Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls

Emmanuel Netter

CEPRISCA
Collection colloques

Regards sur le nouveau droit des données personnelles

Sous la direction de :
Emmanuel Netter,
Maître de conférences HDR en droit privé

LE MODÈLE EUROPÉEN DE PROTECTION DES DONNÉES PERSONNELLES À L'HEURE DE LA GLOIRE ET DES PÉRILS[1]

Emmanuel Netter, maître de conférences HDR en droit privé
Université d'Avignon, Laboratoire Biens, normes, contrats (EA 3788)
Membre associé du Centre de droit privé
et de sciences criminelles d'Amiens (EA 3911)

« La *civilisation de l'informatique ne va-t-elle pas devenir celle de l'indiscrétion et de l'implacabilité, celle qui n'oublie, ni ne pardonne, qui enfonce le mur de l'intimité, enfreint la règle du secret de la vie privée, déshabille les individus ?* » ?
Jean Foyer, rapporteur de la loi informatique et libertés,
JO du 4 octobre 1977, p. 5782

« *Nous abordons un terrain qui est encore en friche et presque inconnu. Il serait déraisonnable de prétendre organiser en détail un domaine aussi nouveau. L'informatique est promise à un développement très rapide qui, dans une assez large mesure, est imprévisible, comme l'est la recherche scientifique elle-même. Par conséquent, la loi que nous vous proposons a un caractère expérimental. Nous ne prétendons pas légiférer pour l'éternité* ».
Alain Peyrefitte, ministre de la Justice,
JO du 4 octobre 1977, p. 5789

Il y a quarante ans, les fondations du droit français des données personnelles étaient posées[2]. Les travaux parlementaires, dont ces deux citations sont extraites, révèlent la conscience qu'on avait alors d'adopter un texte d'ores et déjà fondamental, mais dont l'importance, surtout, ne ferait que croître avec la montée en puissance de l'informatique. La direction exacte que ces progrès devaient emprunter était certes inconnue. Il était difficile, à l'orée des années 80, d'imaginer que les plus puissantes menaces planant sur l'intimité des citoyens seraient à rechercher dans les bases des entreprises privées, et non plus seulement dans le recoupement

1 - Le titre est emprunté à R. Merle, *La Gloire et les Périls*, éd. De Fallois, 1999.

2 - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

des fichiers administratifs. On ne pouvait entrevoir les téléphones perpétuellement géolocalisés, on ne pouvait anticiper la publicité ciblée, on ne pouvait imaginer l'internet des objets ou les réseaux sociaux. Mais si l'on ne connaissait ni la nature ni l'origine exactes des dangers à venir, on avait bien prévu, il y a quatre décennies déjà, leur exceptionnelle intensité.

Pourtant, ces solennelles mises en garde n'ont longtemps suscité qu'un désintérêt poli, que ce soit de la part de la petite communauté des juristes, de celle, autrement plus importante, des entreprises privées et des administrations, ou même du grand public.

S'agissant de la communauté des juristes, remarquons qu'une maîtrise élémentaire de la loi « informatique et libertés » n'était pas attendue, il y a peu, d'un généraliste du droit public ni du droit privé. Il y a dix ans encore, il était commun de suivre un cursus juridique complet sans rien avoir appris de substantiel de ce texte ni de la législation européenne ultérieure en matière de données personnelles. La connaissance de ces règles semblait réservée au petit nombre des spécialistes de droit de l'informatique. Depuis peu, la tendance évolue nettement, et bien des enseignants décident de réserver quelques dizaines de minutes, voire quelques heures à ces questions. En droit privé, ce sera à l'occasion d'un cours de droit des personnes ; en droit public, dans le cadre d'un enseignement de libertés fondamentales. La question, il est vrai, est de celles qui transcendent cette *summa divisio* française. Quant aux formations consacrées plus ou moins directement au « droit du numérique », et qui ne peuvent faire l'économie de modules substantiels consacrés au droit des données, elles se multiplient sur tout le territoire. Le niveau général de connaissance des juristes dans ce domaine a donc fortement augmenté en peu de temps.

Au-delà du milieu des juristes, ce sont les responsables de traitement privés et publics qui semblent avoir redécouvert tardivement l'existence du droit des données personnelles. Autrement dit, pratiquement toutes les administrations et entreprises privées, car chacun est aujourd'hui un « responsable de traitement »[3]. Dès le

3 - V. dans cet ouvrage M. Clément-Fontaine, « Tous responsables de traitement de données personnelles ? ».

texte du Règlement général sur la protection des données (RGPD) divulgué, jusqu'à son entrée en vigueur – et sans doute bien au-delà... – une véritable « course à la mise en conformité » s'est engagée. Son carburant est connu : le net rehaussement des sanctions encourues en cas de violation de certaines dispositions du règlement[4]. «Vingt millions d'euros », répétaient les petits entrepreneurs saisis par l'angoisse. « Quatre pour cent du chiffre d'affaires mondial », scandaient les géants de l'économie, incrédules. Quelles nouvelles obligations issues du RGPD peinaient-ils à mettre en œuvre pour s'effrayer ainsi ? Le droit à la portabilité des données ? Le nouveau régime de la sous-traitance ? Le droit à l'effacement spécifiquement reconnu par le texte aux mineurs ? Non : les obligations qui font l'objet des sanctions les plus lourdes sont celles qui, pour l'essentiel, existent depuis... 1978[5]. Les responsables de traitement et sous-traitants qui tremblaient tout à coup mettaient parfois en œuvre depuis longtemps des traitements dont la finalité n'était pas identifiée, ou à tout le moins pas communiquée aux personnes concernées ; ils ne pouvaient pas toujours justifier d'un fondement de licéité précis, ou se reposaient sur un consentement grossièrement extorqué aux personnes dont les données étaient traitées, ou encore faisaient un usage abusif du fondement particulier qu'est l' « intérêt légitime » ; ils faisaient fi du principe de minimisation, ou se montraient totalement laxistes sur le terrain de la sécurité des informations[6]. Pourquoi ces exigences avaient-elles mis quarante ans à pénétrer les consciences ? La réponse est simple : une mise en conformité sérieuse est coûteuse en temps ainsi qu'en compétences. Les plus cyniques ajouteront qu'elle peut constituer un désavantage concurrentiel si une entreprise vertueuse fait face à des adversaires moins scrupuleux, voire même qu'elle peut disqualifier certains modèles d'affaires radicalement incompatibles avec le respect des données personnelles. Ainsi, le bilan coûts contre

4 - Art. 83 du 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.

5 - L'art. 83, 5) punit en effet de l'amende la plus lourde, notamment, la violation des « principes de base d'un traitement » (a) et des « droits dont bénéficient les personnes concernées » (b), ce qui renvoie bien à une majorité de règles déjà en vigueur depuis la première version de la loi informatique et libertés.

6 - Il s'agit de contraventions aux « principes relatifs au traitement des données à caractère personnel », que le règlement énonce en son article 5 avant de les développer plus loin.

avantages était bien souvent défavorable lorsque, avant l'entrée en vigueur du règlement, les amendes françaises les plus élevées étaient plafonnées à 150 000 euros[7]. Il est nettement plus incitatif à présent. Le secret de l'effectivité du droit serait-il aussi simple et aussi décevant ? Il semblerait que oui. La loi, dans ce domaine au moins, n'est pas obéie parce qu'elle est l'expression de la volonté générale, parce qu'elle est bonne et juste ou parce qu'elle a été votée par les autorités habilitées dans les formes constitutionnellement requises, mais parce qu'elle frappe, durement, au portefeuille. En marge d'un colloque, un ancien de la CNIL rappelait malicieusement cette maxime, qui fleure bon l'Amérique de la Prohibition : « on peut obtenir beaucoup plus avec un mot gentil et un revolver qu'avec un mot gentil tout seul ».

