Université Panthéon-Assas – Institut de droit comparé

UNIVERSITÉ
PANTHÉON-ASSAS
- PARIS II -

Master 2 Recherche – Droit européen comparé

2015 - 2016

La protection des données à caractère personnel : importation du modèle américain au sein de l'Union européenne

Mémoire rédigé sous la direction du Professeur Mathieu Carpentier

Sibylle Pouillaude

Travail effectué dans les bibliothèques de la Columbia University et de la New York University dans le cadre d'un séjour de recherche

Remerciements

Tous mes remerciements à mon directeur de mémoire pour son soutien, ainsi qu'au professeur Broyelle pour avoir accepté de prendre part au jury de soutenance.

Tous mes remerciements également à M. Winston Maxwell, avocat au barreau de Paris et au barreau de New-York, pour m'avoir fourni des informations et des articles précieux.

Résumé

Le droit de la protection des données à caractère personnel est un droit relativement jeune, qui est apparu des deux côtés de l'Atlantique vers le milieu du XXème siècle mais qui ne s'affirme réellement que depuis les années 1995. C'est un droit qui est encore en construction. Le droit de la protection des données comporte une importante dimension internationale car les données circulent. Les principes de protection des données aussi.

Aux États-Unis, il existe notamment deux principes fondamentaux de la protection des données à caractère personnel : l'*accountability*, une forme de responsabilité devant autrui, et l'*unfairness* connu en Europe sous le nom de principe de loyauté. Or l'Union européenne cherche également, depuis quelques années, à intégrer ces deux principes dans son propre système de protection des données. L'Union européenne a ainsi absorbé le principe proprement américain d'*accountability* et s'est appropriée sa philosophie et ses outils, la différence résidant dans le fait que l'*accountability* s'inscrit dans un cadre institutionnel fort en Europe. Toutefois le principe d'*accountability* risque de connaître les mêmes difficultés que celles qui se sont posées aux États-Unis. Quant à l'*unfairness*, si les États-Unis et l'Union européenne en ont une approche théorique différente, en pratique, ils appliquent ce principe aux mêmes problèmatiques. Les États-Unis ont par ailleurs étendu l'application du principe d'*unfairness*, ce qui pourra peut-être à l'avenir, inspirer les autorités de contrôle européennes.

Sommaire

Introduction

Avant d'envisager le contenu des principes américains et leur réception en Europe, il convient d'abord de revenir sur le double aspect de la donnée à caractère personnel : elle revêt un aspect économique (I) et un aspect juridique (II).

I - La donnée personnelle : une donnée économique

"*Comprendre le comportement du consommateur afin de pouvoir le cerner, lui proposer le bon produit au bon moment, mais surtout le convaincre que le produit qui lui est proposé est adapté à ses besoins : voilà ce dont rêvent toutes les entreprises*[1]."

Selon un rapport de la commission européenne, l'ensemble des données personnelles des citoyens européens pourra être évalué d'ici 2020 à près de 20 000 milliards d'euros[2]. Face à un tel constat, des questions émergent : qu'est-ce qu'une donnée, qu'est-ce qui fait sa valeur, à quoi sert-elle ?

Selon M. Dewost, directeur adjoint de la mission "Programme d'investissements d'Avenir", l'apparition de la donnée personnelle est liée au développement de l'outil informatique, à la standardisation des smartphones, et aux trois lois fondamentales de l'informatique[3]. Tandis que la loi de Moore (la puissance de calcul des micro-processeurs ou puces double tous les 18 mois) prévoit que les machines seront de moins en moins coûteuses et de plus en plus efficaces, la loi de Metcalfe prédit que la valeur totale du réseau augmente en proportion du carré du nombre d'utilisateurs, c'est-à-dire que la mise en réseau des outils informatiques est facilitée et accélérée. La loi de Rifkins démontre quant à elle que le coût marginal de stockage

---

[1] Jean-Louis BARMA, *À quoi rêvent les entreprises*, Épigraphe in Michel Houellebecq *Plateforme*, éditions Flammarion, Paris, 2001

[2] European Commission, *The EU Data Protection Reform and Big Data*, mars 2016, consultable sur http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf, ci après *The EUDP and Big Data*

[3] M. DEWOST, lors de la conférence *Données personnelles, Big Data et droits individuels. Les différentes approches entre les différents systèmes juridiques*, organisée par la Société de Législation Comparée le 29 janvier 2016

de l'information tend vers zéro. Ceci permet d'expliquer pourquoi 80% des données personnelles ont été produites au cours de ces deux dernières années[4].

Or les données personnelles sont devenues l'or noir de l'économie numérique[5]. Plus l'outil informatique se banalise et plus la technologie numérique innove et pénètre le quotidien des consommateurs, plus les entreprises exploitent des données qui, dans leur ensemble, sont désignées par l'expression "Big Data". Le Big Data désigne une large variété de données, de sources différentes (données produites par les hommes, par les machines ou par des capteurs), et de nature différente (données climatiques, données de santé, données de géolocalisation etc.) ; parmi les données qui composent le Big Data, il y a donc les données personnelles (c'est-à-dire les données qui ne sont plus anonymes[6] (voir *infra*)). Il suffit de citer le secteur de l'assurance, de la santé, de la publicité, du divertissement ou encore du service à la personne, pour comprendre que l'entreprise, si elle en sait plus sur le consommateur, le ciblera plus facilement ou lui proposera plus rapidement le service approprié. Par ailleurs, de plus en plus d'applications ou de services sont désormais construits sur la donnée personnelle, que ce soit aujourd'hui les applications qui utilisent la géolocalisation pour trouver le restaurant le plus proche,[7] ou qui proposent la musique que le consommateur est susceptible d'aimer grâce à l'analyse de ses goûts[8], et demain la voiture connectée[9].

---

4 Ibid - M. DEWOST, lors de la conférence *Données personnelles, Big Data et droits individuels. Les différentes approches entre les différents systèmes juridiques*, organisée par la Société de Législation Comparée le 29 janvier 2016

5 Expression utilisée par Bruno LASSERRE président de l'Autorité de la concurrence, conférence *Les données et la concurrence dans l'économie numérique*, organisée par cette Autorité le 8 mars 2016, vidéos disponibles sur http://www.autoritedelaconcurrence.fr/user/rdv.php?id_rub=631

6 Édouard GEFFRAY, secrétaire général de la CNIL, conférence *Les données et la concurrence dans l'économie numérique*, organisée par cette Autorité le 8 mars 2016, vidéos disponibles sur http://www.autoritedelaconcurrence.fr/user/rdv.php?id_rub=631

7 Auteur anonyme, *Dossier : 13 applis gratuites pour trouver et choisir le bon restaurant grâce à l'iPhone*, Site internet iphon.fr, consultable sur http://www.iphon.fr/post/2011/02/18/Dossier-%3A-10-applications-iPhone-pour-trouver-le-restaurant-qu%E2%80%99il-vous-faut

8 Auteur anonyme, *Discover New Music with Spotify's Automagic Playlists*, Site internet make use of, consultable sur http://www.makeuseof.com/tag/discover-new-music-spotifys-automagic-playlists/

9 Auteur anonyme, *La voiture connectée*, Site internet usine digitale, consultable sur http://www.usine-digitale.fr/voiture-connectee/

Les entreprises ont donc intérêt à récupérer les données personnelles de leurs consommateurs, et quant à ces derniers, comme le résumait ironiquement Bruce Schneier à propos de Facebook : "*if you don't pay the product, you are the product*[10]".

Cependant, bien que les consommateurs profitent d'un accès gratuit à de nombreuses sources d'informations ou d'une facilité d'achat sur internet, l'aisance avec laquelle les entreprises peuvent collecter et recouper des informations sur eux, et la perte de contrôle de leurs données qui s'ensuit, ont fait émerger de nouvelles préoccupations concernant la protection de la vie privée. Selon un sondage mené par l'Eurobarometer en 2015, 81% des européens ont le sentiment qu'ils n'ont pas de contrôle sur leurs données personnelles, et seuls 24% font confiance aux entreprises du net[11]. La CNIL remarque également que les plaintes des personnes physiques relatives à l'exploitation de leurs données personnelles ont augmenté de 30% au cours de la dernière année[12].

C'est notamment pour ces raisons qu'une réforme est apparue nécessaire aux États Unis et en Europe. L'Union européenne vient ainsi d'adopter un nouveau réglement européen[13]. La Maison Blanche dans son rapport *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*[14]*,* puis la *Federal Trade Commission* (l'agence gouvernementale chargée de

---

10 Roberto di COSMO, Reprenons le contrôle de nos données, point de vue publié dans le journal du CNRS, 14 avril 2015, consultable sur : https://lejournal.cnrs.fr/billets/reprenons-le-controle-de-nos-donnees?utm_content=buffer5fa32&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

11 Ibid - The EUPD and Big Data

12 Ibid - Édouard GEFFRAY, secrétaire général de la CNIL, conférence *Les données et la concurrence dans l'économie numérique*, organisée par cette Autorité le 8 mars 2016, vidéos disponibles sur http://www.autoritedelaconcurrence.fr/user/rdv.php?id_rub=631

13 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avril 2016, ci après règlement européen sur la protection des données

14 White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, consultable sur https://www.whitehouse.gov/sites/default/files/privacy-final.pdf, introduction, "The Administration has called for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors that are not subject to existing Federal data privacy laws"

l'application du droit de la consommation aux États-Unis[15]), encouragent, quant à eux, le Congrès américain à rédiger une loi de protection des données à caractère personnel. Ce changement de position de la part de la FTC, pourtant historiquement opposée à l'interventionisme législatif[16] (voir *infra*), a été applaudi par les groupes de défense des consommateurs, comme *Consumer Watchdog*[17], et par les défenseurs de la vie privée en ligne.

II - La donnée personnelle et le droit au respect de la vie privée

Bien que les États-Unis[18] et l'Europe fassent le même constat, c'est à dire l'enjeu que représentent les données personnelles pour l'économie numérique et pour la vie privée des consommateurs, leur façon de concevoir la donnée personnelle, et donc leurs systèmes de protection, sont différents (voir *infra*).

Tout d'abord, les conceptions de la notion de vie privée en Europe et de *right to privacy* aux États-Unis sont différentes.
Aux États-Unis, la protection de la vie privée sert d'abord à se protéger du gouvernement. Le droit à la protection de la vie privée découle du 4ème amendement de la Constitution, conçu

---

15 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), p.1 "The commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation"

16 FTC, *Self-Regulation and Privacy Online* : A Report to Congress, juillet 1999, consultable sur https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf. En 2000 le FTC avait cependant demandé la vote d'une loi par le congrès sur la protection des données personnelles, mais suite à l'arrivée du président Bush au pouvoir et au changement de direction au sein du FTC, l'Agence avait repris sa position initiale : encourager la self-regulation (source Michael D. SCOTT, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation : Has The Commission Gone Too Far ?*, Administrative Law Review, Vol. 60, No. 1, décembre 2008, p. 127-183)

17 Internet Business Newsweekly, *Consumer Watchdog Calls On FTC To Enact Do Not Track, Says Force of Law Needed*, Business Insights : Essentials, mars 2011. L'article fait suite au rapport préliminaire du FTC en 2010. "Consumer Watchdog said the FTC report proposes a solid framework with principles drawn from Fair Information Practices (FIPs) that will go far to ensure that consumers are protected. That framework must be enacted by regulation through a rulemaking process".

18 Ibid - White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, introduction "When consumers provide information about themselves ... they reasonably expect companies to use this information in ways that are consistent with the surrounding context. Many companies live up to these expectations, but some do not. Neither consumers nor companies have a clear set of ground rules to apply in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices warrant their trust."

pour protéger les citoyens américains contre l'intrusion de l'État dans leur vie privée (protection contre les perquisitions, les fouilles etc.). Le droit à la protection de la vie privée ne va cependant être reconnu que ponctuellement[19], notamment pour la voiture[20], l'extérieur de la maison[21] et les conversations téléphoniques[22]. C'est la *common law* de chaque État qui va ensuite reconnaître un droit à la protection de la vie privée : l'article du 15 décembre 1890 dans la *Harvard Law Review, The Right to Privacy,* de M. Warren et M. Brandeis, est cité comme la première déclaration implicite du droit au respect de la vie privée, et est compris comme le droit "d'être laissé tranquille". Il identifie les règles de la responsabilité civile en matière d'atteinte à la vie privée : ces *privacy torts* protègent l'individu contre les incursions dans leur vie privée, notamment contre la publication de photographies sans le consentement de la personne intéressée[23].

En Europe, ce droit est consacré comme un droit fondamental à l'article 8 de la convention européenne des droits de l'homme (CEDH) en 1950 : "Toute personne a droit au respect de sa vie privée...[24]". Le principe de protection de la vie privée était connu depuis longtemps en Europe : par exemple en France dès 1791, les constituants prévoyaient déjà un article pour assurer la protection contre les "calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée" (article 17 de la Constitution de 1791), puis la notion se développe au cours du XIXème siècle, est aujourd'hui consacré en France à l'article 9 du code civil, et a valeur constitutionnelle (décision 94-352 du Conseil Constitutionnel).

C'est ainsi qu'en Europe le droit à la protection de ses données à caractère personnel est un droit fondamental[25], et la donnée à caractère personnel est définie de manière constante

---

19 Winston J. MAXWELL et Christopher WOLF, *Protection des données personnelles : États-Unis et Europe convergent sur tout, ou presque*, Éditions multimédia économie numérique et nouveaux médias, édition juridique, numéro 55, avril 2012

20 Supreme Court, *United States v Jones*, 132 S.Ct.949 (2012)

21 Supreme Court, *Florida v Jardines*, 133.S.Ct. 1409 (2013)

22 Supreme Court, *Katz v United States*, 389 U.S 247 (1964)

23 Jean-Louis HALPERIN, *Protection de la vie privée et privacy : deux traditions juridiques différentes ?*, Les nouveaux cahiers du Conseil constitutionnel 2015, p.59-68

24 Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, article 8 "Droit au respect de la vie privée et familiale"

25 Traité sur le fonctionnement de l'Union Européenne, 2012/C 326/01, octobre 2012, article 16 "Toute personne a droit à la protection des données personnelles la concernant"

comme "toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale". (Règlement européen art.4 point 1). La simple collecte de la donnée peut donc être soumise à un contrôle sur les motivations, sur la proportionnalité, etc.

Contrairement à l'approche européenne, l'approche américaine ne retient pas de définition générale de la donnée personnelle. Aux États-Unis, les données personnelles ont un caractère commercial, sauf certaines données sensibles protégées par la loi (comme celles relèvant du *Children's Online Privacy Protection Act* ou celles relevant le *Health Insurance Portability and Accountability Act*[26]). Ainsi, selon le Professeur Solove, "les États-Unis ont laissé au cours des dernières années la protection de la vie privée aux marchés plutôt qu'à la loi[27]"'

Cette différence d'approche permet peut-être d'expliquer la différence qui existe dans les termes utilisés par les textes. Ainsi, pour désigner la personne à laquelle la donnée personnelle se rattache, les textes américains retiennent la notion de "*consumer*" (consommateurs), alors qu'en Europe c'est celle de "personnes physiques" qui est préférée. Pour ensuite identifier les agents qui collectent, utilisent et diffusent ces données personnelles, les États-Unis font directement référence aux personnes morales : on retrouve principalement dans les textes les termes "*companies*", mais aussi "*Data brokers*" ou encore le terme plus général de "*all commercial entities*"[28]. Les textes de l'Union Européenne[29] préfèrent utiliser la notion de

---

[26] Children's Online Privacy Protection Act, 15 U.S.C, §6501-6506, 15 octobre 1998 ; Health Insurance Portability and Accountability Act, 42 U.S.C §1320d-1320d-8, 1996

[27] Daniel J. SOLOVE, *A Brief History of Information Privacy* Law, in Proskauer on privacy, GW Law Faculty Publication & Other Works, PLI, 2006

[28] Voir notamment FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, mars 2012, consultable sur http://www.ftc.gov/sites/ default/files/ documents/reports/federal-trade-commission-report-protecting-consumer-p rivacy-era-rapid-change-recommendations/120326privacyreport.pdf

[29] Voir notamment le règlement européen sur la protection des données

"traitement" et de "responsable de traitement", et ne font ainsi pas de différence entre les entreprises et les administrations[30].

Pour beaucoup d'auteurs cette différence d'approche a pour conséquence que le dialogue entre les systèmes est impossible ou très délicat. Certains estiment même que pour se garantir de toute atteinte à la vie privée il faudrait même arrêter de souscrire aux services proposés par les entreprises américaines[31]. Les deux systèmes de protection des données personnelles seraient en effet diamétralement opposés : à l'approche européenne qui privilégie des règles rigides, impératives et détaillées au nom de la sécurité juridique et de la protection d'un droit fondamental, s'oppose l'approche américaine, qui fonctionne essentiellement avec des standards, au nom de l'adaptabilité des normes aux évolutions technologiques et économiques[32].

Il semble cependant que la compréhension est possible, voir même effective. Ainsi, même si l'Union européenne n'admet le transfert de données vers les pays tiers seulement lorsque le niveau de protection accordé est équivalent à celui qui existe en Europe[33], avec les États-Unis, les enjeux économiques sont si importants (les plus grandes entreprises de l'économie numérique telles Google, Facebook, Twitter, Amazon, etc., sont américaines) que, bien qu'une décision de la Cour de Justice de l'Union européenne le 6 octobre 2015 sur le transfert de données entre Facebook Irlande et Facebook États-Unis ait invalidé le *Safe Harbor* (accord prévoyant le transfert de données personnelles européennes vers les entreprises américaines

---

30 Règlement européen sur la protection des données, article 4 définitions "On entend par "traitement" toute opération... appliquée à des données... à caractère personnel telle que la collecte...l'utilisation... la diffusion... ; ... par "responsable de traitement" la personne physique ou morale... ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement... "

31 Joël IGNASSE, *Richard Stallman veut éliminer Facebook pour protéger la vie privée*, Sciences et Avenir High Tech, 16 mars 2016, consultable sur http://www.sciencesetavenir.fr/high-tech/informatique/20160316.OBS6588/richard-stallman-veut-eliminer-facebook-pour-proteger-la-vie-privee.html

32 Colin J. BENNETT, *International Privacy Standards : Can Accountability be Adequate ?,* Privacy Laws and Business International, Vol. 106, 2010

33 Règlement européen sur la protection des données, Chapitre V "Transferts... Vers des pays tiers..." ; 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 de 1995 sur la protection des données], article 25 sur les transferts

qui présentaient certaines garanties)[34] au motif que la protection des données personnelles n'était plus garantie aux États-Unis suite aux révélations de M. Snowden, la Commission européenne a adopté le 12 juillet 2016 une nouvelle décision d'adéquation, qui reconnaît un *privacy shield*, c'est-à-dire un niveau de protection "essentiellement équivalent" assuré aux données personnelles européennes transférées dans les entreprises américaines qui respectent les termes de l'accord[35]. Ses contradicteurs mettent déjà en lumière l'insuffisance de l'accord, qui ne contiendraient pas plus de garanties que celles déjà prévues par le *Safe Harbor*[36]. Mais au-delà des accords qui mettent en place des "niveaux de protection équivalent", on observe dans les textes, ou en pratique, un certain rapprochement entre les systèmes. Toutefois, avant d'étudier l'influence des principes américains en droit de la protection des données personnelles au sein de l'Union européenne, il faut dans un premier temps regarder comment fonctionnent ces deux systèmes de protection. C'est ce qui va être étudié maintenant.

---

[34] Cour de Justice de l'Union Européenne, *Maximillian Schrems / Data Protection Commissioner*, affaire C-362/14, Luxembourg, 6 octobre 2015

[35] CNIL, *Adoption de la décision d'adéquation du Privacy Shield par la commission européenne*, 12 juillet 2016, consultable sur https://www.cnil.fr/fr/adoption-de-la-decision-dadequation-du-privacy-shield-par-la-commission-europeenne

[36] Syndicat de la magistrature, *Privacy Shield : Alerte de l'observatoire des Libertés et du numérique*, communiqué de presse du 8 avril 2016

Titre préliminaire - Présentation des acteurs et des principaux instruments

L'Union européenne (I) et les États-Unis (II) ont adopté deux systèmes de protection des données à caractère personnel *a priori* différents.

I - Le droit de la protection des données à caractère personnel en Europe

Le principe de la protection des données à caractère personnel est connu depuis longtemps en Europe (A) et l'Union européenne a développé un système général et spécial de protection des données (B). Le nouveau règlement européen vient reprendre le droit de la protection des données et le moderniser (C).

A - Historique de la protection des données à caractère personnel en Europe

Le principe de protection des données à caractère personnel apparait au milieu du XXème siècle (a) mais c'est la directive de 1995 et les textes qui ont suivi qui ont instauré un véritable droit européen de la protection des données à caractère personnel, et qui ont consacré le droit à la protection de ses données comme un droit fondamental (b).

1 - Avant 1995

Le principe de la protection de la vie privée et des données personnelles est apparu au milieu du XXème siècle en Europe. Les premiers textes qui concernent la protection de la vie privée datent du milieu du XXème siècle. En 1950, la Convention Européenne des Droits de l'Homme[37] vient protéger le "droit au respect de la vie privée et familiale" (art.8), sans que la notion de vie privée soit toutefois encore clairement définie. Puis en 1970 l'Allemagne, suivie en 1978 par la France, adoptent une loi de protection des données à caractère personnel[38]. La loi française de 1978, dite loi Informatique et libertés assure la protection des fichiers et institue une CNIL (Commission Nationale Informatique et Libertés). En 1981, la convention 108 est adoptée par le Conseil de l'Europe dans le but "de garantir (...) le respect [des] droits

---

[37] Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, [ci après CEDH], article 8 "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance"

[38] Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978

et [des] libertés fondamentales, et notamment [du] droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel[39]".

2 - La directive de 1995 et la consécration du droit à la protection des données à caractère personnel

En 1995 une étape importante est franchie avec l'adoption de la directive communautaire 95/46, qui devient le texte de référence en droit européen de la protection des données à caractère personnel. La directive, largement inspirée de la loi française de 1978, consacre le principe fondamental de protection des données à caractère personnel et met sur un pied d'égalité le secteur privé et le secteur public sur la question de la protection des données personnelles (alors qu'auparavant, la protection des données ne semblait essentielle, dans les textes, que par rapport à l'État). Un autre des apports de cette directive est qu'elle met au centre la notion neutre de "traitement de la donnée" : peu importe la technologie utilisée, dès lors que la donnée à caractère personnel subi un traitement, elle est protégée[40] ; cela a (entre autre) pour avantage que le droit peut ainsi s'adapter aux évolutions technologiques. Les principes fondamentaux de la protection des données à caractère personnel sont également établis et comprennent le principe de finalité (les données ne peuvent être recueillies et traitées que pour un usage déterminé et légitime), le principe de proportionnalité, le principe de pertinence des données, le principe de durée limitée de conservation des données (ou droit à l'oubli) ; le principe de sécurité et de confidentialité, le principe du respect du droit des personnes (information, accès et rectification, opposition)[41].

L'article 29 de la directive de 1995 a également institué un groupe de travail qui rassemble les représentants de chaque autorité indépendante de protection des données nationales, intitulé Groupe article 29, ou G29. La mission de ce groupe est de contribuer à l'élaboration des normes européennes, de rendre des avis sur le niveau de protection accordé aux données

---

39 Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, dite aussi *Convention 108*, Strasbourg, 28 janvier 1981, article premier de la convention 108

40 Caroline LE GOFFIC et autres, *Droit des activités numériques*, Précis Dalloz, juin 2014

41 Fil d'actualité du Service Informatique et libertés du CNRS, *Les 7 principes clés de la protection des données personnelles*, mise à jour le 18 janvier 2012, consultable sur http://www.cil.cnrs.fr/CIL/spip.php?article1390

personnelles en dehors de l'Union européenne et de conseiller la Commission sur les projets ayant une incidence sur la protection de la vie privée et des données personnelles[42]. L'indépendance des autorités de contrôle fait l'objet d'un examen strict par la Cour de Justice de l'Union Européenne[43]. Les autorités de contrôle jouent un rôle important dans la protection des données. En France par exemple, l'autorité indépendante appelée CNIL (Commission Nationale Informatique et Libertés) remplit trois fonctions. Une fonction d'information (elle veille à ce que les personnes aient connaissance de leurs droits, et conseille les Correspondants Informatiques et Libertés (CIL) qui font le lien entre les entreprises et la CNIL), une fonction de régulation (pour mettre en oeuvre un traitement de données il faut en demander au préalable l'autorisation à la CNIL, elle recense également les fichiers de traitement informatique de données nominatives), et enfin une fonction de contrôle et de sanction (la CNIL peut se rendre dans les locaux de l'entreprise pour effectuer des contrôles, et peut, depuis la loi "Hamon" du 17 mars 2014, effectuer des contrôles en ligne. Elle peut également prendre des sanctions sous la forme de décisions administratives susceptibles de recours devant le Conseil d'état). Les autorités de contrôle peuvent ainsi prononcer des amendes dont le montant varie en fonction des pouvoirs qui leur sont conférés et de la politique de l'agence. Ainsi la CNIL française a plutôt une réputation de clémence : depuis sa création elle a seulement infligé 520 400 euros d'amendes, alors que pour la seule année 2008 l'autorité de contrôle espagnole a puni à hauteur de 22,6 millions d'euros les entreprises qui ne respectaient pas les termes de la directive[44].

La directive de 1995 a par ailleurs créé un Délégué à la Protection des Données[45], que les États sont libres d'introduire, ou non, dans leur système de protection. À l'occasion de la transposition de la directive en 2004, la France a ainsi créé le Correspondant Informatique et Libertés, afin de faire le relai entre l'entreprise et l'autorité de contrôle.

---

42 CNIL, *Le G29, groupe des "CNIL" européennes*, consultable sur http://www.cnil.fr/linstitution/international/g29, le G29 se réunit tous les deux mois environ à Bruxelles

43 Certains États, comme l'Allemagne, ont d'ailleurs déjà été condamné pour ne pas avoir mis en place des statuts qui garantissent la non ingérence de l'État dans le fonctionnement de l'autorité de contrôle, CJCE, *Commission des Communautés européennes / république fédérale d'Allemagne*, affaire C-518/0, 9 mars 2010

44 Ibid - Caroline LE GOFFIC et autres, *Droit des activités numériques*, Précis Dalloz, juin 2014 p. 774

45 Directive de 1995 sur la protection des données, article 18

En 2000 la Charte des droits fondamentaux de l'Union européenne reconnait dans son article 8 que "toute personne a droit à la protection des données personnelles la concernant[46]" : le droit à la protection des données à caractère personnel est reconnu comme un droit fondamental au sein de l'Union Européenne, autonome du droit à la protection de la vie privée de l'article 8 de la CESDH. Puis la directive 2002/58/CE vient compléter la directive de 1995 notamment sur la question des cookies[47] et des spams[48]. Le traité de Lisbonne modifie enfin le traité sur le fonctionnement de l'Union européenne en 2007 par l'ajout d'un article 16, qui consacre aussi le droit à la protection des données à caractère personnel comme un droit fondamental : "Toute personne a le droit à la protection de ses données personnelles[49]". De plus, en incorporant la Charte de l'Union Européenne, le traité donne à l'article 8 de la charte une force contraignante : désormais le principe de la protection des données personnelles devra être respecté par les agences, organes et institutions de l'Union, mais également par les États membres lorsqu'ils mettent en oeuvre le droit communautaire.

