La protection des données personnelles : présentation des approches européennes et américaines

Par Cécilia Darnault

Ulysse s'approche alors du cyclope : [...]
- Comment t'appelles-tu ?
- Je me nomme personne. [...]
Puis, ivre, le cyclope s'allonge et s'endort.
Ulysse et ses compagnons se précipitent sur le pieu qu'ils avaient taillé en l'absence du géant. Il est mis dans le feu, chauffé au rouge et enfoncé dans l'œil du cyclope. Polyphème pousse un hurlement qui se répercute au loin. Les Grecs se cachent au fond de la grotte tandis que d'autres Cyclopes, alertés par les cris de Polyphème, accourent.
- Que se passe-t-il ? demandent-ils du dehors. Qui t'attaque ?
- C'est personne ! personne ![1]

Personne. Qui, comme Ulysse, le héros mythique et très rusé de l'Odyssée d'Homère, peut encore prétendre n'être personne à l'ère de la révolution technologique ? Le XXI[ème] est celui de l'essor de l'intelligence artificielle qui, entre science-fiction et applications concrètes, fait d'ores et déjà partie de notre quotidien. De nos jours, l'identité d'Ulysse n'aurait pas pu échapper à Polyphème, dévoilée qu'elle eût été par les outils technologiques. Les traits de son visage auraient pu être décelés par un simple système de reconnaissance faciale, la spécificité de son timbre de voix par un algorithme de reconnaissance vocale, le caractère unique de ses empreintes digitales enregistré dans un fichier informatique…, tant d'éléments qui en révèlent bien plus qu'il n'y paraît et trahissent l'identité d'un individu à n'importe quel algorithme qui dispose de ces informations. Un mythe qui est réécrit dans une époque où nul n'aurait pu « entrevoir les téléphones perpétuellement géolocalisés, anticiper la publicité ciblée, imaginer l'internet des objets ou les réseaux sociaux »[2]. Certains craignant que cette civilisation de l'informatique ne devienne « celle de l'indiscrétion et de l'implacabilité, celle qui n'oublie, ni ne pardonne, qui enfonce le mur de l'intimité, enfreint la règle du secret de la vie privée, déshabille les individus »[3].

Plus concrètement, l'intelligence artificielle fait référence à un ensemble de théories et techniques (notamment une logique mathématique, des statistiques, des probabilités, la neurobiologie computationnelle et l'informatique) développant des programmes informatiques complexes capables de simuler certains traits[4] de l'intelligence humaine

[1] HOMERE, *L'Odyssée* [1955], trad. du grec ancien par Victor Bérard, Paris, Gallimard, 1993, 1136 p.
[2] NETTER Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », dans NETTER Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, Amiens, Centre de droit privé et de sciences criminelles d'Amiens – CEPRISCA, 2019, p. 5-31.
[3] FOYER Jean (rapporteur), *Projet de loi relatif à l'informatique et aux libertés*, Rapport n° 3125 (1977-1978), JO du 4 octobre 1977, p. 5782.
[4] MERABET Samir, *Vers un droit de l'intelligence artificielle*, Thèse de doctorat, Aix-en-Provence, Université d'Aix-Marseille, 2018, 558 p.

(raisonnement, apprentissage, etc.)[5]. Ces systèmes informatiques fonctionnent en analysant leur environnement et les données qui leur sont fournies et qui, par voie de conséquence, « ont besoin d'être nourris d'un grand nombre de données, impliquant des traitements massifs de données (que l'on appelle le big data) »[6]. Ainsi, la possibilité de « collecter et traiter d'immenses gisements de données numériques permet aujourd'hui de disposer d'outils d'analyse sophistiqués en mesure de délivrer, de manière inédite, des informations fines sur les comportements humains et la probabilité de leur apparition »[7]. Ces innovations techniques ne sont pas sans soulever certains questionnements ; l'accessibilité et l'utilisation de ces données faisant encore l'objet d'épineux débats que ce soit en matière économique, sociale ou juridique. En effet, la succession des révélations largement médiatisées relatives à l'exploitation abusive des données personnelles a permis de sensibiliser les individus sur l'utilisation qui peut être faite de leurs informations, et suscite un intérêt grandissant pour la protection des données personnelles auprès de l'opinion publique. Parmi ces scandales, comment ne pas mentionner l'onde de choc produite par les dénonciations d'Edward Snowden en 2013[8], relatives aux programmes de surveillance américains. Le célèbre lanceur d'alerte a dérobé des documents aux services secrets américains qui ont apporté

> La preuve de l'existence du plus grand réseau de surveillance et d'espionnage mondial dirigé et contrôlé par la NSA dont les pléthoriques ramifications s'étendent aussi bien aux discussions sur Facebook ou Skype de Mr Dupont ou Mr Smith qu'aux conversations téléphoniques de la chancelière allemande Angela Merkel, ou encore aux documents secrets du géant pétrolier brésilien Petrobras.[9]

Plus récemment et dans ce contexte, il est impossible de ne pas aborder le cas de l'entreprise Facebook, notamment suite aux déboires suscités lors de l'affaire dite *Cambridge Analytica*, au cours de laquelle l'entreprise a été accusée d'avoir utilisé les données de trente à soixante-dix millions d'utilisateurs, recueillies sans leur consentement, ensuite exploitées aux fins de démarchage politique ciblé dans le cadre de la campagne électorale américaine de 2016 remportée par Donald Trump[10]. Les dernières auditions de Mark Zuckerberg, fondateur et PDG de l'entreprise Facebook, devant le congrès des États-Unis, témoignent d'une prise de conscience importante au sein de la sphère politique sur la réalité du « marché » de la donnée personnelle et de ses utilisations. Des révélations qui ont indirectement attiré