L'intérêt pour le droit des données personnelles a, enfin, largement progressé au sein du grand public. Il serait certes excessif de dire que, dans les années 70, la question n'intéressait pas du tout l'opinion. On sait que la loi informatique et libertés est l'enfant du scandale : celui provoqué par un article du journal Le Monde révélant l'existence du « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » (SAFARI)[8]. Le ministre de l'Intérieur, un certain Jacques Chirac, se frottait semble-t-il les mains à l'idée que l'INSEE procède à cette interconnexion massive des bases de données des administrations autour d'un identifiant unique pour chaque citoyen, le numéro de sécurité sociale[9]. Il fallut encore plusieurs années avant que la question n'arrive devant le Parlement, et que ne naisse la CNIL. L'émotion suscitée à l'époque dans l'opinion a-t-elle été suivie d'effets durables ? On peut en douter. Les citoyens se pensaient protégés passivement, par les formalités préalables et les obligations diverses pesant sur les responsables de traitements et sous-traitants. Mais bien peu étaient acteurs de la protection de leurs données, même si les droits « informatiques et libertés » qu'il leur

7 - 300 000 euros en cas de récidive.

8 - P. Boucher, « Une division de l'informatique est créé à la chancellerie. «SAFARI» ou la chasse aux français », article *Le Monde* du 21 mars 1974.

9 - Face aux dénégations du ministère de l'intérieur à la suite de son précédent article, le journaliste P. Boucher rétorquait : « Il n'a jamais été écrit que la place Beauvau assurait le leadership du projet SAFARI, mais qu'elle s'y intéressait de très près... Les convoitises dont il est l'objet ne sont un secret pour personne, non plus que les pressions exercées sur M. Jean Ripert, directeur de l'INSEE » : P. Boucher, « Le ministère de l'intérieur affirme qu'il n'est pas question de porter atteinte aux libertés individuelles », article *Le Monde* du 22 mars 1974.

était loisible d'invoquer s'étalaient régulièrement sous leurs yeux, sous forme de mentions obligatoires, à l'occasion de l'ouverture d'un compte bancaire ou de la participation à un jeu-concours, îlots perdus dans l'océan des contrats jamais lus. Mais ici encore, un vent nouveau paraît souffler depuis quelques années. Pour exister sur la scène médiatique et marquer les esprits, il manquait à la cause des données personnelles deux choses dont elle dispose à présent : une actualité perpétuelle et des incarnations marquantes.

D'abord, il existe aujourd'hui dans cette matière une actualité perpétuellement renouvelée. La société Facebook pourrait quasiment l'assurer à elle seule. Elle a particulièrement marqué les esprits à l'occasion de l'affaire dite « Cambridge Analytica »[10]. Un questionnaire d'apparence anodine était autorisé par des utilisateurs du réseau social à accéder à leur profil. Il y aspirait ensuite toutes les données possibles – qui peuvent comprendre, outre les centres d'intérêts des informations sur les convictions politiques ou religieuses, l'orientation sexuelle ou la profession exercée – non seulement sur l'internaute ayant accordé l'autorisation, mais aussi et surtout sur ses centaines d'amis. Il est probable que l'utilisateur du questionnaire n'avait pas véritablement saisi ce à quoi il s'exposait ; il est en toute hypothèse certain que ses amis n'avaient consenti à rien. Ces données, qui concernaient une majorité de citoyens américains – mais aussi des Européens, dont des Français – ont notamment été exploitées aux fins de démarchage politique ciblé dans le cadre de la campagne électorale qui a vu Donald Trump remporter la présidence des États-Unis. Facebook a présenté ses excuses, a modifié sa gestion des applications tierces autorisées à exploiter les profils de ses utilisateurs. Entendu successivement par le Congrès américain et par le Parlement européen, le dirigeant Marc Zuckerberg a impressionné par sa capacité à éviter toute réponse précise et substantielle aux questions qui lui étaient posées[11]. Mais l'affaire Cambridge Analytica, pour fondamentale qu'elle soit, ne doit

10 - Sur laquelle V. par ex. G. Pépin, « Facebook a laissé fuiter les données de 50 millions d'internautes, UE et USA vont enquêter », article *nextinpact.com* du 19 mars 2017.

11 - V. par ex. l'inventaire des questions auxquelles M. Zuckerberg a soit répondu qu'il se concerterait avec son équipe et répondrait ultérieurement, soit qu'il ne connaissait pas la réponse : « Facebook : comment Mark Zuckerberg a évité de répondre à certaines questions », article *lemonde.fr* du 11 avril 2018.

pas occulter les incidents intervenus avant et depuis lors. Avant cette affaire, Facebook s'était déjà distingué lors de son rachat de la célèbre messagerie WhatsApp, en promettant de ne pas croiser les deux bases de données d'utilisateurs, puis en agissant à l'inverse, s'attirant une sanction de la Commission européenne en matière de droit des concentrations, mais sans que la question de la conformité de ces pratiques au RGPD ne soit encore véritablement éclaircie à cette heure[12]. Depuis Cambridge Analytica, l'actualité est restée riche. À la rentrée 2018, on apprenait que la sécurité de millions de comptes, dont certains appartenant à des internautes européens, avait été compromise par des attaques sophistiquées[13]. Il ne faut pas être trop prompt, cette fois-ci, à blâmer la société, car un réseau social d'une telle ampleur et d'une telle complexité ne sera jamais invulnérable du point de vue de la sécurité informatique. Les spécialistes diront si la firme avait fait preuve d'une légèreté blâmable, ou si les diligences accomplies avaient été à la hauteur des moyens disponibles. En revanche, quasiment au même moment, une étude menée par des chercheurs américains démontrait que Facebook avait détourné des numéros de téléphone, qui lui avaient été fournis par ses utilisateurs dans le but exclusif d'améliorer la sécurité de leur compte : la société les a pourtant exploités afin de se livrer à de la publicité ciblée[14]. Depuis, la liste des révélations s'est encore largement allongée[15]. Bien d'autres responsables de traitement encourent des reproches

12 - Commission européenne, « Concentrations: la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », communiqué de presse du 18 mai 2017.

13 - V. par ex. L. Ronfaut, « Piratage de Facebook : 5 millions de comptes concernés en Europe », article *lefigaro.fr* du 2 octobre 2018.

14 - G. Gebhart, « You gace Facebook your number for security. The used if for ads », article *eff.org* du 27 septembre 2018 ; G. Venkatadri, E. Lucherini, P. Sapierynski et A. Mislove, « Investigating sources of PII used in Facebook's targeted advertising », : http://mislove.org/publications/PII-PETS.pdf.

15 - Actualisant cet article avant la parution de l'ouvrage, nous pouvons mentionner les accès octroyées par Facebook à Netflix ou à Spotify à la messagerie privée de certains utilisateurs, révélée en décembre 2018 (V. par ex. Le Poiny du 19 décembre 2018, « Facebook a octroyé aux géants du Net un large accès aux données personnelles) ; la possibilité pour des milliers d'employés de Facebook d'accéder aux mots de passe des utilisateurs stockés dans une base non chiffrée, révélée en mars 2019, (V. par ex. L. Ronfaut, « Des employés de Facebook ont pu consulter des millions de mots de passe d'utilisateurs) ; ou encore un nouveau scandale lié à l'accès à des données par des applications tierces, dans la lignée de l'affaire Cambridge Analytica, les informations étant stockées en clair sur des serveurs non protégés, révélé en avril 2019 (V. par ex. l'article du Monde du 4 avril 2019, « Des données de 540 millions d'utilisateurs de Facebook librement accessibles).

sur le plan du droit des données personnelles, mais Facebook, avec 2,2 milliards d'utilisateurs actifs mensuels, occupe une place particulière dans les préoccupations des citoyens[16]. Son seul exemple suffit donc à démontrer que l'opinion publique n'a pas manqué, ces derniers mois, d'occasions de s'interroger sur le sort réservé à ses informations intimes.