B - Le droit spécial de la protection des données à caractère personnel

En plus de ce cadre général, l'Union européenne s'est dotée de textes spéciaux qui aménagent la protection des données à caractère personnel. La directive "*Data Retention*"[50] exige ainsi la conservation de "données relatives au trafic et aux données de localisation (...)

---

46 Charte des droits fondamentaux de l'Union Européenne, 2010/c83/02, Titre II "Libertés" article 8 "Protection des données à caractère personnel", 7 décembre 2000

47 Le cookie est "une donnée que le site internet met dans votre navigateur, à charge pour l'ordinateur de le conserver. Il permet au site internet de connaître votre navigation et vos préférences au cours de votre utilisation". Source : European Commission, Information providers guide, *The EU internet handbook*, dernière mise à jour le 7 juin 2016, consultable sur http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

48 Directive 2002/58 du Parlement Européen et du Conseil concernant le traitement le traitement des donnée à caractère personnel et la protection de la vie privée dans le secteur des communications éléctroniques, réformée par la directive du 25 novembre 2009, article 13 et suivants, les spams étant définis comme des "communications non sollicitées", et des "communications éléctroniques non sollicitées à des fins publicitaires"

49 Traité sur le fonctionnement de l'Union Européenne, 2012/C 326/01, octobre 2012W, première partie : les principes article 16

50 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications éléctroniques accessibles au public ou de réseaux publics de communications, modifiant la directive 2002/58/CE.

ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur", cela à des fins de "recherche, de détection et de poursuite d'infractions graves" (art.1) ; la directive "Vie privée et communications éléctroniques" du 12 juillet 2002[51], qui concerne la protection de la vie privée dans le cadre de la fourniture de services de télécommunications et qui englobe tous les moyens de communications éléctroniques accessibles au public (réseaux internet ou téléphonie), protège également les personnes physiques lorsque leurs données servent de support aux activités de *cookies*, de *spams* et de récupération des données de connexion.
La donnée, lorsqu'elle présente certaines spécificités, peut également être davantage protégée : ainsi les données biométriques et les données dites sensibles[52], qui font apparaître directement ou indirectement les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, ou celles relatives à la santé, etc., et qui en principe ne peuvent être ni collectées ni traitées, relèvent d'un régime propre.

C - Le nouveau règlement européen

Pour assurer une protection plus effective des données tout en tenant compte des évolutions technologiques, la Commission Européenne décide en 2010 de réformer le droit de la protection des données à caractère personnel[53]. Deux ans plus tard, le 25 janvier 2012, le Parlement Européen soumet une proposition de règlement[54]. Le 4 mai 2016, le texte officiel du règlement est publié dans le Journal Officiel de l'Union Européenne, et entre en vigueur 20 jours après sa publication. Les États membres ont un délai de deux ans, jusqu'en 2018, pour assurer sa mise en oeuvre effective.

---

51 Directive 2002/58 du Parlement Européen et du Conseil concernant le traitement le traitement des donnée à caractère personnel et la protection de la vie privée dans le secteur des communications éléctroniques, réformée par la directive du 25 novembre 2009.

52 Fil d'actualité du Service Informatique et libertés du CNRS, *Qu'est-ce qu'une donnée sensible ?*, consultable sur http://www.cil.cnrs.fr/CIL/spip.php?rubrique300

53 Communication de la Commission Européenne au Parlement Européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions, *Une approche globale de la protection des données à caractère personnel dans l'Union Européenne*, 4 novembre 2010

54 Proposition de règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Bruxelles, 25 janvier 2012

Les trois objectifs poursuivis par le nouveau réglement européen[55] sont : le renforcement du droit des personnes, le renforcement du cadre institutionnel chargé de la protection des données, et la promotion de l'économie numérique et des données.

Sur la protection des personnes physiques, le règlement reprend et complète la directive de 1995 et prévoit :

- plus de transparence : droit à une notification en cas de violation des données personnelles (article 34), droit à des informations claires et facilement accessibles (article 12) ; droit à un accès facile aux données à caractère personnel qui concernent la personne physique (article 15) ;
- plus de pouvoirs accordés à la personne concernée : droit de transférer ses données d'un agent à un autre (droit à la portabilité de ses données, article 20) ; droit à la rectification, à l'effacement des données et à l'oubli (article 16 et 17) ; droit de s'opposer à l'utilisation de ses données lorsque l'utilisation est faite à des fins de profilage (article 21 et 22) ; obligation pour le responsable de traitement d'obtenir de la part de la personne concernée son consentement avant de traiter ses données personnelles (article 7) ;
- plus de sécurité par la promotion de l'utilisation de technologies d'amélioration de la confidentialité, comme la *privacy by design*[56] ou les mécanismes de pseudonymisation, de chiffrement, etc. (article 25 et 32).

Sur le renforcement du cadre institutionnel, le règlement met en place :

- une procédure simplifiée : la saisine tout d'abord, avec la possibilité pour les personnes ou les entreprises de saisir directement une autorité de protection des données ou une juridiction de proximité, mais aussi la mise en place d'un guichet unique pour les affaires transfrontalières, ce guichet étant rendu possible par la coopération des autorités nationales de protection des données ;

---

[55] 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

[56] *Privacy by design* est un terme qui renvoie à "la protection intégrée de la vie privée dès la conception. Le but de ce principe est d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, des pratiques internes et des infrastructures matérielle". Source : A. CAVOUKIAN, *Privacy by design*, 2009, disponible sur http://www.ipc.on.ca/images/Ressources/privacybydesign.pdf

- de nouvelles autorités : le règlement confirme l'obligation de créer une autorité de contrôle indépendante au niveau national dans chaque état (article 51 et suivants) ; il impose désormais aux entreprises, lorsqu'elles remplissent certaines conditions, de désigner un responsable indépendant sur le traitement des données, le délégué à la protection des données (article 37 et suivants) ; il met en place un comité européen de la protection des données, qui se composera des représentants des 28 autorités de contrôles indépendantes et remplacera l'actuel comité de l'article 29 de la directive de 1995 (article 68 et suivants) ;
- des sanctions plus importantes (chapitre VIII, notamment l'article 83) : jusqu'à 20 millions d'euros d'amende, ou jusqu'à 4% du chiffre d'affaires annuel mondial de l'entreprise.

En ce qui concerne la promotion de l'économie numérique le règlement prévoit (voir le Chapitre IV Responsable du traitement et sous-traitant, et les considérants, notamment 22 à 24) :
- une égalité au sein de l'UE : un seul ensemble de règles pour toute l'Union européenne ; une approche fondée sur les risques, c'est à dire que tous les responsables de traitement ont des obligations qui seront graduées selon le niveau de risque du traitement ;
- une égalité par rapport aux pays tiers : les conditions de concurrence sont égales entre les entreprises établies dans l'UE et celles établies hors de l'UE qui proposent des biens et de services à des personnes résidant dans l'UE ;
- la promotion du marché numérique par la mise en place de règles au profit des entreprises, notamment des PME, afin qu'elles puissent tirer profit de ce marché des données. Parmi les nouvelles règles adoptées, on peut noter la mise en place d'un formulaire d'enregistrement unique dans toute l'Union européenne afin d'alléger la charge que la protection des données personnelles répresente pour les entreprises.

II - Le droit de la protection des données à caractère personnel aux États-Unis

Il n'existe pas, aux États-Unis, de loi fédérale générale qui règlemente la collecte et l'utilisation des données personnelles. Au contraire, la protection des données à caractère personnel est régie par un ensemble de normes (issues du droit des contrats, de lois fédérales et étatiques ponctuelles, de lignes directrices des agences gouvernementales ou de grands groupes industriels, etc.) au pouvoir contraignant inégal. Mais une tendance apparaît : le droit

des contrats et les législations qui existent sur la protection des données à caractère personnel sont finalement peu efficaces (A), et la protection des données est en fait principalement assurée par une agence gouvernementale de protection des consommateurs, la FTC (B).

A - Le droit de la protection des données à caractère personnel

Que ce soit le droit des contrats ou de la responsabilité (a), ou les législations spécifiques de protection des données à caractère personnel (b), leur application se révèle en pratique limitée.

1 - Les fondements dits classiques : droit des contrats, droit de la responsabilité

Le droit des contrats est étonnamment peu utilisé en matière de protection des données à caractère personnel. Il y a là, selon les professeurs Solove et Hartzog, un véritable "*privacy exceptionalism*"[57], car les entreprises insèrent pourtant leurs politiques de protection de la vie privée et des données personnelles dans leurs conditions générales, conditions générales qui sont soumises au droit des contrats[58]. Ainsi, la doctrine du *promissory estoppel*[59] aurait pu être un mécanisme efficace pour garantir l'application des *privacy policies*[60], pourtant elle n'a été que très peu utilisée[61]. Le fondement du *Breach of contract*, c'est-à-dire de la violation du

---

[57] Daniel J. SOLOVE and Woodrow HARTZOG, *The FTC and the New Common Law of Privacy*, Rev. 583, 2014, ci après SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*. Sur le *privacy exceptionalism* : "A privacy policy . . . need not be set up like a contract. . . . [S]ince privacy policies typically are enforced against a site owner . . . **many sites . . . treat Privacy Statements as notices** to consumers making clear . . . **that it is not a contract**. Others incorporate privacy policies by reference in Terms of Service . . . ."

[58] US district court of Minnesota, 6 juin 2004, *Northwest Airlines Privacy Litigation*, No. Civ.04-126 (PAM/JSM), WL 1278459. Rejet de la demande consistant à alléguer que les engagements pris sur le site de l'entreprise de protection de la vie privée et des données, était un contrat unilatéral.

[59] Restatement (Second) of Contracts § 90(1) (1981). Le *promissory estoppel* permet d'agir contre celui qui s'était engagé mais qui a soit changé d'avis, soit agit, soit est resté inactif, et cela contrairement à la promesse qu'il avait donné.

[60] "Privacy policy in corporation's business refers to a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's personal data such as name, age, address, gender, email, etc." Source : Li YUANGXIANG, et autres, *Online Privacy Policy of the Thirty Dow Jones Corporations*, California State University San Bernardino USA, p. 65 - 89, 2012.

[61] US District Court of New Jersey, *Smith v. Trusted Universal Standards in Elec. Transactions, Inc*., No. 09- 4567 (RBK/KMW), 2011 WL 900096, at *10 n.10, 15 mars 2011. Le problème vient de la difficulté à prouver l'offre préjudiciable.

contrat pour non respect des engagements pris, n'a pas eu plus de succès[62] : dans la plupart des affaires, les Cours ont considéré que les *privacy policies* n'étaient pas des contrats[63] ou que les demandeurs n'avaient pas réussi à prouver le préjudice subi du fait de la violation des engagements pris par l'entreprise[64].

Le droit de la responsabilité n'est pas d'une plus grande utilité[65] : les différents *torts* invoqués sont la plupart du temps rejetés par les Cours, comme celui du *tort of appropriation*[66], invoqué sans succès contre la vente par une entreprise des données personnelles en sa possession[67] ; ou le *tort of public disclosure* du fait de la rédaction du texte[68].

---

[62] NY Supreme Court, *Daniels v. JP Morgan Chase Bank*, N.A., No. 22575/09, 2011 WL 4443599, at *7--*8, 22 Sept. 2001 (finding no breach of contract where bank released confidential documents in response to subpoena) et Northern District of California, *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864–65, 2011 (declining to dismiss contractual claim based on damages arising from breach of privacy policy)

[63] US District Court of Nevada, *Loeffler v. Ritz-Carlton Hotel Co*., No. 2:06-CV-0333-ECR-LRL, 2006 WL 1796008, at *2–*3, 28 juin 2006 ; et Ibid - US District Court of New Jersey, *Smith v. Trusted Universal Standards in Elec. Transactions, Inc*., No. 09-4567(RBK/KMW), 2010 WL 1799456, at *8–*10, 4 mai 2010 (“Some courts have held that general statements like ‘privacy policies’ do not suffice to form a contract because they are not sufficiently definite.”)

[64] Northern District of California, *LinkedIn User Privacy Litig*., 932 F. Supp. 2d 1089, 1094, 2013, (finding “not receiving the full benefit of the bargain” for premium membership based on breach of privacy “cannot be the ‘resulting damages’ of this alleged breach [of contract]”) ; et Northern District of California, *Rudgayzer v. Yahoo! Inc*., No. 5:12-CV-01399 EJD, 2012 WL 5471149, at *6 , 9 novembre 2012 (finding “[m]ere disclosure of such information in and of itself, without a showing of actual harm, is insufficient” to support a claim of breach of contract under California law

[65] SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*, “[A]s a basis for protecting privacy, tort privacy is a very limited remedy.”

[66] Restatement (2d) of Torts §652C, c'est le fait de s'approprier pour son propre usage ou bénéfice le nom ou l'apparence de quelqu'un d'autre.

[67] Court Appellate III, *Dwyer v American Express Co* (1995). Dans cet l'entreprise American Express avait vendu le nom du détenteur de la carte bancaire à un tiers et la cour d'Appel avait estimé que le nom du détenteur de la carte n'avait pas été affecté par cette opération, et donc n'avait pas retenu le *tort of appropriation* comme base légale. Voir aussi Ohio Court Appellate, *Shibley v. Time, Inc*., (1975) ce fondement est refusé, au sujet de la vente par le magazine à des entreprises de poste, des adresses de ses lecteurs.

[68] Restatement (2d) of Torts §652D. Il vient sanctionner la divulgation auprès d'un public d'informations privées, soit d'une façon offensante pour une personne raisonnable, soit dans un but non légitimé par l'information du public. Or en pratique, les entreprises ne dévoilent pas à un grand public des informations privées, ou si elles le font, l'information divulguée est rarement offensante.

2 - Les textes spéciaux du droit de la protection des données à caractère personnel

a - Au niveau fédéral

Il existe deux types de réglementations sur la collecte et l'utilisation des données personnelles. D'une part les réglementations selon la nature de la donnée personnelle : le droit américain, comme le droit européen, vient faire la distinction entre les données sensibles (santé, finance...) et celles qui ne le sont pas, pour mieux protéger ces premières. Ainsi, à titre d'exemple, on peut citer le *Health Insurance Portability and Accountability Act* (HIPAA Act)[69], qui protègent certaines données de santé ; le *Children's Online Protection Privacy Act* (*COPPA*)[70] qui s'applique à la collecte en ligne d'informations sur des enfants ; et le *Financial Services Modernization Act*[71] sur la collecte, l'utilisation et la diffusion des informations financières et qui s'applique aussi bien aux institutions financières qu'à toutes les activités qui fournissent des services de cette nature. D'autre part, les réglementations selon la fonction de la donnée : sont visées ici les activités qui exploitent les données personnelles, par exemple à des fins de télé marketing. Il existe ainsi le *Controlling the Assault of Non-Solicited Pornography and Marketing Act*[72] et le *Telephone Consumer Protection Act*[73] qui régulent la collecte et l'utilisation, respectivement, des adresses e-mails et des numéros de téléphone.

b - au niveau des États

Chaque État a développé une législation en matière de protection des données à caractère personnel et le mouvement de régulation au niveau étatique va croissant. Certaines

---

[69] *Health Insurance Portability and Accountability Act* (*HIPAA* Act), 1996. Il s'applique aux professionnels du secteur et plus largement à toutes les entités (institution, professions...) qui entreraient en contact avec les données visées dans le texte. Plusieurs standards s'appliquent comme le *security standard for the protection of electronic protected health information* (*HIPPA Security Rule* 45 C.F.R. §160 à 164) ; le *standard for privacy of individually identifiable health information (HIPPA Privacy Rule* 45 C.F.R. §160 à 164) ; le *standard for electronic transactions* (*HIPPA Transaction Rule* 45 C.F.R. §160 à 162).

[70] Children's Online Privacy Protection Act, 15 U.S.C, §6501-6506, 15 octobre 1998

[71] Financial Services Modernization Act, 1999

[72] *CAN-SPAM Act*, 2003, 15 U.S.C §7701 à 7713 et 18 U.S.C §1037

[73] *Telephone consumer protection Act,* 47 U.S.C § 227 et suivants

lois fédérales prévalent sur les lois étatiques, comme celle qui portent sur la collecte et l'utilisation des adresses e-mails, d'autres doivent s'appliquer au même titre que la loi de l'État. L'État le plus actif en matière de protection des données à caractère personnel est la Californie, au point que pour certains auteurs, les lois californiennes portant sur la protection de la vie privée et des données sont très proches des lois européennes[74]. La Californie est un des rares États à avoir créé un département dédié à la protection de la vie privée (*Office of Privacy protection*) et a également adopté plusieurs lois protectrices de la sécurité des données personnelles comme le *Security Breach Notification Law*[75], le *Shine The light law*[76] et le *Data Security Law*[77]. La plupart des États s'inspirent de l'exemple Californien, et se préoccupent de plus en plus de la prévention contre la violation des systèmes de sécurité. C'est le cas au Massachussetts, où la *Massachussetts Regulation*[78] prévoit à cet effet une liste de protocoles de sécurité (techniques, physiques et administratifs) que les entreprises concernées devront incorporer dans leur propre système de sécurité.

Mais il apparaît finalement que ces normes ne viennent jouer qu'un rôle subsidiaire en matière de protection des données à caractère personnel. C'est en fait le droit de la consommation qui est le plus sollicité sur cette question.

---

74 Ieuan JOLLY, *Data protection in United States : overview*, Practical Law, Multi-jurisdictionnal guide, 2014/15, p. 3

75 *Security Breach Notification Law,* 1386, California Civil code, §1798.82 et 1798.29, 2002. Il impose, à toutes les personnes physiques et morales qui détiennent ou ont donné une licence d'exploitation sur des données numériques incluant des données personnelles, de communiquer toute défaillance de leur système de sécurité aux résidents californiens principaux intéressés, c'est à dire à ceux dont les données non cryptées ont été acquises par des personnes non autorisées.

76 *Shine The light law*, Cal. civil code §1798.83 à 1798.84, 2003. La loi exige des entreprises, lorsqu'elles ont partagé avec un tiers des données à caractère personnel en leur possession, qu'elles révèlent les informations pertinentes sur ce tiers au consommateur concerné.

77 *Data Security Law*, Cal. Civil code §1798.81.5. La loi impose aux entreprises la mise en place d'un système de sécurité afin de protéger les données personnelles contre leur destruction, leur utilisation, leur modification, leur divulgation, et d'assurer leur accès aux seules personnes autorisées.

78 *Massachussetts Regulation*, 201 CMR 17.00

B - Le coeur de la protection des données à caractère personnel : le FTC Act et le travail de son Agence

Mentionner la protection des données personnelles sans parler de la loi fédérale sur la protection des consommateurs, le *Federal Trade Commission Act* (*FTC Act*), et des mesures prises par l'organisme chargé de son application - l'Agence fédérale pour la protection de la concurrence et des consommateurs (la FTC, aussi appelée la Commission), agence gouvernementale indépendante créée avec l'adoption du *FTC Act* - revient à faire l'impasse sur le droit de la protection des données à caractère personnel aux États-Unis. Pour certains auteurs, c'est en effet grâce à cette agence, et à son travail, que les États-Unis et l'Union européenne ont des systèmes de protection, en pratique, très proches[79].

Le *FTC Act*, adopté en 1914, est d'abord une loi de protection de la concurrence, au champ d'application très large, puisqu'elle s'applique à toutes les entreprises et individus qui ont une activité commerciale sur le sol américain, à l'exception de certaines activités de transport, de finance et de télécommunication. La FTC est l'agence chargée de l'application du *FTC Act* et des autres textes qui sont de son ressort : elle peut prononcer des amendes, conclure des accords, agir en justice contre une entreprise, et dispose de larges pouvoirs d'investigation pour fonder sa plainte[80]. Selon le *FTC Act* "la commission peut engager toute enquête qu'elle jugera nécessaire sur tout le territoire des États-Unis" et peut "rassembler et compiler les informations, mais aussi enquêter sur l'organisation, le fonctionnement, la conduite, les pratiques, de toute personne, société, association, qui affectent le commerce (...)" [81]. À ce titre, la FTC peut émettre des *Orders to File Special Reports*, c'est à dire obliger l'entreprise à lui fournir certaines informations[82]. En décembre 2012 la FTC a ainsi émis des *Orders to File Special Reports* envers neufs *data brokers*, des entreprises qui "collectent les données

---

79 Winston J. MAXWELL et Christopher WOLF, *Protection des données personnelles : États-Unis et Europe convergent sur tout, ou presque*, Éditions multimédia économie numérique et nouveaux médias, édition juridique, numéro 55, avril 2012

80 FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, July 2008, consultable sur http:// www.ftc.gov/about-ftc/what-we-do/enforcement-authority

81 104. 15 U.S.C. § 43

82 15 U.S.C § 46(b) (Federal Trade Commission Act)

personnelles, les organisent et les compilent afin de les vendre à un tiers"[83] pour obtenir diverses informations sur leurs modes de collecte et de diffusion de leurs *privacy policies*[84]. Si l'Agence émet une plainte, l'entreprise peut la contester devant un juge ou choisir de conclure un accord avec la FTC[85]. Devant un juge, la FTC peut demander la condamnation à une réparation équitable, *equitable remedy*, sur le fondement de la section 13(b) du FTC Act[86], ou à des amendes pour non respect des accords passés avec lui, s'il y a eu accord au préalable[87].
De plus, la FTC est une autorité administrative et à ce titre elle peut adopter des règlementations (comme en matière de protection des consommateurs).

En quelques années la FTC est devenu l'autorité de référence en matière de protection des données à caractère personnel. Plusieurs étapes ont marqué l'affirmation de l'Agence, les

---

83 Jonathan A OBAR, *Big Data and The Phantom Public : Walter Lippmann and the fallacy of data privacy self-management*, Big Data and Society, July-December 2015. "Data brokers, (also referred to as data aggregators, information brokers or data vendors), collect information about individuals, then organize and package that information for the purpose of selling data to another party".

84 Hunton & Williams, *FTC Requests Informations About Data Brokerage Companies' Collection and Use of Personal Data*, Privacy and Information security Law Blog, décembre 2012, consultable sur https://www.huntonprivacyblog.com/2012/12/19/ftc-requests-information-about-data-brokerage-companies-collection-and-use-of-personal-data/. Parmi les questions posées il y avait : quels sont les produits ou services de l'entreprise qui impliquent des données personnelles ; comment est-ce que l'entreprise les collecte ; quand et comment les entreprises obtiennent le consentement des consommateurs avant d'obtenir, de collecter, de générer, de déduire, de divulguer ou de stocker des informations personnelles sur eux, etc.

85 Ibid - FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, July 2008

86 Ibid - A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC (July 2008). Passage explicatif de la Section 13(b) : FTC Act authorizes the Commission to seek preliminary and permanent injunctions . . . . **In the early and mid-1980s, . . . the Commission argued that** the statutory reference to "**permanent injunction" entitled the Commission to** obtain an order not only permanently barring deceptive practices, but **also imposing various kinds of monetary equitable relief** (i.e., restitution and rescission of contracts) to remedy past violations. . . . The **courts have uniformly accepted the Commission's construction of Section 13(b)**, with the result that **most consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication**.

87 Northern District of California, *United States v. Google Inc*., No. CV 12-04177 SI, at 7, 16 novembre 2012, (order), consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2012 / 11/121120googleorder.pdf (**approving $22.5 million civil penalty for violation of previous consent order**)

principales étant[88] la promotion par la FTC de la *self regulation* (autorégulation) des entreprises (1), l'élargissement de la juridiction de l'Agence (2), et enfin sa capacité à mettre en place ce que les professeurs Solove et Hartzog appelent la *FTC Common Law Privacy*[89] en matière de protection des données à caractère personnel (3).

1 - La promotion de l'autorégulation, "*self-regulatory approach*"

Privacy laws began to require privacy policies[90]. Le droit de la protection des données personnelles trouve sa source dans les politiques de protection de la vie privée et des données mises en place par les entreprises.

En 1973, le *HEW* (United States Department of Health Education and Welfare) a rédigé un rapport intitulé "*Records, Computers, and the Rights of Citizens*[91]" et remarquait déjà que les individus partageaient, et étaient de plus en amenés à partager, des informations personnelles les concernant. La rapport remarquait également que ces informations étaient collectées par des inconnus, à l'insu des internautes, et sans que ces derniers puissent entrer en contact avec ceux qui captaient leurs données. Dans la plupart des cas donc, l'internaute n'était pas au courant de l'appropriation de ses données, et même s'il l'était, il ne pouvait pas contester leur utilisation, ni *a fortiori* contrôler l'usage qui était fait de ses données. Le rapport a alors dégagé des principes, les *Fair Information Practises Principles* (FIPPs), proches des principes européens, afin d'assurer la protection de la vie privée et des données[92]. Il a ensuite

---

88 SOLOVE and HARTZOG, *The FTC and the New Common Law of Privacy*. Il faut également ajouter que selon ces professeurs, l'absence d'alternatives et la faiblesse des législations en matière de protection de la vie privée et des données personnelles, ont également joué un rôle important dans l'affirmation du FTC comme l'agence fédérale chargée de la protection des données personnelles aux États-Unis.

89 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

90 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

91 U.S Department of Health Education and Welfare, Records, Computers, and the Rights of Citizens , *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, DHEW Publication No.(OS) 73-94, July 1973

92 Les principes sont les suivants : transparency of data record systems, "notice / awareness" ; the right to prevent data from being used without consent, "choice / consent" ; the right to notice about data record systems, "access / participation" ; the right to correct or amend personal data, "integrity / Security" ; that data holders are responsible for the safekeeping of data and to ensure that data isn't misused, "enforcement / redress". Source : FTC, *Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security*, 1998, rapport au Congrès, consultation sur https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm

recommandé aux entreprises qui utilisent des données personnelles d'y souscrire. Le droit d'être informé (*notice*) et le droit de pouvoir choisir (*choice*) apparaissaient alors, et apparaissent encore aujourd'hui, comme les deux principes au coeur des FIPPs.