> l'attention sur leur carburant : les données de géolocalisation, de navigation, les métadonnées de télécommunication, les publications sur les réseaux sociaux […] À ce moment-là, dans l'esprit du grand public, le concept de données personnelles passait brutalement du statut d'abstraction lointaine et inoffensive à celui de réalité quotidienne et menaçante [d'autant plus que] ces mêmes informations qui font parfois l'objet d'une surveillance publique à des fins de

---

[5] « L'IA : C'est quoi ? », *Portail du Conseil de l'Europe*, consulté le 11 octobre 2020 : https://www.coe.int/fr/web/artificial-intelligence/what-is-ai.

[6] DELMAS-LINEL Béatrice & Grégoire DUMAS, « L'impact du RGPD sur les innovations en matière d'IA », dans G'SELL Florence (dir.), *Le big data et le droit*, Paris, Dalloz, 2020, p. 207-217.

[7] G'SELL Florence (dir.), *Le big data et le droit*, Paris, Dalloz, 2020, 300 p.

[8] Voir notamment le documentaire de POITRAS Laura (réalisatrice), *Citizenfour*, 2015.

[9] PETINIAUD Louis, « Cartographie de l'affaire Snowden », *Hérodote*, Vol. 152-153, n°1, 2014, p. 35-42.

[10] AUDUREAU William, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », *Le Monde*, 22 mars 2018, consulté le 11 octobre 2020 : https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html.

> sécurité nationale sont par ailleurs la matière première d'une industrie privée qui les exploite à des fins lucratives.[11]

En tant que source de renseignements issus de la vie privée des individus (identité, comportements, habitudes, préférences, etc.), l'exploitation des données personnelles entre immanquablement en conflit avec certains des droits dont sont titulaires les personnes concernées. Pour prévenir les mésusages et les usages malintentionnés des données personnelles, et éviter qu'un algorithme ne se transforme en un outil discriminatoire ou d'atteinte aux droits fondamentaux des personnes, une intervention juridique était plus que nécessaire. Un encadrement législatif de la protection des données personnelles qui s'est plus ou moins manifesté, et de manière différente sur la surface du globe. L'ambition européenne consistant à

> protéger toute information concernant une personne physique (vivante) identifiée ou identifiable, notamment les noms, les dates de naissance, les photographies, les séquences vidéo, les adresses électroniques et les numéros de téléphone [, mais aussi d'autres informations telles que] des adresses IP et le contenu de communications se rapportant à des utilisateurs finaux de services de communication ou fournies par ces derniers sont également considérées comme des données à caractère personnel.[12]

Trouvant son origine dans le droit au respect de la vie privée, cette législation vise à « garantir le traitement (collecte, utilisation, stockage) loyal des données à caractère personnel tant par le secteur public que par le secteur privé »[13]. En témoigne la *Figure 1* ci-dessous représentant la protection des données personnelles dans le monde, réalisée par la CNIL, l'autorité administrative indépendante française de contrôle nationale relative à l'informatique, aux fichiers et aux libertés depuis 1978 :

[11] NETTER Emmanuel, « Le modèle européen de protection des données personnelles… », *op. cit.*, p. 11.
[12] « Protection des données », *Le contrôleur européen de la protection des données*, consulté le 11 octobre 2020 : https://edps.europa.eu/data-protection_fr.
[13] *Idem.*

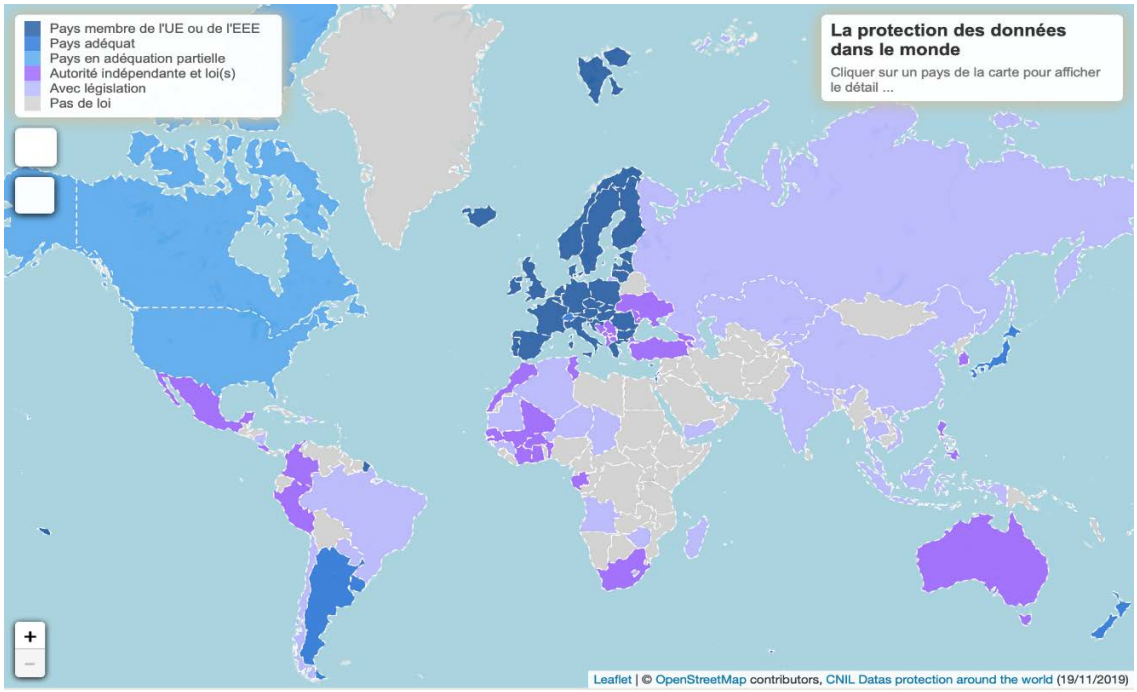

Figure 1: La protection des données dans le monde[14]