Pour aiguillonner encore davantage les consciences et cristalliser l'attention médiatique, la thématique des données personnelles avait besoin d'incarnations marquantes, autrement dit de héros ou d'antihéros. La première de ces figures a surgi en 2013, et il est à peine besoin d'y revenir : c'est celle d'Edward Snowden, qui a interpellé le monde entier en révélant la toute-puissance des services de renseignement américains[17]. Les révélations sur les programmes de surveillance ont attiré indirectement l'attention sur leur carburant : les données de géolocalisation, de navigation, les métadonnées de télécommunication, les publications sur les réseaux sociaux... À ce moment-là, dans l'esprit du grand public, le concept de données personnelles passait brutalement du statut d'abstraction lointaine et inoffensive à celui de réalité quotidienne et menaçante. Or, ces mêmes informations qui font parfois l'objet d'une surveillance publique à des fins de sécurité nationale sont par ailleurs la matière première d'une industrie privée qui les exploite à des fins lucratives. On peut ajouter un deuxième personnage à la galerie de portraits, déjà évoqué du reste : le fondateur et dirigeant de Facebook, Mark Zuckerberg. Tout oppose Snowden et Zuckerberg, et l'on rencontre souvent sur les réseaux sociaux cette présentation en raccourci : le premier est devenu un traître et un fugitif pour avoir dénoncé la surveillance des masses ; le second est devenu l'un des hommes les plus riches du monde pour l'avoir organisée[18]. La réalité est évidemment plus subtile, mais ce qui est intéressant est que l'on assiste ici à la naissance de grandes figures populaires susceptibles l'une et l'autre, selon le locuteur, d'être admirées ou honnies.

16 - Chiffres 2018 issus du *Blog du modérateur* : https://www.blogdumoderateur.com/chiffres-facebook/.

17 - V. not. le documentaire de L. Poitras, *Citizenfour*, 2015.

18 - Réagissant à l'audition de Mark Zuckerberg devant le Congrès suite à l'affaire Cambridge Analytica, Edward Snowden n'a d'ailleurs pas pu s'empêcher d'écrire sur Twitter : « And they call me a criminal » : https://twitter.com/snowden/status/983801604519407616.

Nos peurs et nos fantasmes à l'égard des nouvelles technologies cherchent ainsi à s'accrocher à des visages. Ce besoin, le dénommé Chris Dancy l'a identifié très tôt, et transformé en un fonds de commerce fort lucratif. Se présentant à travers la presse mondiale comme « l'homme le plus connecté du monde », il se vante de mesurer un maximum de paramètres de son existence, à grand renfort « d'internet des objets » : son rythme cardiaque, la fréquence de ses passages aux toilettes, la température et l'hygrométrie de son logement, la qualité de son sommeil, la musique qu'il écoute... Il fait ensuite varier certains de ces paramètres, et observe l'effet produit sur les autres[19]. Il prétend ensuite, à l'intention des naïfs, avoir appliqué la même démarche expérimentale à l'analyse des comportements humains, accédant à une compréhension de leurs mécanismes sous-jacents qui lui procurerait un pouvoir « terrifiant » de manipulation d'autrui [20]. Peu seront dupes, mais suffisamment tout de même pour assurer à ce conférencier professionnel un train de vie confortable. Comment est-ce possible ? Sans doute parce que le personnage de « *mindful cyborg* » construit par M. Dancy n'est qu'une spectaculaire hyperbole, une caricature débridée d'attentes que certains nourrissent véritablement à l'égard du progrès technique. Il prétend qu'en agrégeant assez de données personnelles et en les confiant à des algorithmes suffisamment sagaces, le sens caché de notre environnement, de nos comportements et de nos vies apparaîtra tout à coup[21]. C'est en définitive un pacte faustien qu'il propose à ses adeptes : faire don de son essence à une figure puissante et dangereuse, et recevoir en contrepartie d'extraordinaires pouvoirs. Les grandes entreprises du numérique revêtent, dans ce récit, des atours méphistophéliques, et offrent l'accès à une nouvelle transcendance. Ainsi, plus encore peut-être que Mark Zuckerberg, Faust-Dancy s'offre comme l'exact opposé du martyr Snowden dans l'imaginaire collectif.

19 - C. Richard, « L'homme le plus connecté du monde s'est fait dévorer par ses données », article *nouvelobs.com* du 9 septembre 2016 : Je prenais ces petites unités de comportement et je les changeais de place pour voir ce qui se produisait : une même conversation avec un ami prend-elle un tour différent s'il fait chaud ou s'il fait froid, si on marche ou si on est assis ? ».

20 - *Ibid.* : « c'était trop facile de pousser les gens à faire ce que je voulais ».

21 - Pour un aperçu : chrisdancy.com.

Des scandales d'ampleur survenant à intervalles réguliers, une galerie de personnages marquants, et la couverture médiatique de l'entrée en vigueur du RGPD ont ainsi, à n'en pas douter, éveillé l'intérêt du public. Cela a-t-il produit des effets concrets ? Au premier abord, il semble que oui. La CNIL, en livrant son premier bilan après 4 mois d'application du règlement, faisait état d'une augmentation de 64 % des plaintes par rapport à la même période en 2017, qui constituait déjà elle-même une année record. Et l'autorité de commenter : « Ceci est sans doute consécutif à un coup de projecteur médiatique important récemment sur la protection des données : RGPD, Cambridge Analytica, etc. »[22]. Deux mois plus tard, la CNIL révélait les résultats d'un sondage IFOP dont elle était commanditaire : 66 % des Français se disaient « plus sensibles que ces dernières années à la protection de leurs données personnelles », et 65 % d'entre eux avaient entendu parler du règlement européen[23].

À l'heure des 40 ans de la loi informatique et libertés, le bilan prend ainsi des allures de triomphe. Le droit des données personnelles n'a jamais été mieux considéré, mieux connu, plus puissant en Europe. Toutefois, derrière ces apparences flatteuses se cachent de nombreux motifs d'inquiétude, qui ne doivent pas être occultés. Sans rien remettre en cause des formidables acquis du droit français et, surtout, du droit de l'Union, il nous faut identifier ces difficultés. Si elles n'étaient pas résolues, le RGPD pourrait n'être qu'un feu de paille, dont l'éclat s'épuiserait en quelques années seulement. Ces faiblesses se nichent à la fois au sein du droit européen (I) et en dehors de lui (II).

§1 : Le droit européen des données menacé en dedans

Deux défauts majeurs affectent cette législation. Dans son état actuel, elle est très difficilement intelligible pour les citoyens, et même pour les milieux professionnels non spécialisés (A). Surtout, si son effectivité semble en nette hausse, à la faveur notamment d'une augmentation drastique des sanctions, elle risque pourtant d'atteindre rapidement un plateau avant de décliner (B).

22 - CNIL, « RGPD : quel premier bilan 4 mois après son entrée en application » ?, article *cnil.fr* du 25 septembre 2018.

23 - CNIL, « RGPD : quel bilan 6 mois après son entrée en application ? », article *cnil.fr* du 23 novembre 2018.

A. Le manque de lisibilité

Si la CNIL se réjouissait des résultats du sondage qu'elle avait commandé s'agissant de la proportion de Français ayant entendu parler du RGPD, elle reconnaissait sa déception quant au chiffre de ceux qui estimaient comprendre l'intérêt du texte : 54 % seulement[24]. Mais il serait déjà extraordinaire qu'une majorité de la population, fût-elle courte, ait accédé à une maîtrise élémentaire de ces règles. Il est permis d'en douter, non par manque de confiance dans les capacités d'apprentissage de nos concitoyens, mais parce que tout a été fait pour leur compliquer la tâche.