Les FIPPs sont rapidements devenus influents dans la formation des lois sur la protection de la vie privée et des données personnelles, et dans la formation des *privacy policies* des entreprises. Comme il n'y a pas de texte général sur la protection des données personnelles, la plupart des entreprises établissent leurs propres politiques de protection de la vie privée et des données selon une approche dite de *self-regulatory* (autorégulation). Elles vont alors pouvoir se servir des FIPPs comme base, en les introduisant dans leurs *privacy policies*. Généralement, la partie information, *notice*, est réalisé par l'inclusion des engagements de l'entreprise en matière de protection des données personnelles dans ses conditions générales, *terms of use* ; quant au *choice*, le consommateur se voit offrir un choix entre plusieurs options de collecte et d'utilisation de ses données[93]. Bien que non obligatoires, ces principes sont devenus si importants que le régime juridique des entreprises en matière de protection des données personnelles est souvent résumé par l'expression "*notice and choice regime*". Selon le professeur Allyson Haynes[94], "*en 1998, seuls 2% des sites internets avaient adopté des politiques de protection de la vie privée, et en 1999, 18 des 100 plus grands sites de commerce en ligne n'avaient [toujours] pas révélé leur politique en la matière. Mais à partir de 2001, tous les sites internets les plus populaires avaient adopté au moins virtuellement une politique de protection de la vie privée*".

La FTC a toujours encouragé ce mouvement de *self regulation.* Dans la continuité du rapport *The Information Infrastructure Task Force* émis par l'administration Clinton en 1993[95], la FTC dans son rapport au Congrès en 1999 estime "qu'une législation portant sur la protection

---

93 Robert GELLMAN, *Fair Information Practises : A Basic History*, décembre 2015, consultable sur http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf

94 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

95 L'administration Clinton, qui avait créé *The Information Infrastructure Task Force* en 1993 pour faire notamment des recherches sur la question de l'adoption d'une législation de protection des données, avait conclu après deux ans d'enquêtes que la meilleure option était une *self-regulatory approach*, c'est à dire d'avoir confiance dans les entreprises et les FIPPs. Source : SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

des données personnelles n'est pas appropriée pour le moment"[96], et les *privacy policies*, mises en place volontairement par les entreprises, constituaient alors un solide argument pour signifier à l'administration fédérale qu'une loi dans ce domaine n'était pas nécessaire. Par la suite, la FTC a eu l'occasion de réitérer son engagement en faveur de la *self regulation* des entreprises, comme en 2007 dans son rapport *Self-Regulatory Principles for Online Behavourial Advertising*[97].

En 1998, compétente depuis 1995 pour protéger la vie privée des consommateurs (voir *infra*), la FTC décide d'adopter et d'encourager les entreprises à incorporer les FIPPs dans leurs *privacy policies*[98]. La FTC se positionne donc en tant qu'autorité souple, à la fois en encourageant les entreprises à adopter les FIPPs dans une optique de *self regulation*, mais aussi en se portant par la suite garante auprès des consommateurs, des engagements qui ont été pris par les entreprises.

2 - L'adoption de nouvelles lois de protection des données dont l'application est confiée à la FTC

L'élargissement de la juridiction de la FTC va se faire progressivement. En 1938, la section 5 du *FTC Act* est amendée[99] pour permettre la prohibition des "actes ou pratiques déloyales et mensongères" (*unfair or deceptive acts or practises*). Cet amendement va rendre la FTC compétente pour protéger les consommateurs directement, et non plus par l'intermédiaire de la protection de la concurrence.
En 1970 la FTC devient l'autorité chargée d'appliquer le *Fair Credit Reporting Act*[100].

---

96 FTC, *Self-Regulation and Privacy Online : A Report to Congress*, 1999, "[T]he Commission believes that legislation to address online privacy is not appropriate at this time."

97 FTC Staff Report, *Self-Regulatory Principles for Online Behavourial Advertising*, 2007 "Staff supported self-regulation because it provides the necessary flexibility to address evolving online business models"

98 Ibid - FTC, *Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security*, 1998, rapport au Congrès, consultation sur https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm

99 Wheeler-Lea Amendment (1995)

100 *Fair Credit Reporting Act*, 15 U.S.C § 1681. Elle doit notamment veiller à ce que les agences d'évaluation des consommateurs respectent la vie privée de ces derniers.

À partir de 1995, à la demande du Congrès, la FTC devient compétente sur les questions mettant en jeu la vie privée des consommateurs[101]. Alors que le *FTC Act* n'était pas considéré comme une loi de protection de la vie privée ni *a fortiori* comme une loi de protection des données personnelles, cela change à partir de 1995. 1995 est ainsi considéré comme un moment charnière de l'histoire de la protection des données à caractère personnel aux États-Unis, car c'est à partir de ce moment que l'Agence va s'affirmer comme l'autorité chargée de la protection de la vie privée et des données personnelles des consommateurs.

En 1998, après avoir validé les FIPPs (voir *supra*), la FTC devient garante des engagements pris par les entreprises, au moins celles qui ont mis en place une *privacy policy*[102].

Puis la FTC devient compétente en 1998 pour le *Children's Online Protection Privacy Act* (*COPPA*), en 1999 pour le *Gramm-Leach-Billey-Act* (*GLBA*)[103]. La FTC était également compétente pour veiller au respect du *Safe Harbor*, accord entre les États Unis et l'Europe sur la question du transfert des données adopté en 2000. Plusieurs principes fondamentaux devaient être respectés (principe de finalité, de non conservation, etc.) par les entreprises concernées, qui étaient ensuite soumises à l'autorité de la FTC.

Toutes ces législations vont mettre en place un régime souple de *notice and choice*[104], régime déjà connu de la FTC. Cela explique pourquoi c'est à la FTC que ces nouvelles législations ont été confié. La FTC est donc désormais compétente depuis 1995 pour protéger les consommateurs des actes ou des pratiques *deceptive* ou *unfair* des entreprises (selon la Section 5 du *FTC Act*), depuis 1998 envers les entreprises qui ont adopté une *privacy policy*,

---

101 Ibid - FTC, *Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security*, 1998, rapport au Congrès, consultation sur https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm (“Since 1995, the Commission has been at the forefront of the public debate on online privacy.”). L'Agence va alors alors utiliser largement la section 5 du *FTC Act*, ainsi que les deux standards légaux qu'elle contient : "*deceptive*" et "*unfair*", pour s'assurer de la protection de la vie privée et des données personnelles.

102 Selon les professeurs Solove et Hartzog, le FTC ferait ainsi office de "pivot" en s'assurant de l'effectivité des textes adoptés par les entreprises, voir SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

103 15 U.S.C. § 6801 à 6809. Le congrès accorde à la FTC le pouvoir d'"établir les standards appropriés afin d'assurer la sécurité et la confidentialité des informations relatives aux consommateurs et détenues par les institutions financières qui tombent sous la juridiction du *GLBA*"

104 Exemple : le COPPA, 15 U.S.C. § 6801 à 6809, édicte un principe de protection de la vie privée (obliger l'entreprise à recueillir une autorisation parentale pour collecter et/ou utiliser les données sur leurs enfants) puis impose à l'entreprise relevant du COPPA de mettre en place une politique de protection de la vie privée sous la forme d'une notice

et enfin envers les entreprises qui tombent sous le coup d'une nouvelle loi spécialisée du ressort de l'Agence.

3 - L'établissement d'une "*FTC common law privacy*" par l'Agence

Pour les professeurs Solove et Hartzog, la FTC, même si elle n'est qu'une agence administrative, a mis en place une véritable *Common Law Privacy* grâce à une analyse rigoureuse et systèmatique des cas qui lui sont soumis[105].

Le *FTC Act*, les décisions (accords de réglements, sanctions, lignes directrices, etc.) et divers rapports de l'Agence, sont devenus en une vingtaine d'années le corps normatif de référence en matière de protection de la vie privée et des données personnelles. Même si la FTC n'a pas précisé la portée des différents documents qu'elle émet (impératifs ou non), ils sont considérés comme des lignes directrices[106] (ce flou a cependant été dénoncé par certains auteurs qui y voient une sorte de "roulette russe" : on ne sait pas ce qui s'applique à quoi et comment éviter une sanction[107]). En pratique, ces documents sont pris en compte par les entreprises. Par exemple, à la suite de la publication des principes sur le publicité, les *FTC's Behavioural Advertising Principles*, plusieurs entreprises, dont Yahoo![108], ont annoncé qu'elles mettraient en place un système d'option au profit des consommateurs, qui pourront alors choisir s'ils souhaitent recevoir de la publicité ciblée ou non.

Les documents émis par la FTC comprennent, d'une part, les accords, ou *consent order*[109]. Ils sont passés entre une entreprise et la FTC, et ils contiennent des principes généraux en

---

105 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

106 Pour les Professeurs Solove et Hartzog, ces documents doivent plutôt être considérés comme des dicta dans les opinions judiciaires, c'est-à-dire qu'ils n'ont pas la même force qu'un accord et indiquent comment la FTC interprète et interprètera la Section 5. La FTC est également libre de changer sa politique, ou peut être désavouée par les Cours de justice.

107 SOLOVE et HARTZOG, *The FTC and the New Common Law of* Privacy, référence à Stegmaier & Bartnick, *Psychics*, "calling lack of clarity “Russian Roulette” where companies essentially operate under strict liability framework"

108 Press Release, Yahoo!, *Yahoo! Announces new privacy choice for consumers*, août 2008, consultable sur http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=327212

109 Consent order : accord volontaire prévu par les lois fédérales ou étatiques, dont le but est de règler un litige entre deux ou plusieurs parties. Une agence fédérale peut être partie. Il a le même effet qu'une décision judiciaire et peut être produit devant une cour pour lui donner effet, si une partie ne respecte pas ses engagements. Source : http://definitions.uslegal.com/c/consent-order/

matière de protection des données à caractère personnel. Les entreprises vont donc pouvoir s'y référer lorsqu'elles établissent leurs *privacy policies*. Pour Chris Wolf, directeur de *Hogan Lovells's Privacy and Information Management Practice Group*, tous les accords mis en place par la FTC sont lus attentivement. Il explique ainsi que : "Premièrement, les violations alléguées par la FTC reflètent ce que l'Agence considère comme une violation de la Section 5 [du *FTC Act*] (ou une violation des autres législations dont elle a la charge). Une entreprise qui s'engage dans une pratique similaire ou semblable peut donc s'attendre à être elle-même soumise à une investigation de la FTC. Deuxièmement, les accords trouvés reflètent parfois ce que la FTC considère comme étant des "*bests practises*" : quand une politique de protection de la vie privée ou de sécurité est demandée, les objectifs poursuivis par la mise en place de ces politiques sont souvent instructifs pour les entreprises, et sont souvent des éléments à mettre en place chez elles à l'avenir"[110]. Les professeurs Solove et Hartzog estiment que plusieurs principes peuvent être dégagés des accords conclus avec la FTC, et forment le droit de la protection des données à caractère personnel. Ce sont : la prohibition des activités illégales (contraires à la législation), *"Prohibition of wrongful activities"* ; l'information des consommateurs et une réparation en cas de dommages, *"Consumer notification and remediation"* ; la suppression des données collectées ou leur usage parcimonieux, *"Deleting data or refraining from using it"* ; la mise en place de *privacy policies* et la notification de leur changement aux consommateurs, *"Making changes on privacy policies"* ; la mise en place d'un système de sécurisation des données cohérent, *"Establishing comprehensive programs"* et diverses obligations d'*accountability* (voir *infra*)[111].

Les documents émis par la FTC comprennent, d'autre part, des instruments de droit souple comme des rapports ainsi que des lignes directrices et des communiqués de presse. La FTC a par exemple émis un tes pour évaluer l'existence d'un acte ou d'une pratique déloyale : *The Commission's 1980 Unfairness Policy Statement*[112]. Il a ensuite été utilisé par l'Agence pour dégager de nouveaux principes, comme celui qui prohibe le changement rétroactif de sa

---

110 Email de Chris Wolf, Dir., Privacy & Info. Mgmt. Groupe Hogan Lovells, au Pr. Solove (Mar. 31, 2013, 11:21 AM), reproduit dans SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

111 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

112 Ibid- *FTC policy statement on unfairness*, décembre 1980

politique de protection des données personnelles de manière secrète (c'est-à-dire sans avertir les intéressés et leur proposer d'opter pour cette nouvelle politique[113]). La FTC identifie également des *bests practises* d'un secteur d'activité (elles émanent parfois dans un premier temps des groupes industriels eux-mêmes, du fait du mouvement de *self-regulatory* : par exemple les *bests practises* en matière de publicité ciblée ont été mises en place par plusieurs associations d'agences publicitaires[114]). La FTC a ainsi émis des rapports sur l'utilisation des technologies de reconnaissance faciale[115], sur la protection des données sur les applications mobiles[116], etc[117].

Pour conclure, selon Steven Hetcher à propos de l'économie numérique en 2000, "la FTC a créé un bien commun que les industries du numérique ont intérêt à promouvoir, à l'abri des législations adoptées par le Congrès. L'agence menace d'ailleurs d'encourager l'adoption d'une législation fédérale si les entreprises ne démontrent pas un plus grand respect pour la vie privée[118]". La FTC a donc transformé les *self-regulatory regimes* des entreprises en des régimes soumis à une autorité et susceptibles de sanctions, et a également mis en place un système de protection de la vie privée et des données personnelles très proche de celui qui existe au sein de l'Union Européenne.

---

113 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*, p.617

114 American Association of Advertising Agencies et autres, *Self-Regulatory Principles for Online Behavioral Advertising*, Juillet 2009, consultable sur http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf

115 FTC, *Facing Facts : Best Practices for Common Uses of Facial Recognition Technologies* (2012), consultable sur http://www.ftc.gov/sites/default/files/documents/ reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fac ialtechrpt.pdf

116 FTC, *Mobile Privacy Disclosures : Building Trust Through Transparency,* 2013, consultable sur http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-dis closures-building-trust-through-transparency-federal-trade-commission-staff-report/130201 mobileprivacyreport.pdf

117 Selon M. Vladeck, ancien directeur du bureau de la protection des consommateurs au sein de la FTC, il y a une grande différence entre les "*bests practises*" établies par la FTC et le test que la FTC a développé pour évaluer l'existence d'une pratique ou d'un acte déloyal. Lorsque la FTC établit un standard, elle est "attentive à la conduite de l'entreprise et regardera jusqu'à quel point elle se conforme aux standards qui s'appliquent à son secteur" mais lorsque la FTC détermine les "*bests practises*" elle fait "attention aux engagements actuels pris par toutes les parties du secteur et fera référence aux législations qu'elle est chargée d'appliquer", Source : Email de David Vladeck, Dir., Bureau of Consumer Prot., au Pr. Solove (Oct. 3, 2013, 1:12 PM), reproduit dans SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

118 Steven HETCHER, *The De Facto Federal Privacy Commission*, 19 J. Marshall J. Computer & Info. L. 109, 131 (2000)

Conclusion

Contrairement aux normes européennes qui fournissent un cadre législatif global, les États-Unis semblent adopter une approche plus ponctuelle. Toutefois, les normes mises en place par la FTC, même si elles sont l'œuvre de la pratique, montrent bien que les deux systèmes de protection ne sont pas opposés. On pourrait peut-être même parler d'influence européenne dans l'affirmation par l'agence de droits fondamentaux tels que le droit à l'information des consommateurs, ou encore le droit à la suppression des données après un certain délai. La nécessité d'instaurer un tel cadre, et donc la légitimité de la mission de l'Agence, est d'ailleurs reconnue par la Maison Blanche, qui justifie une réforme au motif qu'il manquerait "un exposé clair des principes fondamentaux en matière de protection de la vie privée et des données personnelles qui doivent s'appliquer aux entreprises"[119].

Dans un domaine du droit en construction et particulièrement soumis aux influences internationales tel que le droit de la protection des données à caractère personnel, il serait intéressant de s'intéresser à la perméabilité des systèmes. Deux principes américains, *l'accountability* (Titre 1) et *l'unfairness* ou principe de loyauté (Titre 2), sont ainsi considérés comme parmi les principes les plus influents en droit américain de la protection des données à caractère personnel. Or le nouveau règlement européen vient d'introduire le principe d'*accountability* en droit de la protection des données, et témoigne également de la volonté d'assurer une plus grande place au principe de loyauté. Après avoir étudié la signification de ces principes aux États-Unis, puis comment ils s'appliquent et quelles sont les limites qu'ils rencontrent, il sera intéressant de voir dans quelle mesure l'Union européenne intègre à son tour ces principes et quelles difficultées ils seront susceptibles de poser.

---

[119] White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, introduction "The current framework, however, lacks two elements: a clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models".

Titre I – Le principe d'*accountability* en droit de la protection des données à caractère personnel

L'*accountability* est une notion qui n'est pas, ou peu, connue en Europe, mais qui vient d'être introduite en droit européen par le nouveau règlement. Avant de voir comment elle est appliquée en droit de la protection des données à caractère personnel (Chapitre II), et les limites de ce principe (Chapitre III) il faut d'abord revenir sur la signification de ce concept (Chapitre I).

Chapitre 1 - L'*accountability* en droit de la protection des données à caractère personnel

Les États-Unis (II) et l'Europe (III) ont introduit de manière différente le concept d'*accountability* dans leur système de protection des données à caractère personnel. Mais une unité se dégage clairement entre les systèmes quand on regarde les objectifs qui sont poursuivis. Il faut donc commencer par étudier la signification du principe d'*accountability* (I).

I - Remarques préliminaires : qu'est-ce que l'*accountability ?*

Il convient tout d'abord de noter que l'*accountability* est une notion proprement américaine qui n'a pas d'équivalent au sein de l'Union Européenne[120].

Selon les professeurs Joannidès et Jaumier, l'*accountability* pourrait se définir de manière générale comme des "*mécanismes par lesquels des raisons pour sa conduite sont demandées et données, et considérée comme une philosophie du vivre ensemble bien particulière, dont le modèle de management nord-américain, britannique et australien constitue une traduction directe*[121]". Dans leurs travaux, ces professeurs reviennent sur l'émergence du principe d'*accountability*. Elle serait liée à la constitution de l'État américain : avec la Déclaration d'Indépendance, les colons américains rêvent d'un pays de liberté où la fortune est accessible

---

[120] Certains auteurs traduisent toutefois l'*accountability* par le concept de corégulation : Pratique par laquelle "une institution de l'état établit un cadre à l'intérieur duquel des acteurs privés essaient de définir les mesures de régulation destinées à rémedier à une défaillance du marché". Source : MAXWELL, *Protection des données à caractère personnel aux États Unis : convergences et divergences avec l'approche européenne*, Le cloud computing, l'informatique en nuage, société de législation comparée, 2013, p. 76

[121] Vassili JOANNIDÈS, Stéphane JAUMIER, *De la démocratie en Amérique du Nord à l'accountability à la française. Comprendre les origines sociopolitiques de l'accountability*, 2013

car elle ne dépendrait que des qualités individuelles. L'*accountability* serait alors "la capacité (*ability*) de rendre compte (*account*) du caractère juste de sa conduite"[122]. Cette responsabilité devant autrui est capitale car les nouveaux citoyens, égaux en droits, détiennent à la fois des droits et des devoirs. L'*accountability* serait alors un impératif de justification : l'individu ou l'organisation a l'obligation de justifier devant autrui ses actions, en sachant que la réciprocité des droits et devoirs implique une réciprocité de l'*accountability*.

Certaines distinctions de vocabulaire sont alors importantes à faire. Selon le professeur Bennett[123] l'*accountability* est davantage que la réactivité : même si la réactivité d'une entreprise envers ses consommateurs est un comportement encouragé et relevant de l'*accountability*, la notion n'implique pas à elle seule la responsabilité envers un tiers, contrairement à celle de l'*accountability*. L'*accountability* n'est pas non plus un synonyme de responsabilité : même si une entreprise a respecté toutes ses obligations au titre de l'*accountability*, elle n'en reste pas moins responsable si les individus ont subi un préjudice, par exemple du fait de la collecte ou l'utilisation de leurs données personnelles. Ces derniers pourront toujours obtenir réparation devant une cour de justice.

L'*accountability* est une notion apparue pour la première fois en droit de la protection des données à caractère personnel dans les lignes directrices de l'OCDE en 1980. L'OCDE considérait que le principe d'*accountability* était un principe à la base des législations sur la protection des données personnelles[124]. Puis le principe a été inclu dans le système de protection de la vie privée mis en place par l'APEC (coopération économique pour l'Asie-Pacifique réunissant les États-Unis, le Canada, le Mexique et le Japon)[125]. Le principe est également présent dans les Standards internationaux en matière de protection de la vie privée et des données personnelles adoptés à Madrid en 2009 au cours de la conférence

---

[122] Ibid - Vassili JOANNIDÈS, Stéphane JAUMIER, *De la démocratie en Amérique du Nord à l'accountability à la française. Comprendre les origines sociopolitiques de l'accountability*, 2013

[123] Colin J. BENNETT, *International Privacy Standards : Can Accountability be Adequate ?, Privacy Laws and Business International*, Vol. 106, 2010

[124] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980

[125] APEC, *Cross Boarder Privacy Rules* (*CBPR*), 2004

internationale annuelle des Commissaires à la protection des données et de la vie privée[126], et dans la norme ISO/IEC 29100 : 2011 *Privacy framework*. Le principe est enfin contenu dans le nouveau règlement européen sur la protection des données (voir *infra*)[127], et dans certains textes de lois aux États-Unis[128].

Le principe d'*accountability* en droit signifie que l'entreprise est amenée à se responsabiliser et à définir les mesures de mise en conformité qu'elle estime les plus adaptées à son activité, en contrepartie de quoi elle doit fournir, spontanément ou lorsque cela lui est demandé, que ce soit de la part des autorités de contrôle ou des personnes concernées, les éléments qui prouvent qu'elle respecte bien les normes posées. L'intérêt de cette dynamique est d'introduire une certaine souplesse en droit, en accordant à l'entreprise une relative liberté. Mais parallèlement le niveau de protection exigé n'en reste pas moins élevé et les autorités de contrôle vont alors jouer un rôle déterminant : à leur mission habituelle de contrôle vient s'ajouter une mission quasi permanente de vérification et d'accompagnement à la conformité. Ce standard a, de plus, vocation à compléter un système de protection, plutôt qu'à le remplacer[129].

Le principe consiste en pratique à mettre en place "des programmes de conformité à l'intérieur d'entreprises, et [à] superviser ces mesures par les autorités de l'État[130]". On peut donc y inclure les formes que peuvent prendre ces programmes de conformité, comme les Binding Corporate Rules et la certification. Il faut également s'intéresser aux codes de conduite, qui, bien souvent, sont un des premiers supports d'expression des obligations d'*accountability*. Ces mécanismes, sont en effet définis comme suivant :

---

126 ISO/IEC 29100, International standard, information technology - security techniques - privacy framework, 15 décembre 2011

127 Règlement européen sur la protection des données

128 Ibid - *Health Insurance Portability and Accountability Act,* 1996

129 Guillaume DESGENS-PASANAU, *La protection des données personnelles*, LexisNexis, Paris, 2015, p. 182

130 Winston J. MAXWELL, *La protection des données à caractère personnel aux Etats-Unis : convergences et divergences avec l'approche européenne*, Le Cloud Computing, L'informatique en nuage, Société de législation comparée, 2013

- Les code de conduite sont "un ensemble de recommandations pratiques ayant pour objet d'assurer un certain contrôle des comportements". L'adoption et l'application de ces codes renvoie directement à la notion de gouvernance d'entreprise, c'est-à-dire à l'ensemble des processus, lois, et réglementations qui influent sur la manière dont l'entreprise est gérée. Le rôle des codes de conduite est alors "d'encadrer la gestion de l'entreprise, en insufflant un peu d'éthique et de morale"[131]. Ces codes ce sont développés suite aux critiques adressées aux entreprises (soit qu'elles n'assumaient pas assez leurs responsabilité, soit qu'elles pouvaient en assumer davantage, voir sur ce point la RSE *infra*). Le code est animé par la même logique que l'*accountability*. Même s'ils peuvent ne pas comporter d'obligations de type *accountability*, ces codes, permettent aux entreprises de montrer qu'elles sont responsables. Ils contiennent bien souvent des obligations de mise en conformité avec la loi, que ce soit par la mise en place de procédures spécifiques en internes, la réalisation d'audits et de rapports, ou la désignation d'un délégué au sein de l'entreprise. Le processus d'adoption de ces codes, qui réunit les entreprises d'un même secteur et dont les codes doivent ensuite être approuvés par une autorité de contrôle, reflète également la dynamique de l'*accountability*. Les autorités européennes et américaines incitent d'ailleurs désormais les entreprises à adopter de tels codes, qui devront être conçus en partenariat avec elles (voir *infra*).

- Les règles d'entreprises contraignantes ou Binding Corporates Rules désignent, selon la CNIL française, "un code de conduite, qui définit la politique interne d'un groupe en matière de transferts de données personnelles hors de l'Union Européenne[132]". Les BCR sont dès l'origine des règles juridiquement contraignantes[133], qui s'appliquent à l'ensemble des entreprises composant le groupe, quelque soit le pays d'implantation des filiales, et qui doivent reprendre les principes de protection des données personnelles tels qu'imposés par la directive, et aujourd'hui le règlement (limitation des durées de conservation, limitation de la finalité, etc. Voir Article 47 point 2 du règlement). Elles apparaîssent comme un instrument

---

131 Peter WIRTZ, *Les meilleures pratiques de gouvernements d'entreprises*, La découverte, Repères, Paris, 2008

132 Site de la CNIL section "Les BCR qu'est ce que c'est ?" consultable sur http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/

133 Groupe de travail "Article 29" sur la protection des données, *Document de travail : transferts de données personnelles vers des pays tiers : application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprises contraignantes applicables aux transferts internationaux de données*, 11639/FR WP 74, 3 juin 2003, §3.1 a ; règlement 2016 art. 47 point 1 a

juridique qui permet le transfert de données personnelles vers un pays tiers à l'Union Européenne, lorsque ce pays n'offre pas un niveau de protection adéquat aux données[134], tout en garantissant un niveau de protection équivalent à celui qui existe en Europe. Mais les BCR ne sont pas seulement un instrument juridique de transfert, ils consistent également en de véritables programmes de conformité. En effet, "un ensemble de documentations et procédures doit être élaboré, lesquelles procédures constituent en tant que tel un programme de conformité[135]". Les programmes mis en place par les BCR sont spécifiques à chaque entreprise mais on peut dégager les caractéristiques suivantes : implication et soutien de la direction, politiques et procédures claires en interne (ex : mise en place de systèmes d'alerte efficaces), formation continue et sensibilisation(notamment pour les employés susceptibles d'être confrontés à des situations sensibles pour la protection des données), mécanismes de contrôle et d'évaluation crédibles (ex : des audits menés par des indépendants), cadre disciplinaire précis[136]. En Europe, les BCR adoptées par l'entreprise sont ensuite soumises à une procédure de vérification de leur conformité par les autorités européennes[137]. Une fois validées, les BCR deviennent opposables et peuvent fonder une action émanant à la fois des acteurs privés victimes de leur non respect, et des autorités de régulation. Les BCR sont également présents au sein de l'APEC, et prennent alors le nom de Cross Border Privacy Rules (CBPRs)[138].