Bien que cette carte réalisée par un organisme français emporte nécessairement une perspective européiste de la protection des données personnelles, elle offre une visualisation intéressante des différents niveaux de protection en fonction des localités mondiales au regard des standards européens. En effet, « dans le sillon du règlement général sur la protection des données (RGPD) européen, des lois de même nature émergent dans d'autres régions du monde » ; par exemple, « l'État de Californie aux États-Unis, le Brésil, l'Inde et le Canada se sont récemment dotés de leur propre réglementation visant deux objectifs : protéger citoyens ou résidents, et responsabiliser les entreprises qui traitent leurs données personnelles »[15]. Une mosaïque de règlementations internationales, nationales voire régionales qui, convergent certes vers des objectifs communs, mais présentent chacune des spécificités locales emportant des différences notables d'une frontière à l'autre pour la protection des données de leurs citoyens et des ressortissants étrangers. Dans une conjoncture d'économie numérique mondialisée, de mobilité et d'échanges internationaux, une telle disparité n'est pas sans poser quelques difficultés. Dans le cadre de notre étude, nous allons particulièrement nous intéresser aux spécificités juridiques des cas de l'Union Européenne et des États-Unis. Deux parties du monde ayant adopté des stratégies législatives respectives qui reposent sur une philosophie et des régimes juridiques très différents. Les propos qui suivent ambitionnent ainsi de mettre en évidence deux approches transatlantiques politico-juridiques fondamentalement différenciées des données personnelles et de la protection des droits fondamentaux des personnes dans ce domaine.

L'intention de cet article consiste donc en *une présentation de droit comparé des régimes respectifs de protection des données personnelles entre les États-Unis et l'Union européenne*, cette dernière ayant

[14] « La protection des données dans le monde », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, consulté le 11 octobre 2020 : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

[15] VACHON Loïc, « Protection des données : Une mosaïque de réglementations, d'Europe au Canada, de Californie au Brésil », *Le Monde*, 20 avril 2019, consulté le 11 octobre 2020 : https://www.lemonde.fr/idees/article/2019/04/20/protection-des-donnees-une-mosaique-de-reglementations-d-europe-au-canada-de-californie-au-bresil_5452844_3232.html.

harmonisé la réglementation en la matière pour ses États membres. Cela pour mettre en avant les différences entre ces deux régimes et les conséquences qu'elles emportent pour les européens dont les données sont transférées outre-Atlantique. Pour traiter le sujet, cette étude s'intéressera à l'analyse des régimes respectifs de protection des données personnelles pour mettre en lumière tant les divergences fondées sur un traitement différencié de la protection des données personnelles (I) que pour entrevoir les changements respectifs de paradigme en cours afin de tendre vers une protection généralisée des données personnelles (II).

I – Les divergences transatlantiques de la protection des données personnelles

La protection des données personnelles ne se résume pas en une problématique purement juridique, mais elle « est intimement liée à l'histoire et à la culture d'un pays, aussi n'est-il pas surprenant que l'Union européenne et les États-Unis ne l'abordent pas de la même façon [16]» tant dans la manière de définir socialement les données personnelles, que dans l'élaboration d'un régime juridique de protection des individus concernés par ces informations.

A – Une profonde divergence philosophique

Entendu successivement par le Congrès américain et par le Parlement européen suite à l'affaire *Cambridge Analytica*, le célèbre dirigeant de Facebook déclarait que si tout le monde mérite une bonne protection des données, il faut également tenir compte des « sensibilités » de chaque pays sur ces sujets[17]. Si les raisons pécuniaires qui animent son discours sont potentiellement discutables, ses propos soulèvent un point pertinent ; celui de la sensibilité, autrement dit selon la perception de chacun. En effet, la comparaison de deux systèmes juridiques dans un domaine commence nécessairement par l'étude de *l'appréhension culturelle* de la notion étudiée. À ce titre, le concept de « donnée personnelle » emporte une acception totalement différente selon que l'on se situe à l'ouest ou à l'est de l'océan Atlantique.

Définies comme toute information se rapportant à une personne physique identifiée ou identifiable[18], les données à caractère personnel européennes sont de manière irréfragable un élément rattaché à la personne, à l'individu qu'elle concerne. La philosophie européenne consiste à considérer les données personnelles comme relevant d'éléments propres *attachés* à un individu dont l'exploitation, tolérée dans des conditions légales bien spécifiques, doit être encadrée afin de protéger les personnes non seulement au nom des droits fondamentaux, mais également au titre d'un ordre public spécial[19]. Matériellement, la protection des données à caractère personnel et le respect de la vie privée sont des droits fondamentaux majeurs liés,

[16] CASTETS-RENARD Céline, « L'intelligence artificielle, les droits fondamentaux et la protection des données personnelles dans l'Union européenne et les États-Unis », *Revue de Droit International d'Assas*, n°2, 2019, p. 158-174.