Cela a d'abord commencé avant même l'adoption du texte européen. La loi dite « République numérique » du 7 octobre 2016 aborde des thématiques nombreuses[25]. Le droit des données personnelles en fait partie. Au moment où le projet de loi est présenté, et pendant une large part du processus parlementaire, le RGPD est en cours de négociation. Pourquoi adopter une approche purement française de questions qui s'apprêtent à faire l'objet d'une harmonisation européenne complète, dont la teneur n'est pas encore entièrement connue ? Le calendrier politique a ses raisons que la raison ignore. Cette stratégie du cavalier seul n'aura pas nui s'agissant de points sur lesquels le règlement ne s'est finalement pas prononcé, comme le sort qu'il convient de réserver aux données personnelles après la mort[26]. Sur d'autres questions, comme le droit à la portabilité des données, la France a mis au point sa propre qualification juridique et son propre régime, qui sont immédiatement entrés en conflit avec les arbitrages retenus dans le cadre du RGPD. Pour mettre fin à cette situation confuse, les textes français ont récemment été supprimés[27]. Quel citoyen, même s'il avait fait preuve d'une curiosité raisonnable pour l'actualité législative, aurait pu retenir quoi que ce soit d'exact d'un tel processus ?

---

24 - *Ibid*.

25 - Loi ° 2016-1321 du 7 octobre 2016 pour une République numérique.

26 - Art. 40-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, issu de la loi précitée pour une République numérique. Sur cette question, V. dans le présent ouvrage C. Béguin-Faynel, « La protection des données personnelles et la mort ».

27 - Les articles L. 224-42-1 et s. du Code de la consommation ont été supprimés par l'article 33 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

C'est ensuite au niveau européen qu'ont surgi des obstacles à la bonne intelligibilité des textes. Il était attendu du règlement qu'il réalise une harmonisation complète du droit des données personnelles, à la fois au bénéfice des citoyens de l'Union, dotés partout des mêmes droits, mais aussi au bénéfice des responsables de traitement, placés en vertu d'une logique bien connue face à un « marché unique » permettant une « libre circulation » des données. L'échec est patent, puisqu'il est renvoyé aux droits nationaux sur une cinquantaine de points[28]. Était-il véritablement impossible de s'accorder, par exemple, sur l'âge à partir duquel un enfant peut consentir seul à un traitement de données le concernant[29] ? Aujourd'hui, un juriste auquel un parent demanderait si son enfant peut ouvrir un compte Facebook sans son concours ne pourrait répondre sans avoir vérifié quel droit national est applicable, puis sans avoir recherché les textes locaux pertinents, à supposer qu'il maîtrise la langue européenne concernée. Mais ce n'est pas tout. Imaginons un citoyen européen si courageux qu'il aurait entrepris la lecture des 173 considérants et des 99 articles du règlement, tout en acceptant d'être renvoyé 50 fois à son droit national. Pourrait-il se vanter de connaître le droit européen des données personnelles ? Malheureusement pas, car l'Union a de surcroît ajouté à sa législation générale des textes sectoriels qu'il convient de maîtriser également. S'agissant des traitements de données relatifs à des infractions ou sanctions pénales, au moins doit-on se féliciter que la directive sectorielle ait été adoptée en même temps que le RGPD[30]. Il suffit donc de consulter ce supplément de législation… ainsi que l'instrument de droit national l'ayant transposé – ce qui, s'agissant d'une directive, n'est cette fois-ci pas une surprise. Mais considérons à présent la protection de la vie privée dans le secteur des communications

28 - Le décompte est celui de la CNIL dans sa délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978, p. 3.

29 - L'article 8 du règlement 2016/679 fixe un minimum de treize ans et un maximum de seize ans. En France, l'âge de quinze ans a été retenu à l'article 7-1 de la loi précitée du 6 janvier 1978 dans sa rédaction issue de la loi du 20 juin 2018.

30 - 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.

électroniques : elle est principalement régie par une directive quelque peu dépassée par les évolutions techniques[31]. Cela concerne des questions auxquelles nous sommes confrontés tous les jours, comme le dépôt et la gestion des cookies par des sites internet dans les navigateurs internet de ceux qui les consultent, ou encore les campagnes publicitaires de masse par courrier électronique. Un nouveau règlement dit « *e-privacy* » devait être adopté, en principe avant l'entrée en vigueur du RGPD[32]. Cela aurait notamment permis aux services en ligne de travailler de manière globale à leur mise en conformité. Ce texte a pris du retard, et sera adopté, au mieux, au cours de l'année 2019.

Revenons à présent à l'échelon français, mais en nous situant cette fois-ci après l'adoption du règlement. Il fallait prendre position pour chacune de la cinquantaine de « marges de manoeuvre» que le texte offrait aux États membres. Le chef du bureau du droit public à la direction des affaires civiles et du sceau avait surpris l'auditoire, lors d'un colloque, en évoquant la nécessité de « transposer » le règlement alors, que ce terme technique, on le sait, est en principe réservé aux directives[33]. Il avait immédiatement précisé qu'il s'agissait d'une facilité de langage, mais qui révélait l'importance du travail à accomplir. On le conçoit bien, mais tout de même : le règlement avait été adopté le 14 avril 2016 et n'entrait en application que le 25 mai 2018[34]. Le délai semblait suffisant, et il était même souhaitable que les textes nationaux soient adoptés début 2018, afin que les responsables de traitement et sous-traitants aient le

31 - Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, modifiée par la 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.

32 - Pour l'heure V. la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03 (COD).

33 - Intervention de M. Cyril Noël lors du colloque *Règlement général sur la protection des données : nouveaux principes, nouvelles règles et application sectorielle*, Université Paris V, le 18 mai 2016.

34 - Aux termes de son article 99, le Règlement est « entré en vigueur » le vingtième jour suivant celui de sa publication au JOUE, mais n'est « devenu applicable » qu'à partir du 25 mai 2018.

temps de se mettre en conformité avec un arsenal législatif complet, entrant en vigueur d'un bloc. Malheureusement, le Gouvernement a lancé le processus parlementaire tardivement, et n'a pas demandé le bénéfice de la procédure accélérée. Le texte n'a été adopté en lecture définitive par l'Assemblée nationale que le 14 mai 2018. Il ne restait que dix jours avant l'entrée en application du RGPD, et il fallait encore compter avec la saisine du Conseil constitutionnel. Là encore, le Gouvernement n'a pas usé de la faculté dont il dispose de demander un examen en urgence, de sorte que la décision (de non-conformité partielle) a été rendue le 12 juin, et la loi promulguée le 20 juin[35]. Le règlement était en vigueur depuis plus d'un mois. Il pouvait certes être appliqué, pour l'essentiel, avant l'adoption des dispositions nationales, mais il en résultait au minimum un effet d'image plutôt déplaisant. Passons rapidement sur le fait que la loi elle-même appelle un certain nombre de décrets d'application et d'instruments normatifs que la CNIL produira dans l'avenir, car il est vrai que Rome ne s'est pas faite en un jour.

Mais les pouvoirs publics français ne se sont pas contentés d'être en retard : ils ont pêché dans la forme, et même sur le fond. La forme, d'abord, était critiquable : alors qu'il aurait été bien plus simple de faire table rase du passé, la France a absolument tenu à conserver la loi informatique et libertés, déjà modifiée à plusieurs reprises depuis 1978, et à lui faire subir les lourds remaniements nécessaires à son alignement avec le nouveau règlement. Le résultat est d'une lecture pour le moins pénible. Pire encore : en son article 32, la loi faisait d'elle-même l'aveu que le parti ainsi pris était mauvais, puisqu'elle habilitait le Gouvernement à réécrire l'ensemble du droit français des données personnelles par ordonnance. Le texte est arrivé en décembre 2018[36]. Pourquoi n'avoir pas commencé par là ?

Le fond, ensuite, fait jaillir de nouvelles critiques. Par exemple, le RGPD encadre rigoureusement les décisions produisant des

35 - Décision n° 2018-765 DC du 12 juin 2018. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

36 - Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

effets juridiques sur le fondement de traitements automatisés. Ces décisions peuvent consister par exemple en l'octroi d'un crédit bancaire, dans le fait de sélectionner ou d'écarter une candidature pour un entretien d'embauche, ou dans une décision administrative. Sur cette question d'une grande importance pratique, l'encadrement français a pu sembler moins exigeant que celui décidé par le règlement[37].