- La certification constitue un programme de conformité car l'entreprise doit donner à un agent, privé ou public, la garantie qu'elle a instauré des pratiques respectueuses des données

---

134 Au sein de l'UE la circulation des données personnelles est libre depuis la directive de 1995 mais hors de l'UE, le transfert ne peut avoir lieu si le pays ne présente pas un niveau "adéquat" de protection (Art.25 point 1 directive 1995 ; Art. 45 point 1 règlement 2016). Or à ce jour peu de pays ont été reconnus comme assurant un niveau de protection adéquat (carte sur http://www.cnil.fr/linstitution/international/les-autorites-de-controle-dans-le-monde/), et les transferts ne peuvent donc se faire qu'en vertu de BCR, ou de clauses contractuelles prévoyant des garanties ou encore dans le cadre du Safe Harbor, aujourd'hui Privacy Shield.

135 Guillaume DESGENS-PASANAU et autres, *Informatique et Libertés, Enjeux, risques, solutions et outils de gestion*, Lamy Conformité février 2013

136 Christophe COLLARD et autres, *Risque juridique et conformité, Manager la compliance*, Lamy Conformité, novembre 2011, p.234 paragraphe "Existe-t-il un programme de conformité standard ?"

137 CNIL, *Les BCR règles internes d'entreprises*, consultable sur https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise, Juillet 2016

138 APEC, *CBPRs System*, consultable sur http://www.cbprs.org/

personnelles afin d'obtenir la certification. La certification encourage donc l'autorégulation des entreprises, et permet à l'entreprise d'identifier et de limiter les risques liés au traitement de la donnée. Les agences qui délivrent ces sceaux, parfois appelés "*Accountability Agent*" mettent en oeuvre le processus de la certification, c'est à dire qu'ils examinent si les pratiques et les *privacy policies* de l'entreprise qui demande la certification respectent les normes en place, et demandent, si cela est nécessaire, que l'entreprise intègre certaines garanties supplémentaires pour assurer sa conformité et obtenir la certification[139].

II - L'*accountability* en droit de la protection des données à caractère personnel aux États-Unis

Aux États-Unis, l'affirmation du principe d'*accountability* comme principe fondamental de la protection des données à caractère personnel a été l'œuvre de la pratique, et particulièrement de la FTC : l'Agence l'introduit systèmatiquement dans les accords qu'elle conclut avec les entreprises (A) et le valorise (B). Mais l'Agence n'est cependant plus aujourd'hui la seule institution à le mettre en avant (C).

A - L'*accountability* ou l'obligation, imposée par la FTC, de mettre en place des programmes de mise en conformité

La principale forme d'*accountability* existante est une forme d'*accountability a posteriori* menée par la FTC, grâce aux accords de transaction qu'elle conclut avec une entreprise[140]. Dans la grande majorité des cas[141], les entreprises préfèrent conclure un accord de transaction. Or si l'entreprise accepte l'accord transactionnel, elle accepte la fin des pratiques en cause mais également l'application de mesures contraignantes s'apparentant à des *Binding Corporates Rules* (BCR), c'est-à-dire à l'instauration de programmes de mise en conformité.

---

139 The Information Accountability Foundation, *Accountability Agents*, consultable sur http://informationaccountability.org/category/accountability-agents/

140 Comme cela a été vu en introduction, la FTC peut, après avoir émis une plainte, soit agir en justice soit conclure un accord avec l'entreprise concernée. *The FTC Procedures and Rules of Practice* permet en effet à quiconque soumis à une investigation de la part de la FTC, de proposer un accord dans la mesure où "le temps la nature de l'affaire et l'intérêt général le permettent, *The FTC Procedures and Rules of Practice*, 16 C.F.R. § 2.31

141 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*

Selon les professeurs Solove et Hartzog, ces mesures *d'accountability* sont récurrentes dans les accords conclus avec la FTC, et font parties du système de protection des données mis en place par l'Agence. Ils dégagent ainsi les principes suivants[142] :

- **Le contrôle par des organismes indépendants**, *"Assesments by Independent Professionals"*. Les entreprises mises en cause pour une pratique ou un acte déloyal ou mensonger, se voient souvent proposer une évaluation biennale effectuée par un professionel indépendant, pour s'assurer du respect de l'accord conclu avec la FTC[143]. Les comptes-rendus effectués par cette autorité indépendante doivent être tenus à la disposition de la FTC pendant vingt ans, et les entreprises qui ne respectent pas cette règle risquent de nouvelles amendes. Souvent l'organisme indépendant est un consultant comme *PricewaterhouseCoopers*, qui va envoyer une une équipe de spécialistes dans les entreprises concernées, afin de poser des questions aux employés sur la formation qu'ils ont reçus, examiner les procédures en places, et évaluer le système de sécurité. Ils vont également vérifier quelles sont les entreprises partenaires de l'entreprise évaluée qui ont accès aux données personnelles des consommateurs[144].

- **La tenue de dossiers et de rapports pour faciliter l'action de la FTC** *"Recordkeeping and Compliance Reports"* . Toutes les entreprises qui ont transigé avec la FTC se sont engagées à tenir des rapports et dossiers pour faciliter le contrôle de l'Agence, (on peut également noter que cette mesure est souvent prévue dans les décisions de justice contre une entreprise).[145]

---

142 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy,* p.614 à 619

143 Verne KOPYTOFF, *Privacy Audits Required of Internet Firms*, S.F. Chron, Mars 2013, http:// www.sfgate.com/technology/article/Privacy-audits-required-of- Internet-firms-4343921.php

144 Ibid - Verne KOPYTOFF, *Privacy Audits Required of Internet Firms*, 2013

145 FTC, *Aspen Way Enters., Inc*., FTC File No. 112 3151, No. C-4392, 25 Sept. 2012 (consent order), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120925 aspenwayagree.pdf (mandating recordkeeping for five years after improper activity)

- La notification à la FTC des modifications opérées au sein de l'entreprise qui pourraient affecter les obligations de cette dernière envers l'Agence *"Notification of material changes affecting compliance"*[146].

B - La valorisation du principe d'*accountability*

La FTC valorise ce principe dans ses lignes directrices (1) et dans celles qui sont adoptées par les autres institutions (2).

1 - Dans les lignes directrices

La FTC demande, par l'intermédiaire de ses lignes directrices, à certaines entreprises de mettre en place des dispositifs d'*accountability*. C'est le cas particulièrement des *data brokers*, entreprises qui "collectent les données personnelles, les organisent et les compilent afin de les vendre à un tiers"[147]. Dans son rapport *Data Brokers, A Call for Transparency and Accountability*[148], la FTC remarque que le processus de collecte des données des *data brokers* se fait à l'insu des consommateurs, et que leurs activités sont opaques. L'Agence incite donc les *data brokers* à se lancer dans la création d'un site internet centralisé, afin de s'identifier auprès des consommateurs, d'expliquer comment ils collectent leurs données personnelles et à qui ils les vendent, mais aussi quels sont les droits des consommateurs et les différents choix qui leurs sont offerts. L'Agence est consciente que les consommateurs n'iront probablement pas sur ce portail, mais justifie cette mesure par la promotion de l'*accountability* : ceux qui sont intéressés par cette question, quelque soit leur intérêt (hommes et femmes politiques, universitaires, avocats, juristes, mais aussi d'autres entreprises ou institutions liées à cette

---

146 FTC, *HTC Am. Inc*., FTC File No. 122 3049, No. C-4406, at 5, F.T.C. 2 juillet 2013 (consent order), available at http://www.ftc.gov/sites/ default/files/documents/cases/2013/07/130702htcdo.pdf

147 Ibid - Jonathan A OBAR, *Big Data and The Phantom Public : Walter Lippmann and the fallacy of data privacy self-management*, Big Data and Society, July-December 2015, "Data brokers [also referred to as data aggregators, information brokers or data vendors], collect information about individuals, then organize and package that information for the purpose of selling data to another party".

148 *FTC, Data Brokers, A Call for Transparency and Accountability,* mai 2014. Le FTC recommande dans le rapport l'adoption d'une loi spécialisée sur la question par le Congrès, à partir des propositions de régulations que l'Agence à émis. Cette position est d'ailleurs approuvée par la House of Representatives (Joe BARTON, *Rush welcome FTC report calling for greater transparency and accountability among Data Brokers*, U.S House of representatives documents, mai 2014).

question), pourront, sur ce portail, trouver des informations utiles et observer si les informations fournies sont suffisamment claires, précises, et exactes par rapport à leurs pratiques[149].

L'Agence soutient également les institutions qui valorisent ce principe.

2 - Dans les travaux menés par les autres institutions

La FTC soutient les *bests practises* identifiées par d'autres institutions qu'elle et qui mettent en place des obligations d'*accountability*. C'est le cas par exemple pour les *Self-Regulatory Principles for Online Behavioral Advertising*[150]*,* lignes directrices rédigées par plusieurs associations du secteur publicitaire, qui identifient l'*accountability* comme une *best practise*. Les lignes directrices appellent ainsi les entreprises dont les activités sont en lien avec la publicité à mettre en place les programmes de conformité suivant : *monitoring*[151]*, transparency and reporting*[152]*, compliance*[153]. Dans son rapport, "FTC Staff : *No Present Intention of Challenging Council of Better Business Bureaus' Accountability Program for Online Behavioral Advertising as Anticompetitive*", l'Agence annonce qu'elle ne remettra pas en question ces *bests practises* et considèrent que les mesures adoptées, notamment celles relèvant de l'*accountability*, vont dans le sens de la protection des consommateurs[154].

---

149 FTC*, Data Brokers, A Call for Transparency and Accountability,* mai 2014, p.53

150 Ibid - American Association of Advertising Agencies et autres, *Self-Regulatory Principles for Online Behavioral Advertising*, Juillet 2009, consultable sur http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf. Compilation de *bests practises* dans le secteur de la publicité ciblée, et rédigé par plusieurs associations d'entreprises de publicités (American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, etc.)

151 Programme de surveillance du respect de ces principes, de manière systématique et aléatoire. Ce processus de surveillance devra aussi permettre le dépôt de plainte, que ce soit de la part des consommateurs, d'autres entreprises ou du gouvernement.

152 Transparence et tenue de rapports afin s'assurer du respect des principes. Les rapports devront établir quel principe a été violé, s'il y a lieu, et les mesures prises pour y remédier.

153 C'est un obligation de conformité. Quand une entreprise ne se conforme pas aux principes, elle doit prendre les mesures nécessaires afin d'être de nouveau en conformité avec eux. Si elle ne le fait pas, elle risque de voir sa violation rendue publique par les *reports* du point deux, auprès des agences gouvernementales.

154 FTC Staff : *No Present Intention of Challenging Council of Better Business Bureaus' Accountability Program for Online Behavioral Advertising as Anticompetitive*, Federal Trade Commission Documents and Publications, Août 2011

C - Actualité de la notion

Devant l'importance que sont en train de prendre à la fois les données personnelles pour les entreprises, et la protection de leur vie privée pour les consommateurs, la FTC et la Maison Blanche ont réagi. Dans leurs deux rapports respectifs, le FTC[155] et la Maison Blanche[156], établissent de nouveaux principes, qui s'appuient sur les FIPPs, auxquels les entreprises devraient se référer. Les rapports comportent des idées innovantes, comme l'implantation de mécanismes de *privacy by design,* mais un de leurs principaux apports est la prise de conscience des faibles efforts de *self regulation*[157] effectués par les entreprises et la volonté de lutter contre cela en mettant en place des mécanismes d'*accountability* pour davantage les responsabiliser.

Les principes dégagés par les rapports qui mettent en place des obligations d'accountability

Codes de conduite

Afin d'assurer le respect des principes énoncés dans les rapports par les entreprises, la FTC et la Maison Blanche appellent les entreprises à mettre en place des "codes de conduite", désignés sous le nom de "*code of conduct*" ou "*self-regulatory codes*". Ces codes, rédigés selon une dynamique de *multi-stakeholder process*, c'est à dire en incluant une grande variété d'acteurs comme les entreprises du secteur, le *Department of Commerce* et la FTC, ont vocation à reprendre les principes énoncés par les rapports. La FTC sera ensuite l'autorité

---

155 Ibid - FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, mars 2012, consultable sur http://www.ftc.gov/sites/ default/files/ documents/reports/federal-trade-commission-report-protecting-consumer-p rivacy-era-rapid-change-recommendations/120326privacyreport.pdf

156 Ibid - White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, consultable sur https://www.whitehouse.gov/sites/default/files/privacy-final.pdf,

157 Ibid - FTC, *Protecting Consumer Privacy in an Era of Rapid Change : Recommendations for Businesses and Policymakers* (2012), p. 11 "*The Commission agrees that, to date, self-regulation has not gone far enough*"

compétente pour veiller à leur bonne application parmi les entreprises qui les auront adoptés[158].

Accountability

Le principe même est présent dans le rapport de la Maison Blanche[159] et devrait donc se retrouver dans la future législation concernant la protection des données personnelles, si elle est adoptée (selon l'article *FTC seeks laws to protect consumer privacy online*[160], une forte opposition des entreprises est attendue face à la nouvelle *privacy law*). Il est défini comme le fait pour les consommateurs d'avoir droit à ce que "leurs données soient traitées par des entreprises qui ont mis en place des mesures pour assurer le respect du *Consumer Privacy Bill of Rights*[161]". En pratique cela signifierait, pour les entreprises, l'obligation de mettre en place des audits internes de conformité, prouver qu'elles ont mis en place des mesures de protection et que ces mesures de protection sont régulièrement testées et adaptées à l'évolution de la technologie afin de garantir leur efficacité[162].

---

158 Ibid - White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, "The Administration's framework for consumer data privacy offers a path toward achieving these goals. It is based on the following key elements : (...) Enforceable codes of conduct (...) " ; "Such practices, when publicly and affirmatively adopted by companies subject to Federal Trade Commission jurisdiction, will be legally enforceable by the FTC"

159 Ibid - White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, p.21

160 Byron ACOHIDO, *FTC seeks laws to protect consumer privacy online*, Gannett News Service [McLean] 27 Mar 2012, consultable sur ProQuest Central Columbia

161 Ibid - White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, "Accountability : Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights"

162 Ibid - Winston J. MAXWELL et Christopher WOLF, *Protection des données personnelles : États-Unis et Europe convergent sur tout, ou presque*, Éditions multimédia économie numérique et nouveaux médias, édition juridique, numéro 55, avril 2012

III - L'intégration du principe d'*accountability* en droit européen

Le principe d'*accountability* est un principe qui a fait son apparition dans les textes dans les années 2010 (A), mais c'est le règlement européen sur la protection des données à caractère personnel qui le consacre comme en principe fondamental du droit de la protection des données à caractère personnel (B).

A - L'émergence du principe d'*accountability*

Le principe d'*accountability* est connu du droit européen dans la pratique : l'Union européenne connait depuis plusieurs années le mécanisme des BCR et de codes de conduite (voir *infra*).

Dans les textes, le principe d'*accountability* est connu des institutions européennes depuis les années 2010. Ainsi, selon le Groupe de travail Article 29, les éléments centraux de *l'accountability* sont identifiés comme étant : "l'obligation du responsable de traitement de mettre en place des mesures, qui (...) garantissent que les règles de la protection des données sont respectées dans le contexte de traitements ; et de disposer de documents démontrant aux personnes concernées et aux autorités de traitement quelles mesures ont été prises pour obtenir le respect des règles relatives à la protection des données[163]". On retrouve donc bien l'idée de la mise en place de programmes de conformité au sein de l'entreprise, et l'idée du comportement actif de l'entreprise afin de pouvoir prouver à tout instant le respect effectif e la réglementation. Le "Manuel de droit européen en matière de protection des données à caractère personnel" rédigé en 2014 identifie le principe d'*accountability* comme un des principes clés de la protection des données à caractère personnel en Europe[164]. On retrouve dans la définition du principe les critères de "pouvoir démontrer à tout moment la conformité avec les dispositions relatives à la protection des données" et de "mise en oeuvre active de

[163] Groupe de travail Article 29, *Avis 3/2010 sur le principe de responsabilité*, WP 173, Bruxelles, juillet 2010

[164] Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, Cour européenne des droits de l'homme, *Manuel de droit européen en matière de protection des données*, Luxembourg, avril 2014

mesures par les responsables de traitement pour promouvoir et garantir la protection des données[165]".

B - L'apport du règlement européen

Depuis 2016, le principe d'*accountability* est désormais inscrit dans la réglementation européenne, dès l'article 5 point 2 : "le responsable de traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté". L'objectif est, qu'en contrepartie de faveurs administratives accordées aux responsables de traitement et notamment aux entreprises, les obligations de ces dernières soient accrues. Le règlement présente le principe *d'accountability* comme un principe fondamental en matière de protection des données à caractère personnel : "Il y a lieu d'instaurer la responsabilité du responsable de traitement pour tout traitement de données à caractère personnel (...) Il importe, en particulier, que le responsable de traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures (...)[166]". Les responsables de traitement sont donc désormais tenus, et selon une démarche d'autorégulation, de mettre en place des procédures internes pour assurer un contrôle permanent de conformité. Le règlement contient ainsi les obligations d'*accountability* suivantes, qui sont soit obligatoires (1), soit obligatoires lorsque l'activité du responsable de traitement présente certains caractères (2), soit conseillées (3).

1 - Le mécanisme à mettre en place obligatoirement : tenir un registre sur son activité de responsable de traitement

La tenue de registre est prévue à l'article 30 du règlement. Chaque responsable de traitement ou sous-traitant est désormais obligé de tenir des registres sur ses activités, qui doivent contenir des informations telles que la finalité du traitement, les noms et coordonnées du responsable de traitement, une description des catégories de personnes et de données

---

165 Ibid - Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, Cour européenne des droits de l'homme, *Manuel de droit européen en matière de protection des données*, Luxembourg, avril 2014, p.83

166 Règlement européen sur la protection des données, considérant 74

concernées, et de les mettre à disposition de l'autorité de contrôle lorsque cela leur est demandé.

2 - Les mécanismes qui peuvent être obligatoires

Certaines obligations d'*accountability* sont imposées lorsque le traitement présente un risque (a) ou lorsque le traitement porte sur des données sensibles ou nécessite un suivi régulier (b).

a - Effectuer une analyse d'impact sur les données personnelles

Chaque responsable de traitement doit, selon sa propre initiative, effectuer une analyse d'impact sur la question de la protection des données personnelles[167]. Cette obligation est imposée seulement si le traitement qu'il envisage de mettre en oeuvre est susceptible d'engendrer un risque "élevé pour les droits et libertés des personnes physiques[168]". Cette analyse d'impact doit permettre d'identifier l'origine, la nature, la particularité et la gravité de ce risque, et le résultat doit être pris en compte pour déterminer les mesures à prendre pour assurer le respect le règlement. L'article précise quelles informations l'analyse doit comporter (comme la description de l'opération de traitement, ou ses finalités). Si le résultat de l'analyse montre que le risque est effectivement élevé, et qu'il ne peut être diminué ou alors que le coût de cette diminution serait trop important, le responsable de traitement doit consulter l'autorité de contrôle avant de mettre en oeuvre le traitement concerné.

b - La désignation d'auditeurs indépendants

L'article 37 impose aux responsables de traitement la désignation d'un délégué à la protection des données, dont les coordonnées sont transmises à l'autorité de contrôle lorsque

---

[167] Règlement européen sur la protection des données, article 35

[168] L'article 74 et le considérant 91 du règlement européen expliquent qu'un risque élevé peut consister en un traitement d'un volume considérable de données, affectant un nombre important de personnes, et qui met en oeuvre une nouvelle technologie ou technique ; ou encore en un traitement qui servirait à prendre des décisions par rapport à des personnes physiques déterminées, décisions qui les impacteraient, et dont les données personnelles ont été évaluées de façon systématique et approfondie au préalable ; ou encore un traitement qui mettrait en place une surveillance à grande échelle de zones accessibles au public ; etc.

ses activités sont de nature à exiger un suivi régulier, ou lorsque le traitement porte sur les données sensibles définies par le règlement. La désignation d'un délégué est seulement encouragée dans les autres cas. Le délégué peut être un membre du personnel du responsable de traitement, mais ne reçoit aucune instruction sur la façon d'exercer sa mission, et ne peut être ni relevé de ses fonctions ni pénalisé. Ses missions sont d'informer les responsables de traitement de leurs obligations en vertu du présent règlement, contrôler le respect du règlement, conseiller le responsable de traitement, coopérer avec l'autorité de contrôle, faire la liaison entre l'autorité de contrôle et le responsable de traitement. (Art.38 et 39).

3 - Les mécanismes encouragés

Dans tous les cas, le règlement encourage les entreprises à adopter des BCR si leur activité implique le transfert de données personnelles vers des pays tiers à l'Union européenne (a), de mettre en place des codes de conduite par secteur identifié (b) et d'adopter la certification (c).

a - L'adoption de règles d'entreprises contraignantes en cas de transfert de données vers un pays tiers à l'Union européenne

Les entreprises peuvent mettre en place des "règles d'entreprises contraignantes[169]" pour encadrer le transfert de leurs données vers des pays tiers à l'Union Européenne, tout en assurant un niveau de protection équivalent à celui qui existe en Europe. Cela est vivement encouragé par les autorités européennes lorsque les transferts se font avec un pays qui ne présente pas, selon la Commission Européenne, un "niveau adéquat de protection de des données à caractère personnel". Les deux aspects des BCR (voir *supra*) vont être repris par le règlement.

D'une part, les BCR prévoient le transfert de la donnée. Les BCR doivent être juridiquements contraignantes pour le groupe d'entreprises, conférer aux personnes concernées des droits opposables, et préciser plusieurs points comme l'application des principes généraux relatifs à la protection des données (limitation de la finalité, limitation de la conservation, qualité de la donnée, mesures pour garantir la sécurité des données, etc.), les droits des personnes concernés, les transferts concernés ainsi que les données susceptibles d'être transférées,

[169] Règlement européen sur la protection des données, article 47, considérant 108

l'acceptation de la responsabilité par le responsable de traitement qui viole ses engagements, etc.

D'autre part, l'adoption des BCR implique pour l'entreprise qu'elle mette en place des procédures de mise en conformité. Les BCR doivent ainsi prévoir plusieurs mécanimes : des mécanismes de contrôle qui garantissent le respect des BCR (audits sur la protection des données et méthodes pour adopter des mesures correctrices) ; des mécanismes pour "communiquer et consigner les modifications apportées aux règles[170]" ; des mécanismes pour coopérer avec l'autorité de contrôle ; des mécanismes pour assurer une formation appropriée au personnel.

Les BCR sont enfin soumises à l'autorité de contrôle pour validation.

b - L'adoption de codes de conduite

Les autorités européennes et les états membres continuent de promouvoir l'adoption, par les responsables de traitement, de codes de conduite pour chaque secteur identifié, et contenant les principes du présent règlement[171]. L'adoption de ces codes par des responsables de traitement extérieurs à l'Union européenne est également vivement incitée. Le contrôle du respect du code de conduite par le responsable de traitement est confié à un organisme indépendant, agréé par l'autorité de contrôle (l'organisme est agréé lorsqu'il a notamment rapporté la preuve de sa compétence en matière de droit des protection des données à caractère personnel, le preuve de son indépendance, et qu'il a établi des procédures pertinentes afin de vérifier que le responsable de traitement respecte bien le code de conduite). Le code de conduite est également soumis à l'autorité de contrôle pour approbation. Ces codes sont ensuite mis à disposition du public par le Comité.

c - Le développement de la certification

Les autorités européennes et les États membres incitent les responsables de traitement à mettre en place, ou à accepter le principe de la certification, des labels ou des marques en

---

[170] Règlement européen sur la protection des données, article 47, 2) k)

[171] Règlement européen sur la protection des données, article 40, considérant 98 ; directive de 1995 sur la protection des données, article 27

matière de protection des données à caractère personnel[172]. Cette dynamique est également connue depuis les années 1990 aux États-Unis (voir *infra*). La certification est délivrée par des autorités agréées par l'autorité de contrôle (qui présentent les mêmes garanties que les autorités chargées de veiller à la bonne application des codes de conduite), ou par l'autorité de contrôle, pour une durée de trois ans maximum. Elle est renouvellable dans les mêmes conditions. Toutefois, la procédure qui conduit à l'octroi de la certification n'est pas précisée. L'objectif est de permettre aux personnes concernées d'évaluer rapidement le niveau de protection offert à leurs données, mais aussi, s'ils sont acceptés par des pays tiers à l'Union Européenne, d'assurer aux personnes concernées que le niveau de protection accordé aux données personnelles est satisfaisant[173].

[172] Règlement européen sur la protection des données, articles 42 et 43

[173] Règlement européen sur la protection des données, article 41

Chapitre II - Exemples d'application du principe d'*accountability* en droit de la protection des données à caractère personnel

Aux États-Unis (I) et en Europe (II) le principe d'*accountability* ne se traduit pas de la même manière, mais reflète une même logique.

I - L'application du principe d'*accountability* aux États - Unis

Plusieurs exemples traduisent l'application pratique du principe d'*accountability*. Le choix s'est porté ici sur les accords transactionnels qui appliquent une forme d'*accountability* proche des BCR, (A) et sur la certification (B).

A - L'*accountability* par les accords transactionnels

La FTC, par la conclusion d'accords portant sur la protection des données personnelles avec des entreprises, rend effectif le système d'*accountability*. Les accords les plus notables, qui mettent à la charge de grandes entreprises des obligations d'*accountability*, concernent Google et Facebook en 2011[174].