[17] LAUSSON Julien, « RGPD : vers une loi de protection des données personnelles aux USA ? », *Numerama*, 22 juin 2018, consulté le 11 octobre 2020 : https://www.numerama.com/politique/388051-rgpd-vers-une-loi-de-protection-des-donnees-personnelles-aux-usa.html.

[18] Règlement (UE) n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), JOUE L127 2 du 23/05/2018 (article 4).

[19] OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse de doctorat, Paris, Université Paris 1 Panthéon-Sorbonne, 2014, 763 p.

bien qu'au au fil des années le premier soit devenu un concept à part entière, un droit fondamental indépendant du second. L'agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe considèrent ainsi que

> tous deux tendent à protéger des valeurs similaires, à savoir l'autonomie et la dignité humaine des individus, en leur accordant une sphère privée dans laquelle ils peuvent librement développer leur personnalité, penser et se forger des opinions [, constituant] une condition préalable essentielle à l'exercice d'autres libertés fondamentales, telles que la liberté d'expression, la liberté de réunion et d'association pacifiques et la liberté de religion.[20]

Des droits protégés par le Parlement européen qui « a toujours insisté sur la nécessité de maintenir une approche équilibrée entre renforcement de la sécurité et sauvegarde des Droits de l'homme[21]». À ce titre,

> le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 [de la Convention européenne des droits de l'homme qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance] […]. Peu importe que les informations mémorisées soient ou non utilisées par la suite […]. Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu [un aspect] de la vie privée […], la Cour [européenne des droits de l'homme] tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés.[22]

Les données personnelles sont ainsi appréhendées dans l'Union européenne comme des informations constituant *une émanation des éléments protégés par les droits fondamentaux des personnes* ; à l'inverse de la culture économique américaine du marché de la donnée personnelle.

Il est peu dire que, sur ce point, les Américains ne sont pas sur la même longueur d'onde que les Européens. En effet, alors qu'en Europe les données personnelles relèvent des droits fondamentaux, aux États-Unis elles sont davantage considérées comme un *bien* commercialisable qui, mise à part des protections sectorielles spécifiques, se rattache principalement à l'individu à travers son statut de consommateur[23]. « Nouvel or noir de l'internet et nouvelle monnaie du monde digital »[24], elles représentent la genèse de la valorisation économique de l'information et constituent la matière première essentielle des modèles économiques mis en place par les géants du numérique tout autour du globe.

---

[20] Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données personnelles*, Luxembourg, Office des publications de l'Union européenne, 2019, p. 21.

[21] Cour Européenne des Droits de l'Homme, « Protection des données personnelles », *Unité de la Presse – Cour européenne des droits de l'homme*, septembre 2020, consulté le 11 octobre 2020 : https://www.echr.coe.int/documents/fs_data_fra.pdf.

[22] CEDH 4 décembre 2008, S. et Marper c. Royaume-Uni, Requêtes nos 30562/04 et 30566/04.

[23] LAZAREGUE Alexandre, « RGPD : Les Américains considèrent la donnée personnelle comme un simple bien commercialisable », *Le Monde*, 20 janvier 2020, consulté le 11 octobre 2020 : https://www.lemonde.fr/idees/article/2020/01/20/rgpd-les-americains-considerent-la-donnee-personnelle-comme-un-simple-bien-commercialisable_6026550_3232.html.

[24] KUNEVA V. M., Commissaire Européen à la Consommation, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling (31 mars 2009), citée dans *Personal Data : the emergence of a new asset class*, World Economic Forum, janvier 2011, p. 5 ; DELTORN Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », *Revue des Droits et Libertés Fondamentaux*, 2017, consulté le 11 octobre 2020 : http://www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/.

Un adage veut que si vous ne payez pas, vous êtes le produit. Dans un rapport, l'ONG Amnesty International dénonce ce modèle économique de « capitalisme de surveillance »[25], fondé sur la collecte des données personnelles des utilisateurs pour des publicités ciblées, utilisant ainsi ces données pour manipuler et influencer les utilisateurs au profit des annonceurs[26]. Un marché qui fait du profit à travers l'exploitation des données humaines à une échelle industrielle, ayant généré des milliers de milliards de dollars, faisant des entreprises du secteur les plus riches jamais connues de l'humanité[27]. Des modèles économiques basés sur l'exploitation publicitaire de la collecte des données personnelles qui font grincer des dents en Europe ; mais l'*ethos* libéral des États-Unis fait que l'idée qu'un consommateur soit un produit que des entreprises commerciales peuvent vendre semble beaucoup mieux acceptée politiquement. À l'opposé de la culture juridique européenne du droit fondamental à la protection des données personnelles, l'approche américaine attribue un caractère commercial aux données collectées qui, en dehors de zones de protection spécifiques, peuvent librement être exploitées par les entreprises. Au regard de ce caractère commercial, les Américains ne protègent pas les personnes concernées par les données personnelles collectées au titre de la protection des droits fondamentaux, mais en vertu des droits reconnus aux consommateurs. Alors que l'Europe a étendu les droits compris dans la protection des droits de l'Homme, « au fil des années, la Commission fédérale du commerce (*Federal Trade Commission*, plus loin FTC) a étendu le concept de "pratique déloyale" pour inclure tout traitement de données à caractère personnel incompatible avec les attentes légitimes du consommateur »[28]. La FTC est une agence fédérale indépendante et dont les compétences vont bien au-delà de la protection de la vie privée (lutte contre les monopoles, la concurrence déloyale et la publicité mensongère, protection des consommateurs, répression des fraudes, etc.)[29]. Initialement créée pour protéger le consommateur, son rôle accru dans la protection des données personnelles s'est amplement développé. Elle a pour mission d'informer le consommateur sur la collecte, l'utilisation et le partage de ses données personnelles et condamnant « cinq types de comportements : les changements rétroactifs en matière de confidentialité, les pratiques pour installer des logiciels espions, l'utilisation inappropriée des données, la collecte illicite d'informations, et les pratiques déloyales en matière de sécurité »[30]. Récemment, elle a particulièrement fait parler d'elle en sanctionnant lourdement l'entreprise Facebook, lui infligeant une amende record d'un montant de cinq milliards de dollars pour ses manquements aux principes susmentionnés[31]; les conditions générales d'utilisation du réseau social étant qualifiées en tant que contrats de consommation.

