêts de la CEDH en matière de protection des données à caractère personnel 62
Tableau 14 : tableau de synthèse des principaux arrêts de la CJUE en matière de protection des données à caractère personnel 80
13 Sources et bibliographie 91