Le bilan est donc celui-ci : le droit européen des données personnelles est constitué d'un empilement d'une législation générale et de législations sectorielles, chaque texte étant par lui-même d'une grande complexité ; les droits nationaux transposent ensuite les directives et exploitent les « marges de manœuvre » du règlement en ordre dispersé ; la France, pour ce qui la concerne, a produit en retard un texte de son propre aveu inintelligible, et peut-être déloyal à l'égard des solutions européennes sur certains points.

À ce manque de lisibilité, qui suscite déjà l'inquiétude, il faut ajouter le risque d'un manque d'effectivité, qui en découle pour partie.

B. Le manque d'effectivité

L'effectivité du droit européen des données personnelles peut être évaluée d'un double point de vue : celui des personnes concernées, et celui des responsables de traitement.

37 - N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT*, 2018, 459 : « L'article 22 du RGPD prévoit un droit (subjectif ?) de tout individu «à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire». La reconnaissance d'un tel droit confère donc un caractère automatique à cette prérogative de la personne concernée et va évidemment au-delà d'une simple faculté d'opposition ou du renforcement des conditions de licéité des traitements automatisés reposant sur un tel profilage permettant une prise de décision ayant des effets juridiques ou affectant la personne concernée de manière similaire ». En revanche, poursuit l'auteur, « (...) l'alinéa 2 de l'article 10 de la LIL (...) prévoit désormais que «Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception : [...]». Une telle rédaction n'a pas le même sens que celle précité prévue dans le règlement. Le fait qu'aucune décision «ne peut être prise sauf exception», n'a pas la même force que la reconnaissance d'un droit subjectif à ne pas faire l'objet de décision prise sur le fondement d'un profilage ».

1) Du point de vue des personnes concernées

En dépit des quelques améliorations récentes, il faut constater la faible mobilisation de leurs droits par les personnes dont les données sont manipulées. L'entrée en application du RGPD a suscité l'attention médiatique, ce qui a certes contribué, on l'a vu, à sensibiliser la population à l'importance de ces questions. Mais l'optimisme, en cette matière, doit rester mesuré. Il est facile de faire état d'une forte croissance du nombre de plaintes en un an lorsque l'on part de loin. Moins de 3800 signalements entre la fin mai et la fin septembre 2018 : le chiffre est loin d'être spectaculaire, rapporté à la population du pays, dans un contexte où les entreprises privées comme les administrations en parfaite conformité avec le règlement sont encore bien rares[38]. Il est probable que la capacité à défendre son intimité numérique soit fort mal distribuée dans la population. Le recours à la CNIL est le fait d'une petite élite bien renseignée, capable de comprendre ses droits et d'en demander le respect au régulateur : c'est elle seule qui a été aiguillonnée par les récentes actualités. Ses effectifs ont bel et bien augmenté, mais ils restent faibles. La grande complexité des textes applicables risque de dissuader le plus grand nombre, en dépit des efforts remarquables de vulgarisation de la CNIL - qui prennent la forme de synthèses rédigées dans un langage clair et de fiches pratiques.

Non seulement la motivation des individus s'effrite rapidement lorsqu'ils cherchent à comprendre la nature de leurs droits, mais leur patience est également mise à rude épreuve par les trop nombreuses demandes de consentement au traitement de leurs données qu'ils reçoivent. Le « bandeau cookies » qui s'affiche sur chaque site internet visité pour la première fois constitue l'illustration la mieux connue de ce phénomène[39]. Cette formalité vise en théorie un double objectif : rendre visibles les collectes de données en ligne pour en

38 - CNIL, « RGPD : quel premier bilan 4 mois après son entrée en application » ?, art. préc.

39 - Ce bandeau vise à délivrer l'information exigée par l'art. 5, 3) de la directive 2002/58 précitée : « Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données [...] ».

avertir l'individu et, surtout, permettre à la personne concernée de refuser son consentement, si elle le souhaite et que le traceur n'est pas absolument indispensable à l'exécution du service. Chacun sait qu'en pratique, il n'en est rien : ces bandeaux sont considérés par la plupart des internautes comme de simples obstacles placés sur le chemin de la lecture d'un article ou de l'accès à un service, et ils ne cherchent qu'à s'en débarrasser le plus vite possible. Lorsque l'on propose à un individu de choisir entre une récompense immédiate et tangible, même minuscule, et un danger lointain et impalpable, même redoutable, la fiction de l'agent rationnel a tôt fait de disparaître[40]. Certaines extensions de navigateur ont même été créées aux fins d'assurer la fermeture automatique et invisible de ces bandeaux. Certes, les rédacteurs du projet de règlement *e-privacy* sont conscients de cette difficulté, que l'on va tenter de contourner en invitant l'internaute à s'exprimer une fois pour toutes dans les réglages de son navigateur[41]. Mais si un tel système entre véritablement en action demain, rares seront les personnes qui choisiront, si elles ont la possibilité de s'exprimer une et une seule fois, d'être suivies au travers de leur navigation par des régies publicitaires centralisées, et de s'exposer à des annonces personnalisées. On touche ici à un non-dit de cette réglementation : s'il était véritablement aussi facile de dire oui que de dire non à ces formes de collecte de données, des centaines d'entreprises feraient faillite en quelques semaines. Un secteur économique entier s'est bâti sur le relâchement total, par sa clientèle, de son contrôle sur ses données.

Laissons de côté le cas particulier des cookies, et laissons même derrière nous le droit des données personnelles : le consentement machinal, rituel purement mécanique sans signification intellectuelle, affaiblit depuis longtemps le droit des contrats de masse. On signe sans les lire ses contrats bancaires, d'assurance et de

40 - En ce sens : Alessandro Acquisti et al., « Les comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », *Réseaux,* 2011/3 (n° 167), p. 105-130.

41 - « Le fait de centraliser le consentement dans des logiciels comme les navigateurs Internet, d'inviter les utilisateurs à choisir leurs paramètres de confidentialité et d'étendre les exceptions à la règle du consentement pour les cookies donnerait à une grande partie des entreprises la possibilité de se débarrasser des bandeaux et avis en la matière et conduirait donc à des économies de coûts et une simplification potentiellement importantes » (extrait de l'analyse d'impact accompagnant la proposition de règlement 2017/003 précitée).

téléphonie mobile. En ligne, on clique pour cocher une case « j'accepte les conditions générales » d'iTune*s*, ou de Google, ou de Facebook. S'il y a une deuxième case pour la politique de confidentialité, parce que le RGPD exige que le sort des données personnelles ne soit pas mêlé au reste du contrat, on cliquera simplement une deuxième fois[42]. Et si le traitement concerne des données sensibles au sens de l'article 9 – les convictions politiques, l'orientation sexuelle, des données génétiques – il y aura peut-être une troisième case à cocher, puisque le consentement doit alors être « explicite »[43]. Mais cela changera-t-il quelque chose, au fond ? Le Comité européen de la protection des données fait de son mieux, au travers de ses lignes directrices, pour donner de l'épaisseur, de la substance, de la réalité au consentement[44]. Mais la bataille est perdue d'avance et la réalité est celle-ci : le consentement est une machine à faire sauter la protection des personnes. Placées dans un contexte propice et face à un design suffisamment habile, elles disent oui à tout[45].

Postulons donc que la quasi-totalité de la population n'invoquera jamais les droits qu'elle tire du RGPD, et qu'on cherchera à lui extorquer des consentements vides de toute signification. Cette situation pourra s'améliorer (très) lentement si la CNIL est rejointe par l'Éducation nationale dans ses efforts de pédagogie et que l'on change ainsi d'échelle. En attendant, si la connaissance et le maniement habile du règlement sont le fait d'une petite élite spécialisée, alors pourquoi ne pas se reposer en partie sur elle ? C'est le sens des actions de groupe en matière de violation du droit des données personnelles. Le droit français s'est montré volontariste en la matière, puisque ces actions permettent aujourd'hui non seulement de faire cesser les violations de la réglementation, mais aussi d'obtenir la réparation des préjudices matériels et moraux

42 - Art. 7, 2) du règlement 2016/679 précité.