---

[25] Formulation théorisée par le Pr. Shoshana Zuboff, dans « *The Social Dilemma* », documentaire réalisé par Jeff Orlowsk ; ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, New York, Zulma, 2020, 864 p.

[26] Amnesty International, « La surveillance intrusive exercée par Facebook et Google : un danger sans précédent pour les droits humains », *Amnesty International*, 21 novembre 2019, consulté le 11 octobre 2020 : https://www.amnesty.org/fr/latest/news/2019/11/google-facebook-surveillance-privacy/.

[27] Interview du Pr. Shoshana Zuboff, dans ORLOWSK Jeff (réalisateur), « *The Social Dilemma* », 2020.

[28] MAXWELL Winston J., « La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne », *Le cloud computing*, p. 71-78.

[29] DÉTRAIGNE Yves & Anne-Marie ESCOFFIER, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », *Senat.fr*, 27 mai 2009, consulté le 11 octobre 2020 : https://www.senat.fr/rap/r08-441/r08-44128.html.

[30] VERMERSCH Léa, « La protection des données personnelles aux États-Unis, une approche différente de l'Europe », *Économie numérique*, 18 février 2019, consulté le 11 octobre 2020 : http://blog.economie-numerique.net/2019/02/18/la-protection-des-donnees-personnelles-aux-etats-unis-une-approche-differente-de-leurope/.

[31] United States District Court for the District of Columbia, Stipulated Order for Civil Penalty, Monetary Judgment, and Injuctive Relief, United States vs Facebook Inc., July 24, 2019, n° 19-cv-2184.

Matériellement, la FTC s'appuie sur une ordonnance de 2012[32] qui faisait déjà suite à une enquête menée sur les pratiques de Facebook concernant l'utilisation des données personnelles de ses utilisateurs. Juridiquement cette ordonnance reprochait notamment

> au réseau social de ne pas avoir respecté les choix de configuration effectués par ces derniers. Des informations normalement qualifiées de "privées" ou "réservées" aux amis avaient ainsi été divulguées ou partagées avec des applications tierces sans que leurs titulaires en soient informés. Le recoupement et l'analyse de ces données permettaient de dégager potentiellement d'autres informations telles que les opinions politiques, la vie sexuelle ou les croyances religieuses, ce qui constitue autant d'atteintes aux droits fondamentaux.[33]

Qualifiant les faits reprochés en tant que pratiques déloyales et trompeuses, la FTC avait ainsi enjoint Facebook « de délivrer une information précise et fiable quant à l'utilisation de leurs données personnelles et d'obtenir leur consentement préalable à tout partage de ces mêmes données avec des applications et entreprises partenaires »[34]. La récente décision vient sanctionner le non-respect des obligations de mise en conformité issues de l'accord de 2012 par le réseau social, tenant compte des précédents avertissements, pour pratiques commerciales trompeuses.

De fait, en pratique, si les approches européennes et américaines marquent une divergence profonde dans la conception des données à caractère personnel et dans la philosophie juridique qui régit leur protection, chacun dispose respectivement d'outils juridiques pour protéger tant les droits fondamentaux des européens que les droits des consommateurs américains en la matière.

B – Une divergence juridico-systémique

Au-delà d'une simple divergence philosophique, la protection des données s'inscrit dans un contexte juridique historiquement dissemblable. En effet, les systèmes juridiques respectifs de l'Union européenne et des États-Unis sont marqués par un clivage historique entre les deux modèles juridiques traditionnels, mis à part le droit coutumier ou religieux, l'un dit de *civil law* et l'autre de *common law*[35]. Le premier fait référence au fonctionnement juridique en vigueur dans la majorité des pays européens, repris pour la construction de l'Union européenne, et désigne un système juridique caractérisé par un fort élément de codification où le droit écrit d'expression législative constitue la principale source de droit[36]. À l'inverse, « les pays sous la Common law sont les anciennes colonies ou les anciens protectorats britanniques y compris les États-Unis[37]» et répondent à un système qui résulte non de textes législatifs codifiés, mais de la pratique des juridictions[38], les juges ayant un rôle prépondérant dans la création du droit. Au prisme de cette différenciation entre les régimes juridiques de

---

[32] United States of America – Federal Trade Commision, Decision and Order in the matter of Facebook Inc., August 10, 2012, n° C-4365.

[33] MOURON Philippe, « Une amende record de 5 milliards de dollars prononcée par la FTC contre Facebook », *La revue européenne des médias et du numérique*, automne 2019, consulté le 11 octobre 2020 : https://la-rem.eu/2019/12/une-amende-record-de-5-milliards-de-dollars-prononcee-par-la-ftc-contre-facebook/.