L'*Electronic Privacy Information Center*, EPIC, une association de défense des consommateurs et droits civiques, avait porté plainte contre ces entreprises pour non respect de leurs *privacy policies*. La FTC a lancé une enquête, pour savoir si notamment, lors du lancement de Google Buzz (le réseau social de Google) l'entreprise Google avait violé ses engagements en matière de protection des données personnelles[175], et si Facebook avait violé son engagement de garder privées les données personnelles qu'elle avait en sa possession[176]. La FTC a ensuite assigné ces entreprises devant les tribunaux pour violation de la Section 5 du FTC Act. Les deux entreprises ont contesté ces accusations et ont préféré conclure un

---

174 Ibid - FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, mars 2012, p.ii

175 Press Release, *FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, octobre 2011, consultable sur https://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout

176 Press Release, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, novembre 2011, consultable sur https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

accord avec la FTC plutôt que d'aller en justice. Les accords conclus obligent ces entreprises à obtenir le consentement express de leurs consommateurs avant de changer certaines de leurs pratiques en matière de protection des données personnelles, mais surtout à adopter une solide politique de protection des données personnelles et de mettre en place des dispositifs d'*accountability*. Ces programmes de protection de la vie privée et des données incluent :

- l'obligation d'avoir des employés spécifiquement formés sur la question de la protection de la vie privée ;
- un programme d'identification des risques et de mise en place de gardes-fous contre les violations ;
- le recours à des contrôleurs indépendants afin de surveiller leurs efforts, sachant que les rapports biennaux de ces contrôleurs devront être tenus à disposition du FTC pour les prochains vingts ans.

Elles risquent 16 000 $ d'amendes par violation par jour[177].

B - Les programmes de délivrance des sceaux

Un autre exemple d'application du principe d'*accountability* est l'octroi de sceaux (*privacy seals*) par des entreprises, qui attestent ainsi que l'entreprise contrôlée a une politique de protection des données conformes aux exigences légales et à celles de la FTC. À partir des années 1990, des entreprises ont en effet commencé à délivrer ces sceaux ou *seals* pour certifier que leur partenaire sur le net respectaient bien les principes élémentaires de respect de la vie privée et des données personnelles, et leurs *privacy policies*[178]. Ces programmes fournissent un ensemble de lignes directrices, ainsi que des mécanismes à intégrer par l'entreprise. Ils doivent être obligatoirement adoptés par les entreprises qui souhaitent obtenir la certification[179]. Aujourd'hui il existe trois principaux organismes de délivrances de seaux :

---

177 Ibid - Verne KOPYTOFF, Privacy Audits Required of Internet Firms, S.F. Chron. (Mar. 10, 2013), http://www.sfgate.com/technology/article/Privacy-audits-required-of- Internet-firms-4343921.php

178 SOLOVE et HARTZOG, *The FTC and the new common law of privacy*

179 Nora J. RIFON, Robert LaROSE, Sejung Marina CHOI, *Your Privacy is Sealed : Effects of Web Privacy Seals on Trust and Personal Disclosures*, The journal of consumer affairs, volume 39 issue 2, sept 2005

1) "TRUSTe", 2) "BBBOnLine" et 3) "WebTrust[180]". Le premier, "TRUSTe", est le plus gros programme de délivrance de sceaux au monde. Fondé en 1997, il a certifié plus de 3500, dont LinkedIn et Nike. Cet organisme se conforme à la réglementation mise en place par la FTC. "TRUSTe" est également devenu en 2013 un "*Accountability Agent*", chargé de certifier les transferts de données qui ont lieu dans le cadre des Cross-Border Privacy Rules (CBPR) de l'APEC[181].

II - L'application du principe d'*accountability* en Europe

L'Europe connaît depuis quelques années le principe des *binding corporates rules* et des codes de conduite (A), et les entreprises européennes prévoient depuis peu d'inclure le principe d'*accountability* dans leur politique de protection des données (B).

A - Les BCR et les codes de conduite en Europe

Les BCR ont été reconnues en Europe par le G29 en 2003, dans le document de travail WP 74, comme une "solution convenant aux multinationales et autres groupes semblables, qui leur permet de (...) garantir un niveau adéquat de protection des informations à caractère personnel lors du transfert de données à l'extérieur de l'Union Européenne"[182], et encouragent depuis lors les entreprises à les adopter. En 2012 les BCR sont ouvertes aux sous-traitants[183]

---

180 "BBBOnLine" et "WebTrust" sont toutefois d'une relative importance. "BBBOnLine" a été lancé en mars 1999 et moins d'un an plus tard, il avait déjà certifié 450 sites. Il a cependant cessé d'accepter de nouvelles entreprises en 2007, Source David WRIGHT, Paul DE HERT, *Enforcing Privacy : Regulatory, Legal and Technological Approaches*, Springer, 2016. "WebTrust" est un programme de délivrance professionnel développé par l'American Institute of Certified Accountants (AICPA), qui avait certifié 28 sites en 2000, Source Li YUANGXIANG, Walter STEWART et autres, *Online Privacy Policy of the Thirty Dow Jones Corporations*, California State University San Bernardino USA, p. 65 - 89, 2012

181 Ces CBPR ont été adoptées par les membres de l'APEC pour assurer un transfert sécurisé et respectueux de la vie privée de données personnelles entre les pays membres, source : Site internet de l'organisme de certification TRUSTe : https://www.truste.com/business-products/apec-accountability/

182 Site internet de la CNIL : https://www.cnil.fr/sites/default/files/typo/document/FAQ_fr.pdf

183 Personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement. Source règlement européen sur la protection des données.

et non plus seulement aux responsables de traitement[184]. Les BCR ont connu une croissance forte entre 2010 et 2012 (+300%), et depuis 2012 le nombre d'entreprises qui adoptent des BCR est en augmentation constante (20% environ), sachant que pour l'année 2014, 56 entreprises ont adopté des BCR en Europe et 45 demandes de validation avaient été déposées auprès de l'autorité de contrôle[185]. En 2016, 84 entreprises en Europe avaient adopté des BCR[186]. Comme le montre la liste, la plupart des entreprises concernées sont des grandes entreprises qui ont une activité internationale, et notamment une activité avec les États-Unis : il paraît donc logique que ce soit elles qui aient, les premières, décidées de les adopter.

Les codes de conduite sont également connus en Europe. Ils sont adoptés dans le cadre de la responsabilité sociétale d'entreprise (RSE). La RSE désigne le "concept dans lequel les entreprises intègrent les préoccupations sociales, environnementales et économiques dans leurs activités et dans leurs interactions avec les parties prenantes sur une base volontaire[187]". Depuis le début des années 1980 plusieurs codes de conduite ont ainsi été rédigé pour différents secteurs, dont celui de la protection des données à caractère personnel. Ainsi, l'entreprise Daimler, constructeur automobile[188], ou encore le Groupe Generali en décembre 2012[189], entreprise d'assurance, ont adopté des codes de conduite pour assurer le respect de la vie privée et des données personnelles. Si le code du groupe Generali ne prévoit pas la mise en place de mécanimes d'*accountability*, le code de conduite de l'entreprise Daimler prévoit la désignation d'un délégué du groupe indépendant chargé de la protection des données, afin de

---

184 Ibid - Site internet de la CNIL : https://www.cnil.fr/sites/default/files/typo/document/FAQ_fr.pdf

185 Anne Barbier GOLIRO, *Les Règles Contraignantes d'Entreprises (BCR), Enjeux juridiques et pratiques*, Thèse professionnelle réalisée à l'Institut Supérieur d'Electronique de Paris, consultable sur http://www.formationcontinue-isep.fr/images/stories/food/thesesIL/TPABG4

186 European Commission, *List of companies for which the EU BCR cooperation is closed*, consultation juillet 2016 sur http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

187 Commission européenne, *Promouvoir un cadre européen pour la responsabilité sociale des entreprises,* Livret vert, juin 2001

188 Groupe Daimler, *Protection des données et de la vie privée, le Code de conduite Daimler*, consultable sur www.mercedesbenz.ma/.../CodeOfConduct.../Code_of_Conduct_franz_2007. pdf

189 Groupe Gennerali, *Code de conduite*, approuvé le 14 décembre 2012, consultable sur http://institutionnel.generali.fr/sites/default/files/code_conduite_2014.pdf

veiller à ce que les entreprises du groupe aient bien mises en place les mesures nécessaires, en interne, pour assurer le respect de la législation en matière de protection des données.

B - Les entreprises européennes et le principe d'*accountability*

Le principe est également connu de certaines entreprises. Ainsi selon l'entreprise General Electric, les objectifs du principe d'*accountability* en matière de protection des données personnelles sont notamment : identifier les risques ; identifier les faiblesses ; renforcer les bonnes pratiques ; démontrer l'attention portée à la protection des données personnelles ; atténuer les effets d'une faille de sécurité ; prendre en compte le développement des technologies et de l'entreprise avant de lancer un nouveau produit. On retrouve donc les éléments essentiels de l'*accountability*. Dans son plan d'intervention, l'entreprise prévoit d'assurer le respect de ces principes par la mise en place d'un "Programme de Gestion de la Protection des données" en trois points : mettre en place une structure de gouvernance (nommer un "Chief Privacy Officer" responsable de la protection des données, mettre en place un réseau de "Privacy officers" adaptés à la taille de l'entreprise, former) ; mettre en place un programme de contrôles (inventaire des activités de traitement des données personnelles, rédaction de politiques et de procédures de protection des données, mise en place d'outils d'évaluation des risques, mise en place de gestion des incidents et des failles dans le système de sécurité) ; évaluer et réviser périodiquement le programme (gérer et mettre à jour l'inventaire des traitements, réviser les politiques et procédures périodiquement, réviser et modifier les formations périodiquements etc)[190].

[190] Christian PARDIEU, *Accountability & Data Protection, Données personnelles : Les impacts du futur règlement européen*, pour General Electric, AFDIT, consultable sur http://www.afdit.fr/media/pdf/20%20mars%202014/Accountability%20%20Data%20Protection%20Christian%20Pardieu%20GE%2020%2003%202014.pdf

Chapitre III - Les limites du principe d'*accountability*

Le principe d'*accountability* comporte toutefois plusieurs limites : d'une part il n'est pas toujours bien compris et donc bien appliqué (A), d'autre part les autorités de contrôle, qui jouent un rôle essentiel dans son application, ne disposent pas toujours des moyens nécessaires pour rendre le principe efficace (B).

I - La difficulté à délimiter le standard

En 1995 dans un rapport du Canadian Standards Association[191] le professeur Bennett effectue une distinction entre l'*accountability* politique, l'*accountability* procédurale et l'*accountability* pratique. La plupart des mécanismes de l'*accountability* se concentrent seulement sur *l'accountability* politique, c'est-à-dire qu'ils comparent les *privacy policies* ou les codes de conduite avec les normes existantes. La plupart des programmes chargés de délivrer des "sceaux", certifiant la conformité des acteurs aux standards de protection des données, fonctionnent comme cela[192]. Or des questions plus profondes sont liées à la procédure et à la pratique, et sont souvent oubliées. Par exemple est-ce que l'entreprise a mis un place un traitement des plaintes relatives aux données personnelles ? Est-ce qu'il existe un référent au sein de l'entreprise sur cette question ? Est-ce que les employés ont été sensibilisé et formés à la protection des données personnelles ? Est-ce qu'il existe des audits pour savoir si la politique de protection des données personnelles mise en place est efficace ? Peu d'entreprises et d'institutions pourtant se soumettent à un contrôle de leurs pratiques sauf si elles ont conclu un accord avec la FTC, or le principe l'*accountability* repose avant tout sur le bon vouloir des acteurs. Pour le professeur Bennett il est difficile de comprendre comment l'*accountability* peut réellement être efficace si les entreprises ne sont pas contrôlées sur de tels points.

---

191 Colin J. BENNETT, "*Implementing Privacy Codes of Practice*" (PLUS 8830), Canadian Standards Association, 1995

192 Chris CONNOLLY, *Trustmark Schemes Struggle to Protect Privacy*, pour Gallexia (consultant indépendant spécialisé dans la protection de la vie privée et des données personnelles, et le commerce éléctronique), 26 septembre 2008 consultable sur http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_strug gle_public.html

De plus, pour le professeur Bennett, les *data controller*[193] nationaux ne peuvent pas être les seuls organismes garants de la protection des données personnelles, car ils n'ont pas assez de moyens pour conduire toutes les investigations nécessaires. Ils devraient travailler avec différents corps, aux compétences différentes, et indépendants, comme des organismes de délivrance de sceaux, des organismes de médiation de résolutions alternatifs des conflits, des cabinets comptables etc, qui mettront également en place des mécanismes d'*accountability* entre eux et les entreprises. Il faut donc examiner maintenant la faiblesse des autorités de contrôles.

II - Les difficultées liées à la faiblesse des autorités de contrôle

Il apparaît qu'aux États-Unis la FTC est une agence au faible pouvoir contraignant. Cette faiblesse de la FTC est d'ailleurs connue des groupes de protection des consommateurs, qui ont félicité l'Agence pour avoir encouragé l'adoption d'une législation par le Congrès en matière de protection des données personnelles[194]. En Europe, la faiblesse des autorités de contrôle a également été dénoncé par l'Agence des droits fondamentaux de l'Union européenne dans son rapport "La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données[195]". Plusieurs faiblesses apparaissent : le peu de pouvoirs consenti aux autorités de contrôle (A), le peu de moyens dont elles disposent (B), et plus particulièrement en Europe, le fossé qui peut parfois exister entre la législation sur la protection des données et la pratique (C).

---

193 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Le *data controller* est défini comme une partie qui, conformément à la loi nationale, est compétente pour décider du contenu et de l'utilisation des données personnelles, peu importe que les données soient collectées, stockées, traitées ou diffusées par cette partie ou par un agent qui agit sous ses ordres, "data controller means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf".

194 Ibid - Acohido BYRON, *FTC seeks laws to protect consumer privacy online*, Gannett News Service [McLean] 27 Mars 2012, consultable sur ProQuest Central Columbia, Christopher Calabrese conseil pour l'American Civil Liberties Union : "The FTC is very clearly saying that they don't have authority to do all that they need to do to protect consumers"

195 Agence des droits fondamentaux de l'Union Européenne, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg : Office des publications de l'Union Européenne, 2010

A - Les pouvoirs limités accordés aux agences de contrôle, et la faiblesse des sanctions prononcées par ces autorités

1 - Au sein de l'Union européenne

Concernant la réparation en cas d'atteinte à ses données personnelles, l'Agence des droits fondamentaux remarque qu'elle est souvent difficile à obtenir à cause de la combinaison de plusieurs facteurs juridiques comme "la charge de la preuve, les difficultés liées à la quantification des dommages et un manque de soutien des autorités de contrôle qui mènent principalement des activités de promotion "souples" telles que l'enregistrement et la sensibilisation". Ainsi l'Agence des droits fondamentaux a pu remarquer qu'en Autriche, en Hongrie et en Pologne les autorités de contrôle ne pouvait pas faire appliquer leurs décisions pour exiger du sous traitant ou du responsable principal la fin de ses pratiques. En Allemagne et en Belgique les autorités de contrôle ne peuvent pas ordonner le verrouillage, l'effacement ou la destruction des données ni imposer une interdiction temporaire ou définitive de leur traitement. En France et au Royaume-Uni elles ne peuvent pas pénétrer dans des locaux où des données personnelles sont traitées, sans avoir obtenu au préalable un mandat de justice. Enfin dans plusieurs pays (comme en Autriche, en Hongrie, en Pologne, en France, au Royaume-Uni, en Irlande, en Grèce, en Slovénie, à Malte, en République tchèque), les autorités de contrôle sont consultées de façon aléatoire au cours du processus d'édiction de normes concernant la protection des données à caractère personnel ou des normes liées au respect de la vie privée et à la question des données.

Concernant les sanctions, l'Agence des droits fondamentaux remarque que les amendes ont un pouvoir dissuasif limité et/ou sont rarements imposées, ou même plus encore, que les états membres n'ont pas mis en place de procédures pour leur imposition (comme au Danemark, en Finlande, en Hongrie, en Lituanie, en Pologne, en Autriche, au Royaume-Uni).

2 - Aux États-Unis

Seules les cours de justice ont un fort pouvoir de coercition aux États-Unis, et non la FTC[196]. La FTC ne peut en effet pas condamner une entreprise à des dommages et intérêts sur le fondement de la Section 5 (la protection des consommateurs contre une pratique ou d'un acte déloyal ou mensonger)[197]. Or la plupart des litiges entre la FTC et une entreprise se règlent par un accord et non devant la justice, et l'accord se revèle de plus souvent peu contraignant : les entreprises n'ont donc pas à craindre du côté de la justice américaine et des lourdes sanctions qu'elle pourrait émettre. Elles n'ont donc pas non plus à craindre pour leur réputation car un procès signifierait la reconnaissance d'une pratique ou un d'acte déloyal ou mensonger, ce qui n'est pas le cas d'un accord[198].

De plus, la FTC ne prononce que rarement des sanctions : d'une part même si la FTC peut prononcer des amendes en pratique elle ne le fait que très peu lorsque la question concerne la violation du droit des données personnelles[199], et dans les cas où les entreprises doivent tout de même payer eu égard à la gravité de la violation, les entreprises qui trouvent un accord avec la FTC avant le jugement, paient moins que ce qu'elles auraient dû payer si elles étaient

---

196 Les Cours peuvent condamner les entreprises qui ne respectent pas la législation ou l'accord passé avec la FTC à des dommages et intérêts jusqu'à 16.000$ pour chaque violation, Press Release, *Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts*, FTC 23 décembre 2008, http://www.ftc.gov/opa/2008/12/civilpenalty. shtm (**announcing increases in civil penalties**). En plus de ces dommages et intérêts, une District court saisie pour faire appliquer l'accord peut aussi émettre des injonctions et condamner à d'autres formes de réparations (*equitable relief*), source : SOLOVE et HARTZOG, The FTC new privacy common law, citation de Stephanie W. Kanwit, Federal Trade Commission §12:1 (2013)

197 Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012)

198 Ibid - FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, July 2008, "If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review."

199 SOLOVE et HARTZOG, The FTC new privacy common law

allées devant le juge directement[200]. La faiblesse des amendes prononcées par la FTC s'explique par le fait qu'elles sont calculées en fonction du préjudice subi par les consommateurs, et non par rapport à la taille de l'entreprise[201]. Ainsi en 2012, dans une procédure qui mettait en cause Google pour avoir accédé frauduleusement au navigateur Safari de Apple, et pour avoir ensuite suivi les internautes dans leur navigation internet afin de leur proposer des publicités, la FTC a fait condamner l'entreprise à 22,5 millions de dollars d'amende, soit la plus lourde amende jamais prononcée pour violation de la vie privée. Mais comme un média l'a noté, "c'est une goutte d'eau car l'an passé Google a généré 37,9 milliards de chiffre d'affaires"[202]. D'autre part, dans la plupart des procédures judiciaires pour violation de la vie privée, la FTC ne demande pas une réparation monétaire seulement des mesures de réparation équitable du préjudice[203].

B - Le manque de ressources financières et de personnel

1 - Au sein de l'Union européenne

Le rapport de l'Agence des droits fondamentaux relève qu'en Autriche, en Bulgarie, en France, en Grèce, à Chypre, en Italie, en Lettonie, aux Pays-Bas, au Portugal, en Roumanie et

---

200 Comparaison entre, Middle District of Florida, *FTC v. Action Research Grp., Inc*., No. 6:07-cv-00227-Orl-22UAM, at 1, 5, 18 mars 2008, (stipulated order & settlement), consultable sur http://www. ftc.gov/sites/default/files/documents/cases/2008/05/080528fo.pdf (**entering $67,000 judgment against several codefendants who settled with FTC**) ; et Middle District of Florida, *FTC v. Action Research Grp., Inc*., No. 6:07-cv-227-ORL- 22GJK, at 1, 6, 18 mars 2008 (default judgment), consultable sur http://www.ftc. gov/sites/default/files/documents/cases/2008/05/080528judgmentwagner.pdf (**entering default judgment of $428,085 against codefendant, Wagner, in same action**)

201 US Northern District Court of California, United States' Response to Consumer Watchdog's Amicus Curiae Brief at 9, *United States v. Google Inc.*, No. 3:12-cv-04177-SI, 28 septembre 2012, consultable sur http://www.consumerwatchdog.org/resources/ftcresponse092812.pdf (arguing "Commission must examine a number of factors, including the benefit obtained by the alleged violator and the harm suffered by consumers" in determining appropriate civil penalty) ; US Court of Appeals for the 11th circuit, *United States v. Danube Carpet Mills, Inc*., 737 F.2d 988, 993, 1984 (indicating "injury to the public" as factor in determining penalty amount).

202 Gerry SMITH, *FTC: Google to Pay Record Fine over Safari Privacy Violation*, Huffington Post, Août 2012, consultable sur http://www.huffingtonpost.com/2012/08/09/ ftc-google-fine-safari-privacy-violation_n_1760281.html

203 Ibid - FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, July 2008. Cela explique qu'une cour peut émettre des injonctions et accorder une réparation équitable. + Voir note sur section 13 (b) réparation équitable FTC

en Slovaquie, les autorités de contrôle n'ont pas de ressources suffisantes, ni économiques ni humaines pour mener à bien leur mission. Or disposer des ressources nécessaires et d'un personnel qualifié est une condition essentielle pour garantir la protection effective des données à caractère personnel, mais est également un préalable à toute indépendance par rapport au gouvernement[204].

2 - Aux États-Unis

La FTC dans sa mission de prohibition des pratiques et des actes déloyaux et mensongers, est soumise à des contraintes d'ordres techniques. Le personnel et les budgets sont limités ce qui a pour conséquence que la FTC est souvent obligée de se fonder sur les plaintes de consommateurs, ou sur les travaux réalisés par la presse, ou encore sur des questionnaires, pour être au courant d'activités potentiellement illégales[205]. De plus, cette faiblesse de moyens est un véritable handicap lorsque la FTC doit examiner les rapports émis par les contrôleurs indépendants sur les activités de grosses entreprises comme Google ou Facebook, dans le cadre des accords qu'elle a passé avec ces dernières. Le risque est que la FTC se contente de les survoler, en effectuant un contrôle superficiel ou limité sur les points manifestement contraires aux engagements pris. Vu la puissance économique de ces entreprises, qui ont les moyens de financer une défense juridique efficace, on peut douter de la réelle efficacité de ces comptes-rendus. En pratique, la remise de comptes-rendus d'activités auprès de la FTC aux fins de contrôle risque donc de ne produire que des résultats très limités.

C - Les limites spécifiques aux autorités de contrôle européennes

Au sein de l'Union Européenne, l'Agence des droits fondamentaux relève que les autorités de contrôles ne sont souvent pas suffisamment indépendantes vis-à-vis du pouvoir exécutif (1),

---

204 Ibid - Agence des droits fondamentaux de l'Union Européenne, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg : Office des publications de l'Union Européenne, 2010, page 42

205 FTC, *Performance & Accountability Report Fiscal Year 2012*, at 6 (2012), consultable sur http:// www.ftc.gov/sites/default/files/documents/reports/federal-trade- commission-performance-and-accountability-report/2012parreport.pdf (noting "agency's workforce consists of over 1,100 civil service employees dedicated to addressing the major concerns of American consumers," 613 of whom are attorneys)

mais aussi qu'il peut parfois exister une importante différence entre la protection des données à caractère personnel dans les textes et celle qui existe en pratique (2).

1 - Le manque d'indépendance fonctionnelle

L'Agence des droits fondamentaux relève qu'au Royaume-Uni, en Estonie, en Lituanie, en Lettonie, en Irlande, les délégués chargés de s'assurer de la protection des données à caractère personnel sont nommées ou désignés par le gouvernement exclusivement, sans avis, contrôle ou approbation du législateur. Il existe donc un risque de subordination[206].

2 - La différence existant entre le droit de la protection des données et la pratique de ce droit

Selon l'Agence des droits fondamentaux il existe un véritable fossé entre le droit à la protection des données à caractère personnel en théorie et en pratique (même si cette Agence reconnaît qu'il est difficile d'évaluer le respect effecfif de la législation en raison d'un manque d'informations fiables et précises). De plus, l'Agence des droits fondamentaux dénonce l'absence de notions claires, ou l'absence d'interprétation commune, sur des concepts majeurs tels que le "traitement" ou le "fichier". Elle reconnaît que le groupe des G29 joue un rôle majeur pour établir une interprétation commune mais que le processus "dépend également de l'acceptation et de l'application de ces interprétation par les états membres". L'Agence des droits fondamentaux identifie enfin un problème majeur : "le non-respect de l'obligation fondamentale de s'enregistrer auprès de l'autorité en charge de la protection des données avant de s'engager dans des opérations de traitement des données". L'exemple donné est celui des caméras de surveillance en France, en Autriche, en Suède, en Bulgarie, en Lituanie, en

206 Ibid - Agence des droits fondamentaux de l'Union Européenne, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg : Office des publications de l'Union Européenne, 2010, page 42

République tchèque, où la grande majorité des caméras ne sont pas enregistrées en pratique et donc échappent au contrôle des autorités nationales[207].

Conclusion

L'Union Européenne a donc intégré dans son système de protection des données le principe d'*accountability*, en assimilant sa philosophie et ses outils et en l'inscrivant dans un cadre institutionnel fort. Toutefois, pour être effectif, il faut que le principe soit accepté par les entreprises qui en sont les premiers acteurs, qu'il soit bien compris dans toutes ses dimensions, que les autorités de contrôle disposent de pouvoirs importants et qu'elles travaillent, lorsque cela est nécessaire, avec d'autres acteurs de la protection des données. Sur ces points, le principe d'*accountability* en Europe risque de se heurter aux même difficultés qu'aux États-Unis.

L'*unfairness* est également un principe fondamental de la protection des donnés aux États-Unis, et il s'est développé comme un standard souple aux multiples applications, ce qui est particulièrement intéressant en droit de la protection des données car la frontière est souvent difficile à tracer entre un traitement de la donnée attentoire à la vie privée et un traitement respectueux de la vie privée. Là aussi l'Union Européenne dans son nouveau règlement européen témoigne d'une volonté d'assurer au principe de loyauté une plus grande place.

---

[207] Certaines des critiques de l'Agence ont toutefois été prises en compte dans le nouveau règlement européen. Si la directive de 1995 exigeait des autorités de contrôle qu'elles "exerçent en toute indépendance les missions dont elles sont investies" (article 28 paragraphe 1) elle ne précisait pas la nature de cette indépendance. Le nouveau règlement européen vient désormais dans son l'article 52 "Indépendance" préciser ce qui est attendu de l'autorité de contrôle : une indépendance à l'égard de "toute influence extérieure directe ou indirecte", l'interdiction pour le personnel de l'autorité de contrôle d'exercer, dans le même temps, un travail rémunéré incompatible avec ses fonctions, l'obligation pour chaque état de veiller à ce que l'autorité de contrôle dispose des moyens matériels financiers et humains pour mener à bien sa mission, et enfin qu'elle dispose d'un budget propre. L'indépendance d'une autorité pourra donc, sur ces critères, faire l'objet d'un contrôle par la Cour de Justice de l'Union Européenne.