43 - Art. 9, 2), a) du règlement 2016/679 précité.

44 - G29 (qui était la dénomination du Comité européen de la protection des données avant le RGPD), *Lignes directrices sur le consentement*, 28 novembre 2017, révisées le 10 avril 2018.

45 - Sur ce point, la délibération SAN-2019-001 du 21 janvier 2019, par laquelle la CNIL inflige à Google une sanction de 50 millions d'euros, constituera sans doute un tournant historique. En exigeant un véritable « opt-in » clair et précis des utilisateurs pour que de la publicité ciblée puisse leur être adressée, la CNIL va contraire les modèles d'affaires à évoluer profondément.

subis par les personnes ayant rejoint l'action[46]. Toutefois, il faut ici encore regretter que la question n'ait fait l'objet d'aucune harmonisation européenne au sein du règlement, alors même que certaines des violations les plus graves du texte seront le fait d'acteurs internationaux et concerneront de nombreux pays de l'Union[47]. Les différences entre les législations nationales rendront difficiles, parfois même impossibles les regroupements de personnes concernées dépassant les frontières des États. Mais même ainsi entravées, ces actions de groupe constituent des outils puissants pour pousser les plus grands acteurs à se mettre en conformité avec la loi. Devant la CNIL, trois plaintes collectives ont été déposées par « la Quadrature du Net (plaintes concernant Google, Amazon, Facebook, LinkedIn et Apple, pour un total de 45 000 personnes concernées), l'association NOYB (Google) et l'ONG anglaise Privacy International (plaintes concernant 7 entreprises procédant à de la collecte à grande échelle de données en ligne) »[48].

Que des foyers de compétence de la société civile s'attribuent ainsi le rôle de vigies est une bonne chose. Mais les moyens qui sont les leurs les obligent à choisir leurs combats et à s'attaquer à quelques géants dont il n'est pas douteux qu'ils auraient fait l'objet de contrôles spontanés de la part de la CNIL assez rapidement. Si ces actions revêtent une importance symbolique indéniable, et à supposer qu'elles soient fondées et qu'elles aboutissent, elles ne feront que retirer quelques – grosses – gouttes d'eau à l'océan de la non-conformité. Il reste en effet à s'occuper des quelques centaines de milliers de responsables de traitement restants : considérons à présent l'effectivité du règlement de ce point de vue.

46 - Art. 43 ter de la loi n° 78-17 du 6 janvier 1978 dans sa rédaction issue de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Dans sa rédaction antérieure issue de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, l'action ne pouvait viser qu'à faire cesser le manquement.

47 - L'article 80 du RGPD laisse aux États membres une très large marge d'initiative en la matière.

48 - CNIL, « RGPD : quel bilan 6 mois après... », art. préc. *Adde* La Quadrature du Net, « Dépôt des plaintes collectives contre les GAFAM », article *laquadrature.net* du 28 mai 2018. En France, ces plaintes ont d'ores et déjà donné lieu à la délibération précitée SAN-2019-001 du 21 janvier 2019.

2 – Du point de vue des responsables de traitement et sous-traitants

À supposer que l'écrasante majorité des individus se désintéresse du sort de ses données personnelles, subsisterait malgré tout l'essentiel du règlement, constitué d'obligations qui pèsent sur les responsables de traitement et sous-traitants sans qu'il soit besoin de ne rien leur demander. Si cette protection plancher, ce statut d'ordre public développe réellement ses effets, l'essentiel est sauf, et l'incurie des personnes concernées sans conséquence grave. Respecter le RGPD, c'est, entre autres : fixer une finalité de traitement claire et précise ; collecter le minimum de données nécessaire à l'accomplissement de cette finalité, et pas une de plus ; les conserver le temps strictement nécessaire, et pas une minute en trop ; si une inexactitude est constatée, la rectifier de son propre chef ; empêcher leur destruction et leur altération par l'effet d'un accident ou d'une attaque ; s'abstenir de faire circuler les données auprès de sous-traitants non fiables ou les envoyer dans des pays où elles sont en danger[49].

La difficulté vient, on l'a dit, de ce que ces exigences existent depuis quarante ans, mais ne sont bien souvent respectées que depuis quelques mois, ou ne sont qu'en voie de l'être. La grande masse des responsables de traitement n'est pas mue par la poursuite de valeurs, par une saine conscience de son propre pouvoir ou des risques liés au développement frénétique de la société de l'information, car sans cela leur adhésion aurait été ancienne : elle a peur du gendarme. Ce ressort est puissant, mais il ne fonctionne durablement que si perdure l'impression qu'une chance sérieuse existe d'être pris et de subir effectivement les foudres de la loi.

Imaginons que la peine encourue pour un important excès de vitesse automobile passe d'un coup à plusieurs dizaines de milliers d'euros. Il s'ensuivrait probablement une stupeur des automobilistes, les poussant à surveiller leur compteur de très près. Mais si après quelques semaines le bruit commençait à courir qu'il n'existe que deux radars sur l'ensemble des routes de France, fussent-ils mobiles, il est probable que monterait doucement un sentiment d'impunité, une certitude qu'on ne sera pas, soi, frappé par un coup du sort aussi improbable. Cette situation, c'est celle dans laquelle se trouveront

49 - Art. 5 du règlement 2016/679 précité.

rapidement les entreprises privées de tailles petite et moyenne, de même que des collectivités territoriales de moindre importance. Car c'est un fait : les effectifs et le budget de la CNIL ne sont pas à la hauteur des missions confiées à cette autorité. Le rapport d'activité 2017 fait état d'environ 340 contrôles, dont une cinquantaine étaient spécifiquement dédiés à la vidéoprotection[50]. C'est beaucoup si l'on considère que la CNIL n'emploie que 198 personnes. C'est peu, très peu si l'on a égard au nombre des traitements de données déployés dans notre pays. Quant au budget de l'Autorité, il était en 2017 d'environ 17 millions d'euros. À titre de comparaison, le budget du Conseil supérieur de l'audiovisuel était de 38 millions d'euros[51].

En révisant tardivement la loi informatique et libertés, pour un résultat peu lisible, et en dotant la CNIL de moyens insuffisants, le gouvernement affiche une regrettable nonchalance à l'égard de la question des données personnelles. Pourtant, le modèle européen de protection des données aura besoin d'une promotion déterminée et d'un soutien sans faille de la part de l'ensemble des pays de l'Union, s'il veut s'imposer sur la scène mondiale. Car c'est bien de cela qu'il s'agit : d'une lutte pour imposer l'un des modèles possibles face à ses concurrents.

§2 : Le droit européen des données menacé au-dehors

Beaucoup de grandes entreprises souhaitent faire circuler les données personnelles des citoyens européens hors de l'Union, en particulier vers les États-Unis d'Amérique. Or, la sécurisation juridique d'un tel transfert se révèle particulièrement délicate, à supposer même qu'elle soit possible (A). Mais il n'y a là qu'une manifestation d'un mal plus profond : il est difficile d'envisager la coexistence de long terme, à l'échelle mondiale, de modèles de protection des données trop divergents (B).

50 - CNIL, 38ème rapport d'activité, présenté le 10 avril 2019, consultable sur cnil.fr.

51 - Source pour la CNIL : https://www.data.gouv.fr/fr/datasets/budget-de-la-cnil-1/. Pour le CSA : http://www.cbnews.fr/medias/plus-de-38-meur-de-budget-pour-le-csa-en-2017-a1031400.