[34] *Idem.*

[35] BLONDEEL Jean, « La Common Law et le droit civil », *Revue Internationale de Droit Comparé*, Vol. 3, n°4, octobre-décembre 1951, p. 585-598.

[36] « Civil Law » : GUINCHARD Serge & Thierry DEBARD (dir.), *Lexique des termes juridiques*, Paris, Dalloz, 22ème éd, 2014, p. 179.

[37] AVGOUSTI Christina, « Common law ou droit civil, est-ce que cela importe ? », *Le Petit Juriste*, 8 juillet 2015, consulté le 11 octobre 2020 : https://www.lepetitjuriste.fr/common-law-ou-droit-civil-est-ce-que-cela-importe/.

[38] « Common Law » : GUINCHARD Serge & Thierry DEBARD (dir.), *Lexique des termes juridiques*, *op. cit.*, p. 208.

l'Union européenne et des États-Unis, il n'est donc pas surprenant que les modèles choisis en matière de protection des données personnelles divergent sur la forme de chaque côté de l'Atlantique.

En effet, l'Europe qui se targue d'être à l'avant-garde mondiale de la protection des données et souhaiterait exporter son modèle au-delà de ses frontières, a opté pour un modèle civiliste de régulation globale en se dotant d'une législation générale. À ce titre, les normes de l'Union européenne (UE) en matière de protection des données reposent essentiellement

> sur la Convention 108 du Conseil de l'Europe, sur les instruments de l'UE – y compris le Règlement général sur la protection des données et la Directive relative à la protection des données destinées aux autorités policières et judiciaires pénales – ainsi que sur la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne dans ce domaine.[39]

Plus précisément, la Convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel fut le premier instrument international juridiquement contraignant adopté dans le domaine[40]. Elle visait à garantir à toute personne physique le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. Une protection reprise dans la directive 95/46/CE du 24 octobre 1995[41] ayant pour vocation d'imposer aux États membres l'obligation de garantir le droit à la vie privée des personnes physiques à l'égard du traitement de leurs données à caractère personnel, en vue de permettre une libre circulation de ces données entre les États membres. L'article 29 de la directive a notamment instauré un groupe de travail (dit G29) qui a émis, sous l'empire de ce texte, des recommandations en la matière. Les données personnelles sont également protégées par les droits fondamentaux ; dont l'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposant que toute personne a droit à la protection des données à caractère personnel la concernant. Une reconnaissance réitérée par la Cour européenne des droits de l'homme (CEDH) qui considère que par principe, le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la Convention européenne des droits de l'homme, au nom du respect de la vie privée et familiale, du domicile et de la correspondance, peu importe que les informations mémorisées soient ou non utilisées par la suite[42]. La protection des données à caractère personnel est ainsi envisagée, disons même élevée en tant que droit fondamental de l'Homme. Un régime global, complété ponctuellement par divers instruments législatifs complémentaires propres à certains secteurs spécifiques, qui trouve son apogée avec l'adoption du règlement général sur la protection des données (RGPD)[43] entré en application en 2018. Ce texte vise à « protéger tous les citoyens européens contre les violations de la vie privée et des données à caractère personnel dans un

---

[39] Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, « *Manuel de droit européen ... », op. cit.*, p. 3.

[40] « La protection des données à caractère personnel », *Fiches techniques sur l'Union européenne*, 2020, consulté le 11 octobre 2020 : https://www.europarl.europa.eu/ftu/pdf/fr/FTU_4.2.8.pdf.

[41] 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, J.O. n° L 281 du 23/11/1995, pp. 31-50.

[42] Cour Européenne des Droits de l'Homme, « Protection des données personnelles », *op. cit.*

[43] Règlement (UE) n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), JOUE L127 2 du 23/05/2018.

monde de plus en plus numérique et il met aussi en place un cadre plus clair et plus cohérent pour les entreprises »[44]. Parmi les droits dont jouissent les citoyens figurent le

> consentement, déclaré par un acte positif clair, au traitement de leurs données à caractère personnel, le droit de recevoir des informations claires et compréhensibles à ce sujet, le droit à l'oubli (tout citoyen peut demander l'effacement de ses données), le droit de transférer leurs données à un autre fournisseur de services (par exemple lors du passage d'un réseau social à un autre) et le droit d'être informés lorsque leurs données ont été piratées.[45]

À l'inverse de cette protection générale adoptée par l'Union européenne pour fournir un cadre global de la protection des données personnelles applicable par tous ses pays membres, et les pays tiers exploitant les données des ressortissants européens, l'approche américaine a opté pour une méthode différente.