Titre II – L'*Unfairness* ou la déloyauté en droit de la protection des données à caractère personnel

L'existence du principe de loyauté est régulièrement rappelée par les textes européens et américains de protection des données à caractère personnel. Ainsi on le retrouve mentionné dans les lignes directrices de l'OCDE[208], dans la Charte européenne des droits fondamentaux[209], dans la Directive Européenne relative aux données à caractère personnel[210], dans la Convention sur la protection des données à caractère personnel du Conseil de l'Europe[211], dans le *Federal Trade Commission Act* (Section 5)[212]. Il faut donc revenir sur la signification de ce principe (Chapitre I), voir comment il est appliqué (Chapitre II), puis quelles sont ses limites (Chapitre III).

Chapitre 1 Le principe de l'*unfairness* aux États-Unis, le principe de loyauté en Europe

Les États-Unis (I) et l'Europe (II) ont une approche différente de la notion de loyauté, elle est considérée d'un côté comme un rapport économique (la différence entre les bénéfices et les coûts d'un acte ou d'une pratique), et de l'autre comme un droit à l'information et un rapport de confiance.

I - L'*unfairness* aux États Unis

C'est grâce au travail de la FTC que le principe *d'unfairness* va devenir effectif (A), et il est aujourd'hui clairement délimité par le test mis en place par l'Agence (B).

---

208 OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractères personnels*, 2013, §7 "les données devront être obtenues par des moyens licites et loyaux"

209 *Charte européenne des droits fondamentaux*, 2000, article 8 "les données doivent être traitées loyalement"

210 *Directive 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*, 1995, article 6 "les données à caractère personnel doivent être traitées loyalement et licitement"

211 Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 1981, article 5 "les données à caractère personnel... Sont obtenues et traitées loyalement et licitement"

212 *Federal Trade Commission Act*, 1914, section 5 prohibits "unfair or deceptive acts or practises"

A - Historique de la notion

En 1938, le *FTC Act* est amendé[213] pour prohiber les "*unfair or deceptive acts or practises*" (pratiques déloyales et mensongères), en plus des "*unfair methods of competition*" (méthodes de concurrence déloyale), afin de protéger les consommateurs directement. Il revenait alors à la FTC, sous contrôle juridictionnel, de définir ce qu'était une pratique ou un acte déloyal[214]. Comme la Supreme Court le faisait remarquer en 1931, la prohibition de la déloyauté "*appartient à ce type de notions qui ne peuvent être précisement définies, mais dont le sens et l'application apparaîtront grâce à ce que cette cour appelle "le processus judiciaire graduel de l'inclusion et de l'exclusion*[215]"".

Cependant, avant 1964, la FTC ne distinguait pas les pratiques déloyales des pratiques mensongères. Cela change avec le *Cigarette Rule Statement of Basis and Purpose*[216] : la FTC met en place pour la première fois une grille de lecture, un test, pour déterminer si la pratique ou l'acte était "*unfair*" ou déloyal :
Est-ce que la pratique ou l'acte est contraire aux politiques publiques, c'est à dire à la *common law*, aux législations ou aux autre textes normatifs ? ;
Est ce que la pratique ou l'acte est immoral, contraire à l'éthique ou sans scrupule ? ;
Est ce que la pratique ou l'acte a causé un préjudice substantiel aux consommateurs ou aux concurrents ?
Une nouvelle théorie de la responsabilité était née.

De 1964 à 1972 le FTC a rarement appliqué ce test. Mais en 1972, la FTC est légitimée par la Supreme Court dans son arrêt *Sperry vs Hutchinson*[217]. Encouragée par la Cour, la FTC a

---

213 *Wheeler-Lee Amendment*, 1938

214 Supreme Court, *Sperry vs Hutchinson C...*, 405 U.S. 223, 244-45 n.5 (1972). La Cour a à plusieurs reprises affirmé que la définition de la déloyauté revenait en dernier lieu au pouvoir judiciaire.

215 Supreme Court, *FTC v Raladam Co*., 283 U.S 643, 648 (1931)

216 Statement of Basis and purpose, *Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking*, 29 Fed. Reg. 8324, 8355 (1964)

217 Supreme Court, *Sperry vs Hutchinson C...*, 405 U.S. 223, 244-45 n.5 (1972). La Cour a cité les critères établis par le *Cigarette Rule* pour évaluer l'*unfairness* et a approuvé la proposition de la FTC, elle voit également le FTC "comme une *Court of Equity*, qui considère que les valeurs vont au-delà de celles seulement consacrées dans les textes ou comprises dans l'esprit des lois antitrusts"

alors utilisé ce standard plus largement. Cependant les critères n'étaient pas assez clairement délimités, et donc sujets à de trop larges appréciations. Ainsi, les critères de conformité aux politiques publiques ne fournissaient pas une base assez indépendante d'appréciation de la loyauté[218], pas plus que les notions d'immoralité, de non conformité à l'éthique, ou de peu scrupuleux[219]. L'"acte ou la pratique contraire aux politiques publiques" a même posé particulièrement problème car il a permis de justifier des décisions originales et souvent mal accueillies : la FTC a par exemple essayé d'utiliser la notion de *unfairness* pour interdire toute publicité dirigée envers les enfants en justifiant cette interdiction par l'existence de politiques de protection de l'enfant, et au motif que cela était immoral, et contraire à l'éthique[220]. Les décisions de la FTC finirent par exaspérer. Les médias d'abord : le Washington Post dans son éditorial du 1er mars 1978 pointait du doigt la FTC comme la "Nounou Nationale[221]". Puis finalement le Congrès américain, qui refusa en 1980 de voter les fonds nécessaires au fonctionnement de la FTC empêchant ainsi l'agence de travailler pendant plusieurs jours, et et qui décida peu après de restreindre l'autorité de l'Agence[222].

Ainsi rappelée à l'ordre, la FTC se mit à retravailler sur la notion d'*unfairness* Les textes adoptés dans les années qui suivirent, *The Commission's 1980 Unfairness Policy Statement*[223], *The Commission's 1982 letters to Senators Packwood and Kasten*, puis leur codification en

---

218 FTC, *The Commission's 1982 letters to Senators Packwood and Kasten*, 5 mars 1982

219 Ibid - *FTC policy statement on unfairness*, décembre 1980

220 FTC Staff Report on television advertising to children, *Notice of Proposed Rulemaking on television advertising to children*, 1978. L'interdiction des publicité ciblée envers les enfants était une des trois propositions émises par le FTC, la deuxième étant de limiter l'interdiction à la publicité portant sur des produits sucrés les plus à même de causer des carries.

221 Washington Post, *The national Nanny*, éditorial, 1er mars 1978

222 *FTC Improvements Act*, Pub. L. No. 96-252, mai 1980. Le Congrès décida de restreindre l'autorité de la FTC, notamment en lui interdisant d'utiliser la notion d'*unfairness* pour limiter la publicité

223 Ibid - *FTC policy statement on unfairness*, décembre 1980

1994, ont alors introduit l'analyse coût-bénéfices comme test adéquat pour évaluer *l'unfairness*[224].

B - Le "*three-part test*"

Les critères, aussi appelés le *three-part test*, qui constituent une véritable ligne directrice et reflètent une approche économique du principe de loyauté, sont désormais :
Est ce que la pratique cause ou est susceptible de causer un préjudice substantiel ? (1)
Est ce qu'il existe des bénéfices qui viendraient contre-balancer le préjudice subi ? (2)
Est ce que le préjudice aurait pu être raisonnablement évité ? (3)

(1) La première étape consiste à déterminer si le préjudice est substantiel. Le préjudice peut être économique, il peut également consister en une menace pour la santé ou la sécurité du consommateur (préjudices qui ne sont pas matériels[225]). Le critère se veut objectif, c'est pourquoi la FTC considère que le préjudice doit être tangible et exclut donc le stress émotionnel[226]. Un préjudice substantiel peut être constitué par un préjudice important à un petit groupe de consommateur, ou par un préjudice moindre à un grand groupe de consommateurs[227]. Enfin, en comparaison avec les bénéfices, le préjudice doit demeurer

---

224 Le nouveau test a écarté les critères de la *Cigarette Rule* et prend désormais davantage en compte le consommateur afin de promouvoir son libre arbitre. Le 17 décembre 1980 à l'occasion de l'adoption de *The Commission's 1980 Unfairness Policy Statement*, puis dans *The Commission's 1982 letters to Senators Packwood and Kasten*, le FTC a d'ailleurs déclaré que l'agence se concentrerait désormais sur le préjudice injustifié subi par le consommateur, considéré comme le plus important des trois critères, et que les politiques publiques n'étaient pas une base assez neutre lorsqu'il s'agissait d'évaluer la loyauté d'une pratique ou d'un acte, même si dans *The FTC policy statement on unfairness*, la FTC permet qu'on prenne en considération une politique publique si elle est "si claire qu'elle suffira à déterminer entièrement la question de l'existence du préjudice subi par le consommateur, et donc que l'analyse de l'agence ne sera requise qu'incidemment"

225 Thimoty J. MURIS, *Cost of Completion or Diminution in Market Value : The relevance of subjective value*, 12 J. Legal Stud. 379 (1983).

226 Ibid - *FTC policy statement on unfairness*, décembre 1980 ; FTC Staff Report, *Dissenting Statement of Commissioner J. Thomas Rosch,* Octobre 2012, consultable sur https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fr_jtr_dissentingstmnt.pdf, p. 1 "... only where there is alleged tangible injury, not simply emotional impact and other more subjective types of harm"

227 Il existe cependant quelques exceptions, ainsi même si le préjudice est formé par l'agrégation de plusieurs petits préjudices, il ne sera pas considéré comme substantiel s'il vient d'une entreprise considéré comme petite, *The Commission's 1980 Unfairness Policy Statement* énonce les critères d'une petite entreprise

substantiel.

(2) La deuxième étape consiste à déterminer s'il existe des bénéfices, au profit des consommateurs ou du marché, qui viendraient contre-balancer le préjudice subi. La FTC va donc tenir une analyse coûts-bénéfices, c'est à dire qu'elle va mettre en relation les différents préjudices (préjudices subis par les consommateurs, mais aussi ceux subis par le marché et la société[228]), et les différents bénéfices provoqués par un acte ou une pratique, pour évaluer leur déloyauté. Cette approche coûts-bénéfices est la traduction de la "*Hand - formula*"[229], approche économique utilisé en droit de la responsabilité, ici en droit de la protection des données personnelles[230]. Selon cette approche, tous les préjudices ne sont pas pris en compte, seul l'est un niveau raisonnable de préjudices qui n'a pas pu être prévenu. La conséquence souhaitée est que le coût total du préjudice et le coût de la prévention seront alors minimisés.

(3) Enfin une pratique n'est pas déloyale si elle aurait pu être raisonnablement évitée. Cette notion est assez difficile à évaluer. *The unfairness Policy Statement* reconnait que la notion de "raisonnablement évitable" touche aux limites de l'action pour pratique déloyale. La FTC est donc claire : elle n'est pas là pour deviner ou dicter la conduite des consommateurs sur les choix qu'ils devraient faire mais est là pour "mettre fin à certaines pratiques des commerçants, qui créent de manière déraisonnable ou qui prennent avantage d'un obstacle au libre exercice du choix du consommateur dans sa prise de décisions[231]". Pour encadrer cette notion, la FTC vient la lier avec le niveau d'information reçu par le consommateur. L'Agence doit donc vérifier que les consommateurs étaient suffisamment

---

228 Dans *The unfairness Policy Statement*, le FTC prend l'exemple d'un vendeur qui n'est pas capable de fournir à son potentiel acheteur tous les détails techniques d'un produit. Le préjudice est que le consommateur a une capacité de choix amoindri ; l'avantage est que cela peut avoir pour conséquence une diminution du prix du bien. Dans ce dernier cas, le préjudice est considéré compensé.

229 Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p.210

230 Ibid - Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p.210. Selon la "Hand - formula", un agent devrait prévoir le coût d'une mesure en investissant un montant "B". Ce montant "B" est égal au montant du préjudice "L" multiplié par une probabilité "P". Quand l'agent calcule la probabilité "P", il prend en compte les mesures raisonables que peut prendre une victime pour éviter le préjudice.

231 Ibid - *FTC policy statement on unfairness*, décembre 1980

au courant et avaient suffisamment d'informations pour prendre une décision relative à leurs données personnelles. Toute collecte dissimulée pourra être regardée comme déloyale car le consommateur n'aura pas eu l'occasion de faire un choix. Cet encadrement évite ainsi à la FTC le risque de dicter des comportements : si les consommateurs pouvaient faire un autre choix mais ne l'ont pas fait, la FTC doit respecter ce choix[232].

À partir de 1980, la FTC a commencé à appliquer ce test aux préjudices substantiels causés aux consommateurs mais qui ne pouvaient pas obtenir réparation sur le fondement de l'acte ou de la pratique mensongère, *"deceptive acts or practises"*[233]. En 1984, la FTC a pour la première fois appliqué le *unfairness test* dans le domaine des crédits à la consommation[234]". Puis en 1986, le test est étendu au domaine contractuel par le *Orkin Case*[235]. Le Congrès autorisa finalement en 1994 la codification du test dans le *FTC Act*[236].

---

[232] Dans Howard BEALES, *The FTC's use of unfairness authority : its Rise, Fall, and Ressurection,* The marketing and public policy conference, Washington D.C, 30 mai 2003, le professeur prend l'exemple des fasts-food : on peut défendre l'argument selon lequel la nourriture de fast fond crée un dommage significatif qui n'est pas contre balancé par des bénéfices, et donc la conséquence devrait être son interdiction. Mais le concept de "raisonnablement évitable" tel que défini par *The unfairness Policy Statement* fait obstacle à cette interdiction : la FTC ne peut substituer sa grille de lecture aux choix effectués par des consommateurs informés

[233] *Deception Theory,* théorie du droit américain de la consommation : elle se fonde sur la section 5 du FTC Act (*unfair or deceptive acts or practises*), Il faut 3 éléments pour introduire une action sur ce fondement : un acte ou une pratique ou une omission susceptible d'entraîner l'erreur du consommateur ; que le consommateur ait agit normalement, de manière raisonnable par rapport au standard de conduite requis ; que la pratique ou l'acte ait été de nature à affecter le comportement du consommateur par rapport au bien ou service vendu. Contrairement à la théorie de *l'unfairness*, il n'y a pas ici de mise en balance des bénéfices et des préjudices.
Source : http://apps.americanbar.org/publicserv/

[234] *Credit Practises Rule*, 49 Fed. Reg. §7745 à 7776 (1984)

[235] U.S Courts of Appeals, 11th circuit, *Orkin Extermination Co. v FTC*, 849 F.2d 1354, (1988). Début de la procédure devant le FTC en 1986. En 1975 Orkin passe plusieurs contrat de consommation dont l'objet est la vente d'un service à vie contre les termites. Aucune clause du contrat ne prévoyait l'augmentation unilatérale de la redevance mais Orkin la décide unilatéralement. Meme si le coût supplémentaire ne s'élève qu'à 7$ par personnes, son entreprise en tirait plusieurs millions de bénéfices. Le FTC a considéré que la pratique avait causé un préjudice substantiel et inévitable aux consommateurs ou à la concurrence et a declaré la pratique déloyale. La cour approuve.

[236] 15 U.S.C §45. Le Congrès codifie également la partie sur le rôle limité des politiques publiques dans l'appréciation de la déloyauté de l'acte ou de la pratique

Cependant l'*unfairness* ou la déloyauté est un standard qui semble difficile à appliquer, même s'il a bien été délimité[237]. Toutefois cette notion paraît aujourd'hui prometteuse pour assurer la protection des données personnelles face au comportement de certaines entreprise, le standard *deceptive act or practises* ne pouvant être utile ici, car il implique que le site ait, par négligence ou volontairement, induit le consommateur en erreur. L'*unfairness* ne demande pas cela, et permettrait donc de réguler certains comportements qui, bien que ne violant aucune norme légale ou de comportement, portent en fait atteinte à la confidentialité des données[238].

II - Le principe de loyauté en Europe

Les textes européens font peser sur les responsables de traitement une obligation de collecte et de traitement loyal des données personnel collectées. Dans le nouveau règlement européen le principe de loyauté est prévu dès l'article 5 1) "Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée". Le principe de loyauté est donc un principe fondamental de la protection des données, et s'il se rapproche du principe de transparence (A), il s'en distingue à certains égards (B).

A - L'assimilation relative du principe de loyauté au principe de transparence

Le principe de loyauté est partiellement expliqué dans les considérants 39 et 60 du règlement européen sur la protection des données à caractère personnel, et ces considérants viennent clairement lier le principe de loyauté au principe de transparence. Ainsi, selon le considérant 39 "tout traitement des données devrait être licite et loyal. Le fait que des données (...) sont collectées, utilisées (...) devrait être transparent à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication

---

237 Ibid - FTC Staff Report, *Dissenting Statement of Commissioner J. Thomas Rosch,* Octobre 2012, consultable sur https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fr_jtr_dissentingstmnt.pdf, Opinion dissidente du commissaire Rosch qui mentionne l'engagement de la FTC auprès du Congrès d'utiliser parcimonieusement le standard de l'*Unfairness*

238 SOLOVE et HARTZOG, *The FTC and the New Common Law of Privacy*, dans leur article les professeurs Solove et Hartzog expliquent que la notion d'actes ou de pratiques *deceptive* est utilisée pour protéger la vie privée (règle la question des *privacy policies* incomplètes ; ou des promesses non tenues) mais c'est la notion de *unfair* qui est préférée pour protéger spécialement les données personnelles.

relatives au traitement de ces données (...) soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples [...]"[239] ; et selon le considérant 60, "le principe de traitement loyal et transparent exige que la personne concernée soit informée (...) le responsable de traitement devra fournir (...) toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées[240]".

Les considérants 39 et 60 suggèrent donc un lien fort entre transparence et traitement loyal, et plus particulièrement entre le niveau d'information fourni et le traitement loyal. Si les informations sont insuffisantes (que cela soit en valeur ou numériquement), le consommateur ne peut pas choisir de manière autonome de quelle façon il souhaite que ses données soient traitées. La loyauté signifierait donc la capacité de la personne concernée à exercer des choix relatifs à ses données de manière autonome, grâce aux informations qui lui ont été fournies. L'absence ou l'insuffisance d'information rendra par conséquent le traitement des données déloyal.

L'article 13 "Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée" vient ensuite lister les informations qui doivent avoir été fournies à l'intéressé pour qu'il puisse exercer son libre arbitre. L'article est divisé en trois points selon l'activité de l'entreprise ou de l'administration : si elle collecte, elle doit fournir à l'intéressé des informations en rapport avec cette activité (notamment l'identité et les coordonnées du responsable de traitement, les finalités du traitement, les destinataires ou catégories de destinataires des données, etc.) ; à partir du moment où elle détient ces données, elle doit indiquer la durée de leur conservation, l'existence du droit d'accès aux données à caractère personnel, l'existence du droit d'introduire une réclamation auprès d'une autorité de contrôle, etc. ; enfin si le responsable de traitement souhaite effectuer ultérieurement un traitement avec ces mêmes données, et pour une finalité autre que celle initialement annoncée, il doit également l'indiquer.

---

[239] Règlement européen sur la protection des données, considérant 39

[240] Règlement européen sur la protection des données, considérant 60

De plus, on peut noter que le considérant 60 reprend le principe de l'article 10 c) de la directive de 1995[241], en imposant au responsable de traitement de fournir toutes les informations nécessaires au vu du contexte à la personne concernée.

Cette approche retenue par le règlement européen n'a pas innové par rapport aux précédents textes européens. La directive de 1995 liait également le concept de loyauté au niveau d'information reçu par le consommateur dans son article 6 et considérant 38[242].

B - La loyauté et l'instauration d'un rapport de confiance dans le nouveau règlement européen

Depuis le nouveau règlement européen sur la protection des données à caractère personnel, la loyauté signifie davantage que la transparence. Le règlement a modifié son article 5, si on le compare avec l'article 6 de la directive de 1995 : désormais les données à caractère personnel doivent être traitées "de manière licite, loyale et transparente" et non plus seulement de manière "loyale et licite[243]". Le règlement distingue donc désormais la loyauté et la transparence, ce qui signifie que la loyauté impliquerait autre chose que la transparence. Cette approche de la loyauté est d'ailleurs celle qui était retenue dans les autres textes européens. L'Agence des droits fondamentaux de l'Union Européenne, la Cour Européenne des Droits de l'Homme et le Conseil de l'Europe ont publié en 2014 un Manuel sur le droit de la protection des données à caractère personnel en Europe, qui résume et compile les arrêts importants de la Cour de Justice de l'Union européenne et de la Court of Human Rights dans ce domaine[244]. Le Manuel définit la loyauté à la fois comme la transparence et comme la

---

241 Directive de 1995, article 10 "Les États membres prévoient que le responsable du traitement (...) doit fournir à la personne auprès de laquelle il collecte des données (...) toute information telle que les destinataires (...), l'existence d'un droit d'accès aux données (...) dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données".

242 Directive de 1995 sur la protection des données

243 Directive de 1995 sur la protection des données, article 5

244 Ibid - Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, Cour européenne des droits de l'homme, *Manuel de droit européen en matière de protection des données*, Luxembourg, avril 2014, p.75

confiance. Il faut désormais que la personne concernée soit en position de "comprendre véritablement" ce qui va advenir de ses données personnelles.

La notion implique que les responsables de traitement aillent au delà des minimums imposés par la loi. "Un traitement loyal signifie aussi que les responsables de traitements sont prêts à aller au-delà des obligations légales minimales de services envers la personne concernée, si les intérêts de celle-ci le requièrent[245]". Cette approche signifie que les responsables de traitements devront prendre en compte les intérêts légitimes de la personne concernée, voir même s'empêcher de procéder à certains actes, même si cela est conforme à la loi. Selon l'avocat général auprès de la Cour Justice de l'Union Européenne, Mme Kokott, l'exigence de loyauté des traitements met concrètement en oeuvre "une exigence plus large de transparence et de prévisibilité des traitements des données personnelles[246]". Le G29 a ainsi instauré une grille de lecture, non contraignante, qui conseille dans un premier temps d'examiner la relation entre les finalités poursuivies par la collecte initiale et les finalités poursuivies par l'usage ultérieur des données (qui devraient contribuer aux mêmes buts), et dans un deuxième temps d'examiner le contexte dans lequel les données ont été collectées : plus la collecte ciblée est spécifique plus le titulaire des données doit pouvoir raisonnablement s'attendre à ce que ses donnée ne soient pas réutilisées[247].
La conséquence pratique risque donc d'être importante : les autorités de contrôle pourront sanctionner une entreprise qui, même si elle respecte les termes du règlement, aura effectué

---

245 Ibid - Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, Cour européenne des droits de l'homme, *Manuel de droit européen en matière de protection des données*, Luxembourg, avril 2014, p.75

246 Conclusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, *Promusicae c Telefonica de Espana SAU*, affaire C-275, paragraphe 53

247 Jean-Philippe FOEGLE, *La CJUE encadre sévèrement les échanges de données entre administrations*, La revue des droits de l'homme, février 2016, consultable sur https://revdh.revues.org/1803#ftn35, paragraphe 17

un traitement considéré en l'espèce comme attentoire aux données personnelles et à la vie privée de la personne concernée, sur le seul fondement de la loyauté[248].

La compréhension du principe de loyauté apparaît donc différente aux États-Unis et en Europe. L'approche européenne se concentre sur l'importance (numérique et en valeur) des informations fournies au consommateur, sur ses intérêts légitimes et sur sa capacité à être autonome. Cette approche traduit le fait qu'en Europe la vie privée et la protection des données personnelles est un droit fondamental. La FTC raisonne elle selon une approche de l'économie du bien-être ("*[a] welfare economics approach*[249]") en prenant en compte aussi bien les inconvénients que les avantages d'une pratique ou d'un acte, ce que ne fait pas l'Union européenne. Toutefois en pratique, le principe de loyauté sert à résoudre les mêmes problèmatiques, à ceci près que les États-Unis ont une interprétation extensive du principe d'*unfairness*. Peut-être qu'à terme, vu la modification du règlement européen, les Cours européennes développeront le principe de loyauté dans les mêmes directions que le principe d'*unfairness* aux États-Unis.

---

248 On peut noter que ce double aspect du principe de loyauté par les textes européen coïncide avec l'approche anglaise, dans laquelle l'autorité de contrôle doit notamment veiller à ce que les responsables de traitement "handle the data in ways not inconsistent with the data subject's reasonable expectations" et vis à vis de la transparence : "be transparent vis-à-vis the data subject as to how the data are being used". Source ICO, *Processing Personal Data Fairly and Lawfully* (Principle 1) consultable sur https//ico.gov.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

249 Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p.205-216

Chapitre II - L'application du principe d'*unfairness* et de loyauté en matière de protection des données à caractère personnel

Si les États-Unis et l'Europe ont une approche différente, en théorie, de la loyauté du traitement des données à caractère personnel, en pratique, les cours appliquent le principe lorsque le consommateur n'a pas été suffisamment informé par l'entreprise de la collecte et du traitement de ses données à caractère personnel (I). Les États-Unis ont cependant développé une interprétation extensive du principe d'*unfairness* (II).

I - L'application du principe de loyauté ou l'*unfairness* en cas de collecte ou d'utilisation des données sans information préalable

Le principe de loyauté sanctionne principalement les entreprises qui n'ont pas, ou pas suffisament, informées leurs consommateurs de la collecte (A) et de l'utilisation (B) de leurs données.

A - La collecte déloyale des données personnelles

La FTC considère que collecter les données personnelles d'un consommateur sans l'en informer est une pratique déloyale.

Dans la décision contre l'entreprise Aspen Way[250], la FTC considère qu'installer un logiciel espion ("*spyware*") pour collecter des données, sans en avertir le consommateur, est une pratique déloyale. La FTC a considéré qu'il y avait bien un préjudice substantiel subi par le consommateur : la surveillance invasive, auquel il ne peut échapper : "*[c]onsumers cannot reasonably avoid these injuries because [the surveillance] is invisible to them*[251]" et non compensé. Il est important de noter ici que la FTC n'a pas reproché à l'entreprise d'avoir pris un engagement dans ses *privacy policies* qu'elle n'a pas tenu : le *FTC Act*, et surtout le

---

[250] FTC, *Aspen Way Enters., Inc.,* (Ci-après Aspen Way), FTC File No. 112 3151, No. C-4392, F.T.C. 11 avril 2013, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt. pdf

[251] Ibid - Aspen Way

standard de *l'unfairness* interprété par la FTC, apparait comme la seule base légale ici. La FTC a utilisé le standard de la déloyauté dans une autre affaire, Sony BMG[252], qui portait sur la même question. Ici la FTC a considéré, comme précédemment, que l'entreprise, en incitant les consommateurs à télécharger un logiciel espion sans les avertir suffisamment, était responsable d'une pratique déloyale.