A. Le difficile dialogue des modèles : le transfert des données hors de l'Union

Il est fréquent que les données personnelles circulent : d'un point de vue organisationnel, entre plusieurs co-responsables de traitement, entre un responsable de traitement et un sous-traitant, entre plusieurs sous-traitants successifs ; d'un point de vue géographique, entre pays de l'Union, mais aussi en direction de pays tiers. Or, une chaîne n'est aussi solide que le plus faible de ses maillons. Il ne servirait à rien d'instaurer un degré élevé de protection dans l'Union si des données pouvaient, en quelques millisecondes, se trouver collectées, hébergées, ou exploitées dans un pays n'y voyant qu'une matière première ordinaire. Dans la plupart des cas, il est ainsi difficile d'exporter des données hors de l'Europe dans un parfait respect du règlement.

La solution théoriquement la plus simple est celle-ci : « Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique »[52].

Mais un étudiant en droit déterminé du nom de Maximillian Schrems a balayé toute certitude en la matière. Membre, s'il en est, de cette élite étroite durablement marquée par les révélations d'Edward Snowden, il a remis en question devant la CJUE la décision de la Commission européenne de reconnaître les États-Unis d'Amérique comme un pays offrant une protection adéquate, dans le cadre du mécanisme appelé *Safe Harbor.* La Cour jugea notamment, à la lumière des révélations sur les programmes de la NSA, que « [...] une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée » [53]. Bien sûr, le RGPD a tiré les conséquences de cet arrêt en livrant à la Commission des instructions précises

52 - Article 45, 1) du règlement précité.

53 - CJUE, 6 octobre 2015, C-362/14, *Maximillian Schrems c/ Data Protection Commissioner*, §94.

dans l'examen des demandes d'adéquation présentées par les pays tiers[54]. Mais la Commission peut néanmoins encore se tromper, et ses décisions être encore invalidées par la Cour, avec effet immédiat au jour du prononcé de l'arrêt. Il n'est pas impossible que ce soit le destin du *Privacy Shield*, successeur du *Safe Harbor*[55].

Que faire, alors, si l'on ne peut faire confiance à une décision d'adéquation ? L'article 46 ouvre dans ce cas la porte à des « transferts moyennant des garanties appropriées »[56]. Deux de ces garanties sont actuellement pratiquées à une large échelle : les « règles d'entreprise contraignantes » et les « clauses types de protection des données adoptées par la Commission »[57]. Commençons par le second type, car il est le plus simple à mettre en œuvre : il suffit d'intégrer – certains diront de « copier-coller » – les clauses conçues par la Commission européenne dans un contrat conclu entre l'exportateur et l'importateur de données. Ce RGPD en miniature va alors contraindre l'importateur signataire, en théorie, à une rigoureuse discipline.

La solution semble simple. Trop peut-être, car il ne faut que quelques heures pour mettre en place le contrat, alors qu'il faudrait des mois d'efforts pour en tirer les conséquences techniques et organisationnelles, et certains risquent de s'en tenir à la première partie. Surtout, M. Schrems a trouvé là un nouveau champ de bataille : il estime que la décision par laquelle la Commission européenne a validé les clauses types peut être remise en cause de la même façon que ses décisions d'adéquation, si ces clauses sont insuffisamment protectrices. L'autorité irlandaise de protection des données a trouvé ses arguments convaincants et posé une question préjudicielle à la CJUE : pour ceux qui espéraient avoir trouvé là un fondement solide aux transferts internationaux de données, un nouveau naufrage est donc à redouter[58].

54 - Art. 45, 2) du règlement précité.

55 - En ce sens, V. not. C. Castets-Renard, « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », *Dalloz IP/IT*, 2016.444.

56 - Pour une présentation plus détaillée de ces mécanismes : F. Naftalski, « L'impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT*, 2016.340.

57 - Art. 46, 2, b) et d).

58 - Hight court commercial, 3 octobre 2017, n° 4809 P, spéc. n° 338 : https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf.

La dernière solution envisageable, les « règles contraignantes d'entreprise » (en anglais *BCR*, pour *Binding corporate rules*), concerne les grands groupes de sociétés. Il s'agit de rédiger un document conçu sur mesure, contraignant et très détaillé sur la politique applicable aux données personnelles au sein de la multinationale considérée[59]. Il n'entrera pas en vigueur avant d'avoir été approuvé par les autorités de contrôle : contrairement aux « clauses types » de la Commission, il garantit donc véritablement un degré élevé de protection avant que la moindre information ne commence à circuler. Mais cette solution s'adresse exclusivement aux très grandes entreprises, qui seules auront les moyens et les compétences nécessaires à la rédaction de ces « règles contraignantes ».

Plus fondamentalement, si l'on reprend le cas d'export le plus courant, celui vers les USA, on comprend que ni les clauses-types, ni les *BCR* ne pourront résoudre l'intégralité des problèmes dénoncés par M. Schrems et les autres défenseurs de la vie privée[60]. Ces mécanismes essaient de faire surgir, sur une base contractuelle et non plus légale, des obligations à la charge des responsables de traitement et des sous-traitants, telles que celles de respecter une finalité de traitement, de minimiser les manipulations de données ou de les sécuriser. Mais la signature d'un simple contrat ne suffira pas à couper l'importateur de données de l'environnement législatif national dans lequel il évolue. Si l'on débarrasse la discussion sur les transferts internationaux de données de ses oripeaux techniques, la question qui surgit est d'une nature fondamentalement politique : si le reste du monde ne veut pas se hisser aux standards européens de protection des données, cela constituera un problème qu'aucun outil exclusivement juridique ne pourra résoudre. Dans un monde où les informations ne demandent qu'à circuler, les modèles de protection des données fondamentalement divergents ne pourront pas toujours coexister de manière simple et pacifique. Régulièrement, ils entreront en collision.

59 - https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr-binding-corporate-rules.

60 - En ce sens : B. Haftel, « Transferts transatlantiques de données personnelles : la Cour de justice invalide le Safe Harbour et consacre un principe de défiance mutuelle », *D.*, 2016.111.

B. L'affrontement des modèles : un choc des souverainetés

Puisqu'il semble aujourd'hui très difficile d'assurer à un export de données hors de l'Union européenne une sécurité juridique satisfaisante à long terme, quelles conséquences faut-il en tirer ? Ces flux doivent-ils tout simplement cesser ? Les grandes multinationales doivent-elles mettre en place deux circuits de traitement de données totalement hermétiques l'un à l'autre : un pour l'Europe, un pour le reste du monde ? On peine à l'imaginer. Certains sites américains, notamment les versions en ligne de grands quotidiens régionaux, ont pourtant choisi de faire sécession d'avec l'Internet européen. Le *Los Angeles Times*, par exemple, indique à ses visiteurs du vieux continent : « *Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism* »[61]. Le symbole constitué par ces blocages de sites est fort, et l'on peut comprendre qu'il ait marqué les esprits[62]. Un « rideau de fer numérique » s'abattrait-il autour de l'Union ? La stratégie autarcique du *Los Angeles Times* est cependant réservée à des acteurs qui tiraient des revenus négligeables, voire nuls, des visites des internautes européens. Tous ceux pour qui l'Europe constitue un marché important, fût-il secondaire, ou qui souhaitent tout simplement véhiculer une image de plus grande ouverture internationale, seront poussés à trouver des solutions pour agir conformément au règlement. Le quotidien national *USA Today* propose ainsi une version de son site internet « spéciale Europe » sans aucun traceur ni publicité ciblée[63].

61 - Il s'agit de la page http://www.tribpub.com/gdpr/latimes.com/ telle qu'elle s'affichait encore à la date du 10 décembre 2018.

62 - Par ex. T. Noisette, « RGPD : des sites américains claquent la porte au nez des internautes européens », article n*ouvelobs.com* du 28 mai 2018.

63 - https://eu.usatoday.com/EU-learn-more/ : « This site does not collect personally identifiable information or persistent identifiers from, deliver a personalized experience to, or otherwise track or monitor persons reasonably identified as visiting our Site from the European Union. We do identify EU internet protocol (IP) addresses for the purpose of determining whether to direct you to USA TODAY NETWORK's EU Experience ».