Outre l'application du modèle de *common Law*, les États-Unis disposent également d'un système juridique à deux échelons constitués d'un niveau fédéral et d'une certaine autonomie propre aux États fédérés, qui explique en partie l'approche sectorielle, plutôt qu'un régime généralisé à l'image des Européens, adoptée par les Américains en matière de protection des données personnelles[46]. En effet, le droit américain utilise des instruments juridiques différents qui forment des éléments de protection relativement éparpillées en fonction du niveau juridico-institutionnel et des domaines considérés comme relevant ou non d'une « zone de protection ». Contrairement à l'Europe qui protège l'individu *per se* contre toute forme d'atteinte, le « droit américain ne dispose pas d'un texte unique, il a au contraire tendance à réguler les atteintes aux données personnelles par catégorie d'individus, par domaines et par secteur d'activités »[47]. Outre la protection accordée aux consommateurs par la FTC sur le fondement des pratiques déloyales abordées précédemment, les États-Unis ont mis en place d'autres mesures. Au niveau fédéral déjà, le 4ème amendement accorde une protection constitutionnelle de la vie privée en mentionnant que

> le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et leurs effets contre les perquisitions et saisies non motivées ne sera pas violé et il ne sera émis aucun mandat si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration solennelle et décrivant avec précision le lieu à perquisitionner et les personnes ou choses à saisir.[48]

Une protection qui est limitée aux seules atteintes du gouvernement fédéral, consacrée dans l'affaire *Schmerber* c. *Californie* de 1966, par laquelle la Cour suprême des États-Unis d'Amérique déclare que la « fonction primordiale du Quatrième amendement est de protéger la vie privée et la dignité contre l'intrusion injustifiée de l'État »[49]. Le principe est complété ensuite en 1973 par l'adoption du *Code of Fair Information Practices* qui

> a identifié les cinq pratiques ou principes suivants : interdiction des systèmes secrets d'enregistrement des données, possibilité d'accès pour l'individu à ces informations, principe

---

[44] « La protection des données à caractère personnel », *Fiches techniques sur l'Union européenne*, p. 3.
[45] Cour Européenne des Droits de l'Homme, « Protection des données personnelles », *op. cit.*
[46] Sur ces différences voir : BIGNAMI Francesca & Giorgio RESTA, « Transatlantic Privacy Regulation: Conflict and Cooperation », *Law and Contemporary Problems*, Vol. 78, n°2015-52, 2015, p. 231-266.
[47] MARTIN Alexandre, « Privacy Shield : Comment protéger les données de votre entreprise aux États-Unis », *Village de la Justice*, 28 novembre 2019, consulté le 11 octobre 2020 : https://www.village-justice.com/articles/privacy-shield-comment-proteger-les-donnees-votre-entreprise-aux-etats-unis,33067.html?page=article&id_article=33067.
[48] Traduction libre. Congrès des Etats-Unis, *Bill of Rights* [1789], IVème amendement, 25 mars 2021, consulté le 11 octobre 2020 : https://www.archives.gov/founding-docs/bill-of-rights-transcript.
[49] Supreme Court of the United States, *Schmerber c. Californie*, 384 U.S. 757, 767, 1966.

> de limitation de la finalité (sauf accord préalable), possibilité de correction des informations, principe de sécurité des informations[50];

et du *Privacy Act* en 1974[51], législation principale couvrant le traitement des données par les agences gouvernementales, qui reprend, entre autres mesures, les principes énoncés en 1973. Cependant, « la protection des données personnelles proprement dite repose essentiellement sur des règles sectorielles spécifiques à certaines activités, selon des finalités déterminées, poursuivies par des opérateurs désignés »[52] ; notamment le *Health Insurance Portability and Accountability Act* (1996) pour le domaine de la santé, le *Children's Online Privacy Protection Act* (1998) visant la protection des données concernant les enfants, le *Fair Credit Reporting Act* (1970) et le *Fair and Accurate Credit Transactions Act* (2003) dans le secteur bancaire, etc.

Par ailleurs, il est important de souligner que la protection fédérale coexiste avec une intervention législative au niveau des États fédérés. Généralement de manière complémentaire, les droits constitutionnels respectifs des États assurent un droit au respect de la vie privée. À ce titre, l'article premier de la Constitution californienne prévoit que « tout individu est par nature libre et indépendant et possède des droits inaliénables » faisant notamment référence à la défense de la vie et de la liberté, la protection des biens, la sécurité, le respect de la vie privée, etc[53]. De plus, si la Constitution fédérale protège la vie privée individuelle à l'encontre du gouvernement,

> la protection à l'égard d'acteurs privés est reconnue au sein de la common law de chaque État, et notamment dans la jurisprudence en matière de responsabilité civile […] appelées « privacy torts », ces règles protègent l'individu contre des incursions dans sa « sphère de vie privée », et couvre notamment la publication de faits relevant de la vie privée, ou de photographies sans le consentement des personnes intéressées.[54]

Le droit américain de la protection des données personnelles doit donc s'appréhender comme un patchwork de réglementations diversifiées, traitant le sujet au cas par cas en fonction des règles propres au secteur et à la localisation de l'atteinte éventuelle. De ce fait,

> une telle approche, empruntée de libéralisme, tend à ne prôner une intervention législative qu'en présence de dysfonctionnements sur un marché ou en cas de risques importants pour la protection des individus [, et emporte une différence systémique qui] constitue la pomme de discorde majeure entre l'Union européenne et les États-Unis, ayant conduit la Commission européenne à considérer que le niveau de protection fourni par le droit fédéral n'est pas "adéquat" au sens de l'article 25 de la directive (UE) 95/46 (désormais article 45 du RGPD).[55]

---

[50] BELLANOVA Rocco & Paul DE HERT, « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », *Cultures & Conflits*, n°74, Été 2009, consulté le 11 octobre 2020 : http://journals.openedition.org/conflits/17429.

[51] Privacy Act (loi sur la protection de la vie privée), 5 U.S.C. § 552a, 1974.

[52] CASTETS-RENARD Céline, « L'intelligence artificielle, les droits fondamentaux… », *op. cit.*, p. 164.

[53] BELLANOVA Rocco & Paul DE HERT, « Protection des données personnelles ... », *op. cit.*.