La FTC considère également que collecter les données personnelles des consommateurs grâce à des manoeuvres est déloyal. En 2009, dans l'arrêt *FTC v. Accusearch Inc*[253]., la Cour du Tenth Circuit a approuvé la FTC pour avoir lancé une action sur le fondement de la Section 5 du *FTC Act*, contre un site internet qui avait collecté et partagé des données personnelles. En l'espèce, l'entreprise Accusearch avait mis en place un site web, abika.com et récupérait grâce à ce site des données. La FTC a considéré qu'Accusearch "a utilisé de faux prétextes, de fausses affirmations, de faux documents ou des documents volés, ainsi que d'autres manoeuvres comme le fait de se mettre en scène comme le client d'un opérateur de télécommunication, pour inciter des fonctionnaires, des employés ou des agents d'une entreprise de télécommunication à exposer les enregistrements téléphoniques privés de leurs consommateurs"[254]. Les enregistrements recueillis sur le site étaient ensuite vendus à des tiers, sans que les personnes concernées soient au courant ni n'aient consenti[255]. La FTC a lancé une action contre l'entreprise Accusearch, opérateur du site, pour mettre fin à la vente des données personnelles et demander le remboursement de l'argent obtenu par la vente de ces

---

252 FTC, *Sony BMG Music Entertainment*, FTC File No. 062 3019, No. C- 4195, 28 juin 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf

253 Court of Appeals for the tenth circuit, *FTC v. Accusearch Inc*., 570 F.3d 1187, No. 08-8003, 29 juin 2009

254 Ibid - District Court for the district of Wyoming, Complaint for Injunctive and Other Equitable Relief at 5, *FTC v. Accusearch Inc*., No. 06-CV-0105, 28 septembre 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501acc_usearchcomplaint.pdf., ("Accusearch used “false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations, including posing as a customer of a telecommunications carrier, to induce officers, employees, or agents of telecommunications carriers to disclose confidential customer phone records.")

255 District Court for the district of Wyoming, Complaint for Injunctive and Other Equitable Relief at 5, *FTC v. Accusearch Inc*., No. 06-CV-0105, 28 septembre 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501acc_usearchcomplaint.pdf. "The FTC alleged that Accusearch obtained and sold to third parties confidential customer proprietary network information without the knowledge or consent of the customer"

enregistrements téléphoniques. La Cour a donné raison à la FTC en considérant que la collecte malhonnête de données personnelles était une pratique déloyale[256]. Il est intéressant de noter ici la double utilisation par la FTC de la *deceptive theory* et de *l'unfairness theory* : ici les deux notions sont utilisées, ce qui n'est pas toujours le cas, et la FTC considérera soit que la pratique est seulement mensongère soit qu'elle est seulement déloyale même si elle implique des manoeuvres[257].

En Europe, les Cours vont sanctionner les responsables de traitement sur le fondement de la loyauté pour ne pas avoir recherché le consentement de la personne concernée à la collecte de leurs données.

La Cour de cassation, dans un arrêt du 14 mars 2006[258], a jugé que le procédé consistant à recueillir des adresses email personnelles sur internet à l'insu des personnes concernées afin de leur envoyer des spams était déloyal.

La CNIL a également condamné Google pour collecte déloyale des données personnelles à cause du Google Street View. Ce service, associé à Google Maps, permet à tout internaute d'accéder à des données cartographiques sous formes de photographies, partout dans le monde. Pour mettre en oeuvre ce service, Google faisait circuler des voitures équipées d'un dispositif de photos. Cela a d'abord posé un problème de confidentialité et de protection de vie la privée car certaines personnes apparaissaient à visage découvert. Toutefois, le principal problème résidait dans le fait que les voitures possédaient un système de captation des données informatiques (celles relatives au réseaux informatiques aux alentours). La CNIL s'est alors saisie de l'affaire. Elle a considéré que la collecte des données personnelles, sans

---

256 Court of Appeals for the tenth circuit, *FTC v. Accusearch Inc*., 570 F.3d 1187, No. 08-8003, 29 juin 2009, l'arrêt décrit la pratique de l'entreprise qui consistait à solliciter de ses consommateurs des informations confidentielles protégées par la loi, mais également à payer des chercheurs susceptibles d'utiliser des méthodes prohibées pour trouver les données dont l'entreprise avait besoin.

257 Southern District of Florida, Complaint for Injunction and Other Equitable Relief at 4–5, *FTC v. CEO Grp., Inc*., No. 06-CV-60602, 2 novembre 2007, consultable sur http://www. ftc.gov/sites/default/files/documents/cases/2006/05/060501ceogroup-cmplt.pdf (alleging fraudulent obtaining of confidential customer phone records was unfair, rather than deceptive, practice)

258 Cour de cassation, chambre criminelle, 14 mars 2006, numéro 05-83-423

informer les personnes concernées et sans obtenir leur consentement, était déloyale, et a condamné Google à 100 000€ d'amendes[259].

B - L'utilisation déloyale des données personnelles

Tout d'abord, la FTC, ainsi que les autorités de contrôle en Europe, font le lien entre la collecte déloyale des données personnelles et l'utilisation qui en découle, pour considérer que cette utilisation est déloyale.

Aux États-Unis cela a été le cas dans la décision *Aspen Way Enterprises Inc*.[260] vu plus haut. Les Cours européennes et les autorités de contrôle sanctionnent également l'utilisation des données qui suit une collecte déloyale. En France, la CNIL a sanctionné l'entreprise Les Pages Jaunes pour ne pas avoir informé et obtenu le consentement des personnes concernées pour collecter leurs données. La collecte a donc été faite sans qu'ils en soient avertis, grâce à leur profil public sur les médias sociaux, et l'entreprise a ensuite utilisé ces données pour les insérer dans son catalogue en ligne les Pages Jaunes. La CNIL a jugé l'ensemble du processus déloyal (la collecte puis l'utilisation qui s'en est suivi) car les personnes concernées n'avaient pas été informées que les données présentes sur leur profil public seraient récupérées et n'ont jamais eu l'occasion de donner leur consentement[261].

La FTC et les autorités de contrôle considèrent également que l'utilisation des données est déloyale dès lors que le consommateur n'a pas donné son consentement à l'utilisation. Ce principe est illustré dans l'arrêt *FTC v Hill*[262], où l'entreprise utilisait les données bancaires des consommateurs pour acheter des biens et des services, sans leur consentement. La FTC a également intenté une action contre une application gratuite qui fournissait une lampe torche à ses utilisateurs ,et qui partageait la géolocalisation de ces derniers avec des publicitaires sans

---

[259] CNIL, *Délibération numéro 2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc*., 6 janvier 2011 consultable sur https://www.cnil.fr/sites/default/files/typo/document/D2011-035.pdf

[260] Ibid - Aspen Way Enters., Inc. 11 avril 2013

[261] CNIL décision 2011-203 du 21 septembre 2011, confirmée par le conseil d'état le 12 mars 2014 (requête 353193)

[262] Southern District Court of Texas, *FTC v. Hill*, No. 03-5537, 22 mars 2004, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323 102.pdf

les avertir ni recueillir au préalable leur consentement[263]. En Europe, dans l'arrêt *British Gas trading v Data Protection Registrar*[264], la Cour anglaise a considéré que l'utilisation des données par l'entreprise de gaz était déloyale car l'entreprise n'avait pas cherché à obtenir le consentement de la personne concernée avant le traitement de ses données.

II - Les autres applications du principe d'*unfairness* aux États-Unis

Les cours américaines utilisent le principe de l'*unfairness* pour sanctionner les entreprises qui rendent, grâce à la structure de leur site internet, l'information difficile d'accès (A), qui ne mettent pas en place des mesures de protection des données à caractère personnel efficaces (B), ou qui changent rétrocativement leurs *privacy policies* (C).

A - La déloyauté de la structure du site internet

La FTC considère qu'une entreprise, en imposant au consommateur des choix par défaut et sans l'en avertir, ou en créant son site internet de manière à rendre l'information difficilement accessible, est responsable d'un acte ou d'une pratique déloyale. Dans l'affaire Sony BMG Music Entertainment, un logiciel était installé sur l'ordinateur des consommateurs mais d'une telle manière que ces derniers n'étaient pas au courant de sa présence et qu'il était très difficile de l'enlever. Cette pratique a été considéré déloyale[265]. Dans un autre arrêt, la FTC a considéré que le fait de ne pas avoir informé les consommateurs que le site choisissait par défaut et pour eux la manière dont leurs données étaient partagées, était une pratique déloyale[266].

---

263 Ieuan JOLLY, *Data protection in United States : overview*, Practical Law, Multi-jurisdictionnal guide, Thomson Reuters, 2014/15, p.1

264 Data protection tribunal, *British Gas trading v Data Protection Registrar*, DA98 3/49/2 1998, consultable sur http://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/foi/bgtdec.pdf

265 Ibid - FTC, *Sony BMG Music Entertainment*, FTC File No. 062 3019, No. C- 4195, 28 juin 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf

266 Southern district court of Florida, Complaint for Permanent Injunction and Other Equitable Relief at 19, *FTC v. Frostwire, LLC*, No. 1:11-cv-23643, 12 octobre 2011, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2011/ 10/111011frostwirecmpt.pdf

B - La déloyauté du fait de l'absence de mesures de sécurité raisonnables

La FTC considère que ne pas réussir à protéger des données sensibles est une pratique déloyale. La FTC a ainsi déposé une plainte contre trois entreprises[267] qui avaient subi une violation de leur système de sécurité, mais qui n'avaient pas violé leurs engagements pris dans leurs *privacy policies*. La FTC a considéré que les entreprises avaient échoué à instaurer des mesures raisonnables de sécurités pour protéger les données sensibles qu'elles avaient à leur disposition et que cet échec en lui même était une pratique de loyale au sens de la Section 5. En 2014, dans un arrêt *FTC v Wyndham Hotels*[268], la FTC a de nouveau considéré que la mise en place de mesures de sécurités est déloyale si ces mesures ne sont pas adéquates.

C - La déloyauté par le changement rétroactif de *privacy policies*

La FTC considère que le changement rétroactif de ses *privacy policies* par une entreprise sans qu'elle en avertisse ses consommateurs et sans qu'elle leur propose d'opter pour cette nouvelle politique est considérée comme une pratique déloyale[269].

---

267 FTC, Complaint *BJ's Wholesale Club*, Inc. No. C-4148, File 042 3160, 23 septembre 2005, consultable sur http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf ; FTC, Complaint, *DSW, Inc*., No. C-4157, File 052 3096, 1er décembre 2005, consultable sur http://www.ftc.gov/os/caselist/0523096/05_120_Icomp0523096.pdf ; FTC, Complaint, *CardSystems Solutions, Inc*., No. C-4168, File 052 3148, 8 septembre 2006, consultable sur http://www.ftc.gov/os/caselist/0523148/0523 1 48CardSystemscomplaint.pdf

268 District Court of New Jersey, *FTC v Wyndham Hotels*, Civ, Action numéro 13-1887, 7 avril 2014

269 FTC, *Gateway Learning Corporation*, 138 FTC 443, 470, File no 042-3047, juillet 2004

Chapitre III - Les limites du principe d'*unfairness* et de loyauté

Aux États-Unis, la conduite du *three-part test* peut s'avérer délicate (I), et aux États-Unis comme en Europe, articuler le principe de loyauté autour de l'information transmise pose plusieurs difficultées (II).

I - Les limites de l'analyse coûts-bénéfices et de l'évaluation du préjudice substantiel

Les principales difficultés sont posées par la conduite d'une analyse coûts-bénéfices (A), et par l'appréciation de la substantialité du préjudice (B).

A - La difficulté à évaluer le coût et la substance du préjudice

Selon Maître Maxwell[270], une des principales difficultés dans l'application du test pour évaluer si la pratique est déloyale, est la conduite d'une analyse coûts-bénéfices, qui suppose la quantification des préjudices et l'évaluation de la substance du préjudice (A) mais aussi la quantifications des bénéfices (B) tirés d'un acte ou d'une pratique. Il revient sur les travaux d'Alessandro Acquisti dans *The economics of personal data and the economics of privacy* (2010) et sur ceux d'Adam Thierer dans *A framework for benefit-cost analysis in digital privacy* (2013).

Alessandro Acquisti et Adam Thierer mettent en avant le fait que le droit à la protection de sa vie privée est un droit intangible et fondamental, mais souvent difficile à évaluer et les préjudices qui en découlent peuvent être de nature tout à fait diverse. Le droit à la protection de la vie privée a bien souvent comme fondement des émotions, des ressentis, ce qui rend son évaluation économique délicate. Il faut également ajouter à cela une certaine tentation à vouloir sous-évaluer le préjudice subi par la violation de la vie privée : même si les consommateurs se disent attachés à la protection de leurs données[271], plusieurs études

---

270 Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p.211

271 Joseph PHELPS, Glenn NOWAK & Elizabeth FERRELL, *Privacy Concerns and Consumer Willingness to Provide Personal Information*, Journal of Public Policy and Marketing, volume 19, 2000

démontrent en fait que les politiques de protection des données mises en place par les entreprises ne sont pas prises en compte par les consommateurs lorsqu'ils prennent une décision en ligne [272].

Dans certaines affaires, le préjudice subi par violation de ses données personnelles peut être facilement quantifié, comme la réception de spams non désirés (détérioration du matériel informatique, temps passé etc.). Mais d'autres préjudices sont plus complexes à quantifier : ces préjudices sont liés à des traitements de la donnée qui vont plus loin que ceux à quoi le consommateur s'attendait[273], et vont rendre le consommateur nerveux et effrayé. Dans son essai, le professeur Calo[274] propose d'ailleurs d'identifier deux aspects du "*privacy harm*" (préjudice découlant de la violation de la vie privée d'une personne) : un aspect objectif, qui consiste en un préjudice externe subi par le consommateur (vol d'identité, la divulgation d'informations que l'on souhaitait confidentielles...) ; et un aspect subjectif qui consiste en des sentiments négatifs perçus par le consommateur comme l'anxiété, ou encore le malaise dû au fait qu'il se sent surveillé (installation de logiciels espions sur son ordinateur, envoi de mails extrêmement ciblés concernant une information que le consommateur tenait confidentielle, partage de données auprès de plusieurs entreprises de différents secteurs etc.). Ces derniers préjudices sont plus difficiles à identifier mais existent pourtant.

L'évaluation de la notion de préjudice substantiel est également extrêmement délicate. Elle suppose la preuve que le préjudice soit tangible, et donc qu'il ne repose pas sur des craintes ou des appréhensions (voir *supra*). Or en matière de protection des données personnelles, de nouvelles technologies sont régulièrement inventées et appliquées, sans que l'on puisse savoir encore quels sont leurs risques et quelles sont toutes leurs modalités d'application. Cette incertitude sur l'existence d'un préjudice substantiel se retrouve dans les opinions dissidentes des rapports émis par la FTC. Dans celle du commissaire Rosch[275], suite au rapport *Bests*

---

272 Ibid - Joseph P. NEHF, *Shopping for privacy online : consumer-decision making strategies and the emerging market for information privacy*, Journal of Law, Technology and Policy, volume 1, 2005

273 Omer TENE, Jules POLONETSKY, *A theory of Creepy : Technology, Privacy and Shifting Social Norms*, 16 Yale Legal Journal & Technology, 2013

274 Ryan CALO, *The boundaries of privacy harm*, Indiana Law Journal, vol 86:1, 2011

275 FTC Staff Report, *Dissenting Statement of Commissioner J. Thomas Rosch,* Octobre 2012, consultable sur https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fr_jtr_dissentingstmnt.pdf

practises for common uses of facial recognition technologies de 2012 (qui encourage une régulation des technologies de reconnaissance faciale par le standard de l'*unfairness*), le commissaire met en avant le flou qui existe autour de la notion de préjudice substantiel, en estimant que rien, dans le rapport, n'indique que la technologie de reconnaissance faciale est assez évoluée pour faire courir un risque pour la sécurité des consommateurs. L'ALJ, la juridiction administrative de la FTC, a également rejeté en novembre 2015 la plainte de l'Agence contre une entreprise pour pratique déloyale, au motif que le FTC n'a pas assez justifié en quoi la pratique cause, ou est susceptible de causer, un préjudice substantiel aux consommateurs. La FTC avait enquêté sur les violations du système de sécurité informatique d'un laboratoire d'essai clinique (violations qui avaient conduit à la divulgation de plusieurs données personnelles des clients du laboratoire). L'Agence avait considéré que ces violations avaient été rendues possibles par l'insuffisance du système de sécurité, et donc que le système de protection des données était déloyal. Mais l'ALJ a estimé que la violation du système de sécurité de l'entreprise, puis l'utilisation des données récoltées qui s'en est suivi, n'avait pas pu causer aux consommateurs de préjudice substantiel, car le fait que l'exploitation de ces données ait été "possible", et non "probable", révèlerait justement que le préjudice n'est pas substantiel... et donc in *fine* que les mesures de sécurité ne sont pas déloyales[276].

B - La difficulté à évaluer le bénéfice

Les bénéfices d'une pratique potentiellement déloyale sont considérés inversement comme "les coûts induits par la régulation, ou les coûts induits par l'arrêt de la régulation, de cette pratique"[277]. Deux situations peuvent donc se produire : soit la pratique n'est pas encadrée, soit elle l'est (en étant alors soit autorisée soit prohibée), et la différence entre ces deux situations indique le coût, et donc *a contrario* le bénéfice tiré de la non intervention. Or tout comme les inconvénients, les avantages d'une pratique, ou plutôt donc, le coût de

---

[276] Timothy TOBIN, *FTC ALJ : Embarrassment / Emotional Harm and Risk of Harm Does Not Satisfy "Substantial Consumer Injury" Prong of Unfairness*, Hogan Lovells, Chronicle of data protection, Consumer privacy, 17 novembre 2015, consultable sur http://www.hldataprotection.com/2015/11/articles/consumer-privacy/ftc-alj-embarrassmentemotional-harm-and-risk-of-harm-does-not-satisfy-substantial-consumer-injury-prong-of-unfairness/

[277] Ibid - Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p.211, "benefits of a potentially unfair practice are equal to the costs associated with stopping or regulating the practice".

l'intervention ou de la non intervention, sont difficiles à évaluer. Cela est d'autant plus vrai que certains coûts, comme celui de l'atteinte à la liberté d'entreprendre auquel se réfèrent certains auteurs, sont particulièrement flous[278].

Si la FTC peut se trouver gênée en appliquant le test du préjudice substantiel et l'analyse coûts-bénéfices, les institutions européennes, comme l'Agence américaine, rencontrent les mêmes difficultés sur le niveau d'information fourni par l'entreprise au consommateur, élément essentiel pour apprécier la loyauté de la collecte et de l'utilisation des données à caractère personnel.

II - Le problème de l'information transmise à la personne concernée

En Europe, la loyauté est conçue notamment comme la capacité de l'individu à exercer son libre arbitre grâce aux informations qui lui ont été fournies (voir *supra*). Aux États-Unis, un des éléments du *three-part test* pour déterminer si l'acte ou la pratique est déloyal, est de savoir si le préjudice était "raisonnablement évitable", c'est-à-dire si le consommateur avait été suffisamment averti de la collecte et de l'utilisation de ses données, et dans quels buts. On retrouve donc en Europe et aux États Unis les mêmes difficultés quant à l'information transmise. Dans leurs textes[279], les institutions américaines et européennes appellent les entreprises à clarifier et à simplifier leurs conditions générales (dans lesquelles sont contenues les engagements de protection des données personnelles), pour informer au mieux les consommateurs. Mais ce qui pose problème ici est l'appréciation de l'information donnée, et

---

278 Avi GODFARB, Catherine TUCKER, *Privacy and Innovation,* National Burreau of Economic Research, Working Paper 17124, Juin 2011, Ces auteurs ont cherché à mesurer les bénéfices, ou plutôt donc les coûts, de la nouvelle législation européenne en matière de publicité ciblée, qui oblige les entreprises à demander leur consentement aux consommateurs pour être suivis par des cookies. Leur conclusion est que cette règle a plusieurs effets négatifs sur le marché de la publicité en ligne, et que cette législation aurait dû être soumise à une analyse coûts-bénéfices car elle aurait des répercussions sur les capacités à innover des acteurs, et sur la liberté d'expression. Or le problème posé par l'analyse est le recours à des notions floues comme les libertés d'innovation ou d'expression : les préjudices attachés au non respect de ces libertés sont difficiles à quantifier, et donc à insérer dans la conduite d'une analyse coûts-bénéfices.

279 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, mars 2012, p. 62 ; White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, p. 14 ; règlement européen sur la protection des données personnelles article 12 transparence

selon Jonathan A. Obar[280], demander aux entreprises d'améliorer leurs conditions générales ne permettra pas d'assurer une meilleure information aux consommateurs. Pour l'auteur, il n'est pas réaliste de demander à quelqu'un, peu importe son statut ou ses capacités, de lire ces notices, puis d'en extraire des informations claires, sachant que, de plus, elles évoluent constamment. L'auteur avance deux arguments : les notices contenant les principes de protection des données à caractère personnel sont trop longues (A) mais aussi trop complexes (B).

A - La longueur des notices

Une étude conduite en 2008 sur les 75 sites les plus populaires[281] a montré que leurs *privacy policies* contenaient une moyenne de 2500 mots, et qu'il fallait environ une vingtaine de minutes pour en parcourir une. L'étude a alors estimé qu'il faudrait 201 heures par an pour lire toutes les *privacy policies* qui entreraient en contact avec un consommateur, avec une moyenne de 40mn par jour. Une autre étude, conduite en 2012 par le site britannique Which?, a, de son côté, montré que les *privacy policies* s'étaient allongées avec le temps. Les appels pour une plus grande transparence ce sont donc traduits en pratique par des *privacy policies* plus détaillées, ainsi que par la rédaction de rapports sur la question de la transparence, et de guides pour appliquer les principes de transparence[282]. Cela suggère que les récents appels pour plus de transparence risquent, en pratique, de produire de nouveau des *privacy policies* plus longues qu'elles ne le sont déjà, ce qui aura pour conséquence de rendre l'information encore plus difficile à appréhender.

---

280 Ibid - Jonathan A OBAR, *Big Data and The Phantom Public : Walter Lippman and the fallacy of data privacy self-management*, Big Data & Society, décembre 2015

281 Aleecia Mc DONALD, Lorrie CRANOR, *The Cost of Reading Privacy Policies*, A Journal of Law and Policy for the Information Society, Privacy Year in Review Issue, 2008

282 Nicolas CARDOZO et autres, *Who has your back ? protecting your data from government requests*, 2014 consultable sur https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-

B - La complexité des notices

Une récente étude conduite par Reidenberg[283] en 2014 a montré à quel point il était difficile de comprendre les *privacy policies*, même pour des experts en la matière. Il apparaît donc difficile, pour les consommateurs, de fournir un consentement éclairé sur des questions mettant en jeu nos données personnelles, et pour les professionnels, de fournir une appréciation sur ce à quoi les entreprises s'engagent. L'étude a réuni plusieurs acteurs plus ou moins spécialisés sur la question de la protection de la vie privée et des données personnelles. Ces personnes étaient divisés en plusieurs groupes de niveaux afin d'évaluer les engagements pris par une sélection d'entreprises sur le partage des données, leur détention, et leur suppression. Ils devaient ensuite comparer leurs résultats au sein de leur groupe, puis avec les autres groupes. Les résultats ont montré que, même au sein des groupes les plus spécialisés, il y avait des désaccords profonds sur le contenu des *privacy policies*.

Par ailleurs, plusieurs études montrent que le problème de compréhension des enjeux attachés à la protection des données personnelles, d'éducation des consommateurs et des acteurs de la protection de leur vie privée en ligne, ne pourra pas se résoudre par des politiques de protection des données plus claires et faciles à comprendre[284].

---

283 J. R. REIDENBERG et autres, *Disagreeable privacy policies : Mismatches between meaning and users' understanding*, Fordham law legal studies research paper, 2014, Consultable sur http:// papers.ssrn.com/sol3/Papers.cfm?abstract_id=2418297

284 Ibid - Joseph P. NEHF, *Shopping for privacy online : consumer-decision making strategies and the emerging market for information privacy*, Journal of Law, Technology and Policy, volume 1, 2005

Conclusion

L'Union européenne s'est inspirée des principes américains d'*accountability* et d'*unfairness* dans sa législation sur la protection des données à caractère personnel. Ces deux principes se retrouvent en effet dans les textes européens. L'Union européenne a ainsi absorbé le principe d'*accountability*, sa philosophie (le principe de responsabilité devant autrui sous le contrôle d'une autorité étatique) et ses outils (la mise en place de programmes de conformité, que ce soit par les accords conclus avec la FTC aux États-Unis, ou par l'adoption de BCR en Europe) pour l'insérer dans son propre système. Et si les États-Unis conçoivent la loyauté principalement comme un rapport économique alors que l'Union européenne écarte cet aspect pour envisager la loyauté comme un droit à l'information et un rapport de confiance, cette différence d'approche ne se traduit pas forcément par une différence d'application de ces principes. Aux États-Unis, comme au sein de l'Union européenne, la loyauté sert à sanctionner les entreprises qui n'ont pas informé leurs consommateurs de la collecte et de l'utilisation de leurs données ; le principe de loyauté pourra peut-être également sanctionner des sites internet qui ont adopté une structure confuse pour le consommateur, comme cela est le cas aux États-Unis, grâce à l'élargissement de la notion de loyauté dans le nouveau règlement européen. Les deux systèmes de protection des données à caractère personnel apparaîssent *in fine* assez proches. L'accent a été mis ici sur la réception par l'Union européenne de principes américains, mais il serait également intéressant de voir dans quelle mesure les États-Unis, et plus particulièrement la FTC dans son travail d'établissement d'une *FTC common law privacy*, se sont inspirés des principes européens de protection des données à caractère personnel pour enrichir leur propre système. On retrouve en effet aux États-Unis des principes connus de l'Union Européenne, comme celui de la suppression des données collectées. De plus, la Maison-Blanche et la FTC appellent aujourd'hui le Congrès à adopter une loi générale de protection des données à caractère personnel.

BIBLIOGRAPHIE

LOIS - RÈGLEMENTATIONS

APEC, *Cross Boarder Privacy Rules* (*CBPR*), 2004

Charte des droits fondamentaux de l'Union Européenne, 2000/C 364/01, 18 décembre 2000

Children's Online Privacy Protection Act, 15 U.S.C, §6501-6506, 15 octobre 1998

Commission européenne, *Directive 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*, 24 octobre 1995

Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003, 15 U.S.C § 7701-7713

Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950

Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, dite aussi *Convention 108*, Strasbourg, 28 janvier 1981

Credit Practises Rule, 49 Fed. Reg. § 7745 à 7776, 1984

Data Security Law, California Civil code §1798.81.5

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

Directive 2002/58 du Parlement Européen et du Conseil concernant le traitement le traitement des donnée à caractère personnel et la protection de la vie privée dans le secteur des communications éléctroniques, réformée par la directive du 25 novembre 2009

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications éléctroniques accessibles au public ou de réseaux publics de communications, modifiant la directive 2002/58/CE.