À présent, que va-t-il se passer ? Entre les modèles européen et américain, la tension continue à monter. La question de la portée territoriale du droit au déréférencement en constitue l'une des plus frappantes manifestations. Dans un arrêt très remarqué de 2014, la Cour de justice de l'Union européenne avait décidé qu'une personne est en droit de demander à un moteur de recherche généraliste, tel que celui de Google, de retirer certains résultats associés à une recherche portant sur ses seuls nom et prénom[64]. Peuvent ainsi être supprimés des liens qui mènent vers des pages pourtant parfaitement licites au regard des règles régissant la liberté d'expression. La solution peut choquer celui qui la découvre pour la première fois. Elle s'explique pourtant : un moteur de recherche peut avoir pour effet d'attacher une information gênante à un individu durant des décennies, alors qu'elle serait sans cela rapidement retournée dans l'ombre. Voici qui rappelle une autre formule visionnaire de Jean Foyer, en 1977 : « [...] l'ordinateur a une mémoire qui, à la différence de la mémoire des hommes, n'a pas la faculté d'oublier. Il n'oublie que ce qu'on efface en lui ». La jurisprudence *Google Spain* constitue un remède à cette hypermnésie informatique, raison pour laquelle elle est parfois désignée sous l'appellation, techniquement trop vague, de « droit à l'oubli ». L'aspect qui nous intéresse ici tient à la manière dont cette décision a été appliquée, s'agissant d'un point sur lequel elle n'avait pas pris position explicitement : sa portée territoriale. Lorsqu'elle devait retirer des résultats de recherche relatifs, par exemple, à un internaute français, la société Google avait commencé par le faire seulement sur l'adresse www.google.fr. La CNIL ne s'en est pas satisfaite, car alors un Espagnol pouvait toujours consulter une version non expurgée du moteur sur www.google.es. Pire, un

64 - CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12 : *RLDI*, août 2014, n° 107, p. 32, note O. Pignatari ; *RJPF*, juill. 2014, n° 7, p. 19, note S. Mauclair ; *JCP G,* juin 204, n° 26, p. 1300, note L. Marino. *Adde* not. J.-M. Bruguière, « Droit à l'oubli numérique des internautes ou... responsabilité civile des moteurs de recherche du fait du référencement ? », *CCE,* mai 2015, n° 5, p. 15 ; R. Perray et P. Salen, « La Cour de justice, les moteurs de recherche et le droit "à l'oubli numérique" : une fausse innovation, de vraies questions », *RLDI,* nov. 2014, n° 109, p. 35 ; V.-L. Bénabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.*, 2014, p. 1476 ; N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.,* 2014, p. 1481 ; L. Marino, « Comment mettre en œuvre le "droit à l'oubli" numérique ? », *D.,* 2014, p. 1680.

internaute français pouvait en réalité accéder lui aussi aux résultats sans censure s'il forçait la connexion à s'instaurer avec google.com ou .es plutôt que .fr. L'Autorité demandait alors qu'un résultat retiré le soit sur toutes les versions mondiales du moteur, ce qui aurait eu pour effet d'altérer même des résultats affichés par un internaute américain sur le sol des USA. Google a alors formulé une nouvelle proposition : détecter, en utilisant l'adresse IP, que la requête était formulée par un internaute situé sur le territoire national du demandeur, et expurger alors les résultats pour toutes les extensions utilisées dans l'adresse du moteur. La CNIL a considéré une nouvelle fois cette proposition comme insuffisante, notamment car « il existe des solutions techniques qui permettent de contourner la mesure de filtrage proposée par la société en permettant à l'internaute de choisir l'origine géographique de son adresse IP (utilisation d'un VPN par exemple) [...]. Seule une mesure s'appliquant à l'intégralité du traitement lié au moteur de recherche, sans distinction entre les extensions interrogées et l'origine géographique de l'internaute effectuant une recherche est juridiquement à même de répondre à l'exigence de protection telle que consacrée par la CJUE »[65]. Saisi d'un recours contre cette décision, le Conseil d'État a posé une question préjudicielle à la CJUE, à laquelle il n'a pas encore été apporté de réponse[66]. L'affaire a suscité une vive émotion outre-Atlantique, où l'on accepte mal qu'une autorité administrative française entende altérer l'information accessible aux Américains sur leur propre sol[67]. L'Europe pourrait rétorquer que de telles altérations ne se produisent que lorsque des données personnelles de citoyens de l'Union sont en cause, et que le lieu où les informations sont consultées n'est pas la considération fondamentale.

Par-delà les argumentations juridiques, on aperçoit donc à nouveau la question politique et, surtout, le choc frontal des souverainetés. Des visions différentes du monde entrent en collision et cherchent à s'imposer. Disons-le d'emblée : il est vain d'espérer que le modèle européen essaime dans son intégralité. La jurisprudence sur le déréférencement en constitue un excellent exemple : certains points

65 - Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X.

66 - CE, 19 juillet 2017, *GOOGLE INC.*, N° 399922.

67 - V. dans le présent ouvrage E. Weil, « Le règlement général sur la protection des données à caractère personnel appliqué aux états tiers : une appréciation de son caractère extraterritorial », spéc. les références citées notes 97 et s.

du régime européen sont le fruit d'un arbitrage si difficile entre des valeurs toutes cardinales – ici, la vie privée contre la liberté d'expression – qu'un large consensus à travers le temps et l'espace apparaît improbable. Tout le monde ne sera pas convaincu. Mais si l'on revient au cœur de ce qui constitue le RGPD, il s'agit d'accepter quelques idées simples : les données personnelles ne constituent pas une matière première comme une autre pour les entreprises ; elles doivent être manipulées d'une main tremblante, rassemblées avec sobriété, pour des objectifs précis, et faire l'objet de protections sérieuses contre les erreurs et les agressions. À partir de là, proposons un parallèle, quelque peu forcé, mais à caractère pédagogique, avec la lutte contre le réchauffement climatique. Si de nombreux pays sont convaincus que les objectifs poursuivis par l'Europe sont louables et servent le bien commun, ils peuvent les rallier et former une zone relativement homogène, au sein de laquelle le jeu économique se déploie ensuite, dans le respect de règles comparables. Mais si certains géants comme les USA considèrent que tout ceci n'est qu'obstacles à l'efficacité de leurs modèles d'affaires, ils peuvent envoyer au monde une contre-proposition, qui risque d'avoir des adeptes, au sein de laquelle les entreprises évoluent sans ces contraintes, ce qui suppose des coûts moindres et des bénéfices plus élevés. Pour représenter cette lutte d'influence, l'image de deux blocs statiques entre lesquels un rideau de fer serait tombé n'est décidément pas la bonne. La tectonique des plaques constitue une meilleure représentation : des deux modèles qui se pressent actuellement l'un contre l'autre, l'un finira par passer au-dessus. L'issue de cet affrontement est en partie dans les mains de l'opinion publique américaine, comme l'a montré l'adoption récente par la Californie, pourtant berceau des GAFA, d'un *Consumer Privacy act* améliorant singulièrement la protection des données personnelles de ses citoyens[68]. L'affaire *Cambridge Analytica* avait donné naissance à une pétition signée plus de 600 000 fois, enjoignant le législateur californien d'agir[69]. À l'heure où le volontarisme de nos décideurs politiques en matière de protection des données manque de constance, il est fort possible que le meilleur ambassadeur du modèle européen se nomme Mark Zuckerberg.

68 - V. not. caprivacy.org, « AB 375 Signed - Californians for Consumer Privacy Applauds Successful Passage of Groundbreaking Legislation », article du 28 juin 2018.

69 - A. Schwartz, L. Tien et C. McSherry, « How to improve the California Consumer Privacy Act of 2018 », article *eff.org* du 8 août 2018.