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications éléctroniques

Fair Credit Reporting Act, 15 U.S.C § 1681

Federal Trade Commission Act, 1914 (aujourd'hui codifié dans le U.S.C §41-58).

FTC Improvements Act, Pub. L. No. 96-252, mai 1980

Financial Services Modernization Act, 1999

Health Insurance Portability and Accountability Act, 42 U.S.C §1320d-1320d-8, 1996

H.R. Conf. Rep. No. 1142, 63d Cong. 2d Sess., at 19 (1914) => soit ici soit dans "autres"

ISO/IEC 29100, International standard, information technology - security techniques - privacy framework, 15 décembre 2011

Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978

Massachussetts Regulation, 201 CMR 17.00

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, revu en 2013

Proposition de règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Bruxelles, 25 janvier 2012

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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avril 2016

Restatement (2d) of Torts

Security Breach Notification Law, 1386, California Civil code, § 1798.82 et 1798.29, 2002

Shine the light law, California Civil code, § 1798.83, Septembre 2003

Telephone consumer protection Act, 47 U.S.C § 227 et suivants

Traité sur le fonctionnement de l'Union européenne (version consolidée), 2012/C 326/01, octobre 2012

U.S Department of Health Education and Welfare, *Records, Computers, and the Rights of Citizens : Report of the Secretary's Advisory Comm. on Automated Personal Data Systems 29* (1973)

Wheeler-Lea Amendment, 1938, amendement du FTC Act

TEXTES ÉMANANT DES AUTORITÉS DE PROTECTION DES DONNÉES

CNIL, *Adoption de la décision d'adéquation du Privacy Shield par la commission européenne*, 12 juillet 2016, consultable sur https://www.cnil.fr/fr/adoption-de-la-decision-dadequation-du-privacy-shield-par-la-commission-europeenne

CNIL, *Le G29, groupe des "CNIL" européennes*, consultable sur http://www.cnil.fr/linstitution/international/g29

CNIL, *Les BCR qu'est ce que c'est ?*, consultable sur http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/

CNIL, *Les BCR règles internes d'entreprises*, consultable sur https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise, Juillet 2016

FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, July 2008, consultable sur http:// www.ftc.gov/about-ftc/what-we-do/enforcement-authority

FTC*, Data Brokers, A Call for Transparency and Accountability,* mai 2014

FTC, *Facing Facts : Best Practices for Common Uses of Facial Recognition Technologies* (2012), consultable sur http://www.ftc.gov/sites/default/files/documents/ reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fac ialtechrpt.pdf

FTC, *Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security*, 1998, consultable sur https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm

FTC, *Mobile Privacy Disclosures : Building Trust Through Transparency,* 2013, consultable sur http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-dis closures-

building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

FTC, *Performance & Accountability Report Fiscal Year 2012*, 2012, consultable sur http://www.ftc.gov/sites/default/files/documents/reports/federal-trade- commission-performance-and-accountability-report/2012parreport.pdf

FTC, *Policy statement on Unfairness*, décembre 1980

Press Release, *Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts*, FTC 23 décembre 2008, http://www.ftc.gov/opa/2008/12/civilpenalty. shtm

FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, mars 2012, consultable sur http://www.ftc.gov/sites/ default/files/documents/reports/federal-trade-commission-report-protecting-consumer-p rivacy-era-rapid-change-recommendations/120326privacyreport.pdf

FTC, *Self-Regulation and Privacy Online : A Report to Congress*, juillet 1999, consultable sur https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf

FTC Staff Report, *Dissenting Statement of Commissioner J. Thomas Rosch,* Octobre 2012, consultable sur https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022fr_jtr_dissentingstmnt.pdf

FTC Staff Report on television advertising to children, *Notice of Proposed Rulemaking on television advertising to children*, 1978

FTC Staff Report : *No Present Intention of Challenging Council of Better Business Bureaus' Accountability Program for Online Behavioral Advertising as Anticompetitive*, Federal Trade Commission Documents and Publications, Août 2011

FTC Staff Report, *Self-Regulatory Principles for Online Behavourial Advertising*, 2007

FTC, Statement of Basis and purpose, *Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking*, 29 Fed. Reg. 8324, 8355, 1964

Groupe de travail Article 29, *Avis 3/2010 sur le principe de responsabilité*, WP 173, Bruxelles, juillet 2010

ICO, *Processing Personal Data Fairly and Lawfully* (Principle 1) consultable sur https// ico.gov.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

MANUELS ET GUIDES ÉMANANT DES INSTITUTIONS

Agence des droits fondamentaux de l'Union Européenne, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données*, Luxembourg : Office des publications de l'Union Européenne, 2010

Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, Cour européenne des droits de l'homme, *Manuel de droit européen en matière de protection des données*, Luxembourg, avril 2014

Commission européenne, *Promouvoir un cadre européen pour la responsabilité sociale des entreprises,* Livret vert, juin 2001

Communication de la Commission Européenne au Parlement Européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions, *Une approche globale de la protection des données à caractère personnel dans l'Union Européenne*, 4 novembre 2010

European Commission, *The EU Data Protection Reform and Big Data*, *Factsheet*, mars 2016, consultable sur http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf

European Commission, Information providers guide, *The EU internet handbook*, dernière mise à jour le 7 juin 2016, consultable sur *http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm*

Groupe de travail "Article 29" sur la protection des données, *Document de travail : transferts de données personnelles vers des pays tiers : application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprises contraignantes applicables aux transferts internationaux de données*, 11639/FR WP 74, 3 juin 2003

U.S Department of Health Education and Welfare, Records, Computers, and the Rights of Citizens, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, DHEW Publication No.(OS) 73-94, July 1973

White house, *Consumer Data Privacy In A Networked World : A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, février 2012, consultable sur https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

JURISPRUDENCE ET DÉCISIONS ADMINISTRATIVES

CNIL décision 2011-203 du 21 septembre 2011, confirmée par le conseil d'état le 12 mars 2014 (requête 353193)

CNIL, *Délibération numéro 2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc*., 6 janvier 2011 consultable sur https://www.cnil.fr/sites/default/files/typo/document/D2011-035.pdf

Conclusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, *Promusicae c Telefonica de Espana SAU*, affaire C-275, paragraphe 53

Cour de cassation, chambre criminelle, 14 mars 2006, numéro 05-83-423

Cour de Justice de l'Union Européenne, *Commission des Communautés européennes / République fédérale d'Allemagne*, affaire C-518/0, Luxembourg, 9 mars 2010

Cour de Justice de l'Union Européenne, *Maximillian Schrems / Data Protection Commissioner*, affaire C-362/14, Luxembourg, 6 octobre 2015

Court of Appeals of Illinois, *Dwyer v American Express Co*, 273Ill. App.3d 742, 652 N.E.2d 1351, 30 juin 1995

Court of Appeals for the tenth circuit, *FTC v. Accusearch Inc.*, 570 F.3d 1187, No. 08-8003, 29 juin 2009

Court of Appeals for the 11th circuit, *Orkin Extermination Co. v FTC*, 849 F.2d 1354, 1988

Court of Appeals for the 11th circuit, *United States v. Danube Carpet Mills, Inc.*, 737 F.2d 988, 993, 1984

Court of Appeals of Ohio, Eight Appellate District, *Shibley v. Time, Inc.*, 45 Ohio App. 2d 69 ; 341 N.E.2d 337 ; 74 Ohio Op. 2d 101 ; 82 A.L.R. 3d 765, 19 juin 1975

Data protection tribunal, *British Gas trading v Data Protection Registrar*, DA98 3/49/2 1998, consultable sur http://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/foi/bgtdec.pdf

District Court for the district of Wyoming, Complaint for Injunctive and Other Equitable Relief at 5, *FTC v. Accusearch Inc.*, No. 06-CV-0105, 28 septembre 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf.

District court of Minnesota, 6 juin 2004, *Northwest Airlines Privacy Litigation*, No. Civ. 04-126 (PAM/JSM), WL 1278459

District Court of Nevada, *Loeffler v. Ritz-Carlton Hotel Co*., No. 2:06-CV-0333-ECR-LRL, 2006 WL 1796008, 28 juin 2006

District Court of New Jersey, *Smith v. Trusted Universal Standards in Elec. Transactions, Inc*., No. 09- 4567 (RBK/KMW), 2011 WL 900096, 15 mars 2011

District Court of New Jersey, *FTC v Wyndham Hotels*, Civ, case 2:13-cv-01887-ES-JAD, Action numéro 13-1887, 7 avril 2014

FTC, *Aspen Way Enters., Inc*., FTC File No. 112 3151, No. C-4392, 25 septembre 2012 (consent order), consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120925 aspenwayagree.pdf

FTC, *Aspen Way Enters., Inc.,* FTC File No. 112 3151, No. C-4392, F.T.C. 11 avril 2013, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt. pdf

FTC, Complaint *BJ's Wholesale Club*, Inc. No. C-4148, File 042 3160, 23 septembre 2005, consultable sur http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf

FTC, Complaint, *DSW, Inc*., No. C-4157, File 052 3096, 1er décembre 2005, consultable sur http://www.ftc.gov/os/caselist/0523096/05 120 Icomp0523096.pdf

FTC, Complaint, *CardSystems Solutions, Inc*., No. C-4168, File 052 3148, 8 septembre 2006, consultable sur http://www.ftc.gov/os/caselist/0523 148/0523 1 48CardSystemscomplaint.pdf

FTC, *Gateway Learning Corporation*, 138 FTC 443, 470, File no 042-3047, juillet 2004

FTC, *HTC Am. Inc*., FTC File No. 122 3049, No. C-4406, at 5, F.T.C. 2 juillet 2013 consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf

FTC, *Sony BMG Music Entertainment*, FTC File No. 062 3019, No. C- 4195, 28 juin 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf

Middle District of Florida, *FTC v. Action Research Grp., Inc*., No. 6:07-cv-00227-Orl-22UAM, 18 mars 2008, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2008/05/080528fo.pdf

Northern District of California, *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864–65, 2011

Northern District of California, *LinkedIn User Privacy Litig*., 932 F. Supp. 2d 1089, 1094, 2013

Northern District of California, *Rudgayzer v. Yahoo! Inc*., No. 5:12-CV-01399 EJD, 2012 WL 5471149, novembre 2012

Northern District Court of California, United States' Response to Consumer Watchdog's Amicus Curiae, *United States v. Google Inc.*, No. 3:12-cv-04177-SI, 28 septembre 2012, consultable sur http://www.consumerwatchdog.org/resources/ftcresponse092812.pdf

Northern District of California, *United States v. Google Inc*., No. CV 12-04177 SI, 16 novembre 2012, (order), consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2012 /11/121120googleorder.pdf

Northern District Court of Illinois, *FTC v. Westby*, No. 03-C-2540, 16 Septembre 2003

NY Supreme Court, *Daniels v. JP Morgan Chase Bank*, N.A., No. 22575/09, 2011 WL 4443599, 22 Sept. 2001

Southern District Court of Florida, Complaint for Injunction and Other Equitable Relief, *FTC v. CEO Grp., Inc*., No. 06-CV-60602, 2 novembre 2007, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501ceogroup-cmplt.pdf

Southern District Court of Florida, Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. Frostwire, LLC*, No. 1:11-cv-23643, 12 octobre 2011, consultable sur http:// www.ftc.gov/sites/default/files/documents/cases/2011/ 10/111011frostwirecmpt.pdf

Southern District Court of Texas, *FTC v. Hill*, No. 03-5537, 22 mars 2004, consultable sur http://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323102.pdf

Supreme Court, *Katz v United States*, 389 U.S 247 (1964)

Supreme Court, *Sperry vs Hutchinson C...*, 405 U.S. 223, 244-45 n.5 (1972)

Supreme Court, *FTC v Raladam Co*., 283 U.S 643, 648 (1931)

Supreme Court, *Florida v Jardines* 133.S.Ct. 1409 (2013)

Supreme Court, *United States v Jones*, 132 S.Ct.949 (2012)

DOCTRINE

Céline CASTETS-RENARD*, Quelle protection des données personnelles en Europe ?*, Larcier, Paris, 2015

Nicolas CARDOZO et autres, *Who has your back ? protecting your data from government requests*, 2014 consultable sur https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-

Christophe COLLARD et autres, *Risque juridique et conformité, Manager la compliance*, Lamy Conformité, novembre 2011

David DECHENAUD*, Le droit à l'oubli*, Droit et justice, Paris, 2014

Pierre DELORT, *Le big data*, Que sais-je, PUF, 2015

Guillaume DESGENS-PASANAU et autres, *Informatique et Libertés, Enjeux, risques, solutions et outils de gestion*, Lamy Conformité février 2013

Guillaume DESGENS-PASANAU, *La protection des données personnelles*, LexisNexis, Paris, 2015

Caroline LE GOFFIC et autres, *Droit des activités numériques*, Précis Dalloz, juin 2014

David WRIGHT, Paul DE HERT, *Enforcing Privacy : Regulatory, Legal and Technological Approaches*, Springer, 2016

Peter WIRTZ, *Les meilleures pratiques de gouvernements d'entreprises*, La découverte, Repères, Paris, 2008

ARTICLES SCIENTIFIQUES

Byron ACOHIDO, *FTC seeks laws to protect consumer privacy online*, Gannett News Service [McLean] 27 Mar 2012, consultable sur ProQuest Central Columbia

Joe BARTON, *Rush welcome FTC report calling for greater transparency and accountability among data brokers*, (2014). Lanham : Federal Information & News Dispatch, Inc. Consultable sur http://ezproxy.cul.columbia.edu/login?url=http://search.proquest.com/docview/1529244431?accountid=10226

Entertainment Close-up, *FTC Issues Report on Protecting Consumer Privacy*, 31 Mar. 2012, Business Insights : Essentials, Web. 7 juin 2016

Howard BEALES, *The FTC's and the New Common Law of Privacy*, Rev. 583, 2014

Howard BEALES, *The FTC's use of unfairness authority : its Rise, Fall, and Ressurection,* The marketing and public policy conference, Washington D.C, 30 mai 2003, consultable sur https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection

Rocco BELLANOVA et Paul DE HERT, *Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique*, Cultures & Conflits, Centre d'études sur les conflits, 2009, p.61-79

Colin J. BENNETT, "*Implementing Privacy Codes of Practice*" (PLUS 8830), Canadian Standards Association, 1995

Colin J. BENNETT, *International Privacy Standards : Can Accountability be Adequate ?,* Privacy Laws and Business International, Vol. 106, 2010

Ryan CALO, *The boundaries of privacy harm*, Indiana Law Journal, vol 86:1, 2011

A. CAVOUKIAN, *Privacy by design*, 2009, disponible sur http://www.ipc.on.ca/images/Ressources/privacybydesign.pdf

Chris CONNOLLY, *Trustmark Schemes Struggle to Protect Privacy*, pour Gallexia, 26 septembre 2008 consultable sur http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_strug gle_public.html

Aleecia Mc DONALD, Lorrie CRANOR, *The Cost of Reading Privacy Policies*, A Journal of Law and Policy for the Information Society, Privacy Year in Review Issue, 2008

Jean-Philippe FOEGLE, *La CJUE encadre sévèrement les échanges de données entre administrations*, La revue des droits de l'homme, février 2016, consultable sur https://revdh.revues.org/1803#ftn35, paragraphe 17

Robert GELLMAN, *Fair Information Practises : A Basic History*, décembre 2015, consultable sur http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf

Avi GODFARB, Catherine TUCKER, *Privacy and Innovation,* National Burreau of Economic Research, Working Paper 17124, Juin 2011

Graham GREELEAF, *Privacy Principles : Irrelevant to Cyberspace ?,* in *Privacy Law and Policy Reporter*, vol.3, n.6, septembre 1996

Jean-Louis HALPERIN, *Protection de la vie privée et privacy : deux traditions juridiques différentes ?*, Les nouveaux cahiers du Conseil constitutionnel 2015, p.59-68

G. S. HANS, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, Michigan Telecommunications and Technology Law Review, Vol.19 Issue 1, University of Michigan Law School, 2012

Steven HETCHER, *The De Facto Federal Privacy Commission*, 19 J. Marshall J. Computer & Info. L. 109, 131 (2000)

Internet Business Newsweekly, *Consumer Watchdog Calls On FTC To Enact Do Not Track, Says Force of Law Needed*, 7 Mar. 2011, Business Insights : Essentials

Vassili JOANNIDÈS, Stéphane JAUMIER, *De la démocratie en Amérique du Nord à l'accountability à la française. Comprendre les origines sociopolitiques de l'accountability*, Revue française de gestion 2013/8 (N° 237), p. 99-116

Ieuan JOLLY, *Data protection in United States : overview*, Practical Law, Multi-jurisdictionnal guide, 2014/15

Verne KOPYTOFF, *Privacy Audits Required of Internet Firms*, S.F. Chron, Mars 2013, http://www.sfgate.com/technology/article/Privacy-audits-required-of- Internet-firms-4343921.php

Caroline LANCELOT MILTGEN, *Vie privée et marketing, Etude de la décision de fournir des données personnelles dans un cadre comercial*, Réseaux, 2011, p.131-166

Winston J. MAXWELL et Christopher WOLF, *Protection des données personnelles : États-Unis et Europe convergent sur tout, ou presque*, Éditions multimédia économie numérique et nouveaux médias, édition juridique, numéro 55, avril 2012

Winston J. MAXELL, *The notion of fair processing in data privacy law*, Quelle protection des données personnelles en Europe ?, Université de Toulouse, 2015

Winston J. MAXWELL, *Principles-based regulation of personal data : the case of fair processing*, International Data Privacy Law, Volume 5 No. 3, Oxford university press, 2015 p. 205-216

Winston J. MAXWELL, *La protection des données à caractère personnel aux Etats-Unis : convergences et divergences avec l'approche européenne*, Le Cloud Computing, L'informatique en nuage, Société de législation comparée, 2013

Thimoty J. MURIS, *Cost of Completion or Diminution in Market Value : The relevance of subjective value*, 12 J. Legal Stud. 379 (1983)

Joseph P. NEHF, *Shopping for privacy online : consumer-decision making strategies and the emerging market for information privacy*, Journal of Law, Technology and Policy, volume 1, 2005

Jonathan A. OBAR, *Big Data and The Phantom Public : Walter Lippmann and the fallacy of data privacy self-management*, Big Data and Society, July-December 2015

Joseph PHELPS, Glenn NOWAK & Elizabeth FERRELL, *Privacy Concerns and Consumer Willingness to Provide Personal Information*, Journal of Public Policy and Marketing, volume 19, 2000

J. R. REIDENBERG et autres, *Disagreeable privacy policies : Mismatches between meaning and users' understanding*, Fordham law legal studies research paper, 2014, Consultable sur http:// papers.ssrn.com/sol3/Papers.cfm?abstract_id=2418297

Nora J. RIFON, Robert LaROSE, Sejung Marina CHOI, *Your Privacy is Sealed : Effects of Web Privacy Seals on Trust and Personal Disclosures*, The journal of consumer affairs, volume 39 issue 2, sept 2005

Ira S. RUBINSTEIN, *Regulating Privacy by design*, Berkeley Technology Law journal, Vol. 26, 2012, disponible sur http://ssrn.com/abstract=1837862

Michael D. SCOTT, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation : Has The Commission Gone Too Far ?*, Administrative Law Review, Vol. 60, No. 1, décembre 2008, p. 127-183

Daniel J. SOLOVE and Woodrow HARTZOG, *The FTC and the New Common Law of Privacy*, Columbia Law Rev. 583, 2014

Daniel J. SOLOVE, *A Brief History of Information Privacy* Law, in Proskauer on privacy, GW Law Faculty Publication & Other Works, PLI, 2006

Omer TENE, Jules POLONETSKY, *A theory of Creepy : Technology, Privacy and Shifting Social Norms*, 16 Yale Legal Journal & Technology, 2013

Stéphane TIJARDOVIC, *La protection juridique des données personnelles. Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique*, Les cahiers du numérique, 2003, p.185-203

Timothy TOBIN, *FTC ALJ : Embarrassment / Emotional Harm and Risk of Harm Does Not Satisfy "Substantial Consumer Injury" Prong of Unfairness*, Hogan Lovells, Chronicle of data protection, Consumer privacy, 17 novembre 2015, consultable sur http:// www.hldataprotection.com/2015/11/articles/consumer-privacy/ftc-alj-

embarrassmentemotional-harm-and-risk-of-harm-does-not-satisfy-substantial-consumer-injury-prong-of-unfairness/

Eduardo USTARAN, *EU General Data Protection Regulation : things you should know,* Privacy & Data Protection, Hogan Lovells, Volume 16, Issue 3, 2016

Li YUANGXIANG, Walter STEWART et autres, *Online Privacy Policy of the Thirty Dow Jones Corporations*, California State University San Bernardino USA, p. 65 - 89, 2012

Raymond WACKS, *Privacy in Cyberspace : Personal information, free Speech and the Internet,* in P. BIRKS, dir. publ. *Privacy and Loyalty,* Oxford, 1997

ARTICLES DE JOURNAUX

Joël IGNASSE, *Richard Stallman veut éliminer Facebook pour protéger la vie privée*, Sciences et Avenir High Tech, 16 mars 2016, consultable sur http://www.sciencesetavenir.fr/high-tech/informatique/20160316.OBS6588/richard-stallman-veut-eliminer-facebook-pour-proteger-la-vie-privee.html

Internet Business Newsweekly, *Consumer Watchdog Calls On FTC To Enact Do Not Track*, Says Force of Law Needed." 7 Mars 2011: 2. Business Insights: Essentials. Web. 2 June 2016.

Press Release, *FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, octobre 2011, consultable sur https://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout

Press Release, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, novembre 2011, consultable sur https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Press Release, Yahoo!, *Yahoo! Announces new privacy choice for consumers*, août 2008, consultable sur http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=327212

Gerry SMITH, *FTC: Google to Pay Record Fine over Safari Privacy Violation*, Huffington Post, Août 2012, consultable sur http://www.huffingtonpost.com/2012/08/09/ ftc-google-fine-safari-privacy-violation_n_1760281.html

Washington Post, *The national Nanny*, éditorial, 1er mars 1978

SITES INTERNETS

Site internet de l'organisme de certification TRUSTe : https://www.truste.com/business-products/apec-accountability/

Site officiel du barreau américain : http://apps.americanbar.org

Site officiel de la Commission Européenne sur le futur réglement européen sur les données personnelles : http://ec.europa.eu/justice/data-protection/reform/index_en.htm, dernière actualisation du 2 août 2016

Site du Conseil Européen et du Conseil de l'Union européenne : http:// www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/

Site officiel de la CNIL : https://www.cnil.fr

US Legal definitions : http://definitions.uslegal.com/c/consent-order/

AUTRES

APEC, *CBPRs System*, consultable sur http://www.cbprs.org/

Auteur anonyme, *Discover New Music with Spotify's Automagic Playlists*, Site internet make use of, consultable sur http://www.makeuseof.com/tag/discover-new-music-spotifys-automagic-playlists/

Auteur anonyme, *Dossier : 13 applis gratuites pour trouver et choisir le bon restaurant grâce à l'iPhone*, site internet iphon.fr, consultable sur http://www.iphon.fr/post/2011/02/18/Dossier-%3A-10-applications-iPhone-pour-trouver-le-restaurant-qu%E2%80%99il-vous-faut

Auteur anonyme, *La voiture connectée*, Site internet usine digitale, consultable sur http://www.usine-digitale.fr/voiture-connectee/

Jean-Louis BARMA, *À quoi rêvent les entreprises*, Épigraphe in Michel Houellebecq *Plateforme*, éditions Flammarion, Paris, 2001

CNIL, *La protection des données personnelles dans le monde,* carte consultable sur http://www.cnil.fr/linstitution/international/les-autorites-de-controle-dans-le-monde/

Roberto di COSMO, Reprenons le contrôle de nos données, point de vue publié dans le journal du CNRS, 14 avril 2015, consultable sur https://lejournal.cnrs.fr/billets/reprenons-le-controle-de-nos-donnees?utm_content=buffer5fa32&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Données personnelles, Big Data et droit individuels. Les différentes approches entre les différents systèmes juridiques, conférence, cycle entreprise et numérique, organisée par la Société de législation comparée, février 2016

Les données et la concurrence dans l'économie numérique, conférence organisée par l'Autorité de la concurrence, le 8 mars 2016, vidéos disponibles sur http://www.autoritedelaconcurrence.fr/user/rdv.php?id_rub=631

European Commission, *List of companies for which the EU BCR cooperation is closed*, consultation juillet 2016 sur http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Fil d'actualité du Service Informatique et libertés du CNRS, *Les 7 principes clés de la protection des données personnelles*, mise à jour le 18 janvier 2012, consultable sur http://www.cil.cnrs.fr/CIL/spip.php?article1390

Fil d'actualité du Service Informatique et libertés du CNRS, *Qu'est-ce qu'une donnée sensible ?*, consultable sur http://www.cil.cnrs.fr/CIL/spip.php?rubrique300

Anne Barbier GOLIRO, *Les Règles Contraignantes d'Entreprises (BCR), Enjeux juridiques et pratiques*, Thèse professionnelle réalisée à l'Institut Supérieur d'Electronique de Paris, consultable sur http://www.formationcontinue-isep.fr/images/stories/food/thesesIL/TPABG4

Groupe Daimler, *Protection des données et de la vie privée, le Code de conduite Daimler*, consultable sur www.mercedesbenz.ma/.../CodeOfConduct.../Code_of_Conduct_franz_2007.pdf

Groupe Gennerali, *Code de conduite*, approuvé le 14 décembre 2012, consultable sur http://institutionnel.generali.fr/sites/default/files/code_conduite_2014.pdf

Syndicat de la magistrature, *Privacy Shield : Alerte de l'observatoire des Libertés et du numérique*, communiqué de presse du 8 avril 2016

Christian PARDIEU, *Accountability & Data Protection, Données personnelles : Les impacts du futur règlement européen*, pour l'entreprise General Electric, AFDIT, consultable sur http://www.afdit.fr/media/pdf/20%20mars%202014/Accountability%20%20Data%20Protection%20Christian%20Pardieu%20GE%2020%2003%202014.pdf

The Information Accountability Foundation, *Accountability Agents*, consultable sur http://informationaccountability.org/category/accountability-agents/