[54] MAXWELL Winston J., « La protection des données à caractère personnel ... », *op. cit.* ; WARREN Samuel D. & Louis D. BRANDEIS, « The Right to Privacy », *4 Harv. L. Rev. 193* (1890) ; PROSSER William L., « Privacy », *48 Calif. L. Rev. 383*, 383 (1960).

[55] CASTETS-RENARD Céline, « L'intelligence artificielle, les droits fondamentaux ... », *op. cit.*, p. 164.

II – Les convergences transatlantiques de la protection des données personnelles

Malgré cette divergence d'approches philosophiques qui se traduit par l'adoption de régimes juridiques fondamentalement différenciés en matière de protection des données personnelles d'un côté et de l'autre de l'Atlantique, des convergences entre les deux modèles juridiques commencent à émerger. Cependant, et dans l'attente d'un niveau de protection jugé équivalent par les institutions européennes, l'Union européenne et les États-Unis travaillent ensemble à encadrer les traitements des données européennes transférées sur le territoire américain de manière à répondre à des exigences minimales requises en droit de l'Union.

A – L'émergence d'une concordance transatlantique

L'Union européenne et les États-Unis s'inscrivent dans une profonde divergence juridico-institutionnelle en matière de protection des données personnelles qui semble manifestement irréductible. Pourtant, l'adoption du « nouveau règlement européen sur la protection des données personnelles signe l'amorce d'une convergence entre les deux systèmes »[56]. En effet, ce dernier constitue une réforme majeure du droit de la protection des données personnelles, tant en Europe qu'à l'étranger, par la dynamique de prise de conscience inédite et l'inspiration qu'il a suscité, notamment aux États-Unis, et permet d'entrevoir l'amorce d'un cheminement commun en la matière. Plus concrètement, l'adoption européenne du RGPD

> entraîne un basculement d'un régime administratif de formalités préalables à un régime de conformité globale dans le cadre duquel les entreprises et les organismes traitant des données doivent être en mesure de démontrer à tout moment qu'ils respectent les principes du Règlement.[57]

Ce basculement vers un régime de conformité permet de créer un *pont transatlantique* alliant l'approche européenne du droit fondamental à la protection des données personnelles attaché à l'individu et la philosophie économique libérale américaine en s'adressant directement aux acteurs privés. En pratique, le corpus de règles européen introduit une gouvernance de la protection des données personnelles à travers une approche dite de « *compliance* », *via* le concept d'*accountability*, c'est-à-dire de conformité par la responsabilisation des acteurs[58], qui symbolise ce changement de paradigme. Ce principe se traduit notamment par l'exercice des contrôles *a posteriori* et par un pouvoir de sanction potentiellement dissuasif. Cela se matérialise par « la définition de politiques de protection des données et de sécurité des systèmes d'information, d'un registre des activités de traitement et des violations de données et par la prise en compte des principes de *Privacy by design* et *Privacy by default* »[59]. Ces derniers, élaborés par la Commission à l'information et à la protection de la vie privée de l'Ontario et repris par le RGPD[60], consistent en l'intégration de la protection des données

---

[56] POZZO DI BORGO Valérie & Jérôme COUZIGOU, « Données personnelles aux États-Unis et dans l'UE : vers une convergence des règles de protection ? », dans « RGPD : quelques mois pour se mettre en conformité ! », *Revue Banque.fr*, n°810, 28 juin 2017, consulté le 11 octobre 2020 : http://www.revue-banque.fr/risques-reglementations/article/donnees-personnelles-aux-etats-unis-dans-ue-vers-u.

[57] BANCK Aurélie, *RGPD : la protection des données à caractère personnel, 19 fiches pour réussir et maintenir votre conformité*, Paris, Lextenso, 2020, p. 4.

[58] FAUVARQUE-COSSON Bénédicte & Winston J. MAXWELL, « Protection des données personnelles », *Recueil Dalloz,* décembre 2016 - mai 2018, p. 1033.

[59] BANCK Aurélie, *RGPD : la protection des données à caractère personnel*, *op. cit*., p. 29.

[60] *Ibid*., p. 31.

par défaut dès la conception des produits et services.

Ce rapprochement par la responsabilisation qui s'exerce également grâce à l'approche par les risques introduite à travers le mécanisme d'analyse d'impact du paragraphe 7 de l'article 35 du Règlement, suivant les lignes directrices élaborées par le G29, permettant d'adopter une démarche pour la limitation des atteintes graves pour la vie privée des personnes[61] et mettant l'accent sur la responsabilisation des acteurs économiques. Ces principes sont directement inspirés des mécanismes de régulation anglo-saxons qui favorisent un système d'accompagnement et de coopération, en lieu et place d'un système d'analyse et d'autorisation de traitement, coûteux en moyens institutionnels et en temps, préconisant ainsi davantage la confiance par une mise en conformité structurelle des organisations de manière autonome.

Par ailleurs, une volonté commune de privilégier une approche sectorielle adaptée aux contraintes et spécificités des grands secteurs de la vie économique se renforce. En effet, les réglementations juridiques européennes et américaines convergent quant à l'utilisation d'instruments de co-régulation destinés à rendre les processus de protection des données personnelles plus adaptés ou à apporter des garanties outre-Atlantique. Ces outils permettent, entre autres, d'instituer des standards de protection, à travers des autorités de régulation, accueillis de manière plus légitime, et donc mieux appliqués par les acteurs privés. La sectorialisation se traduit, par exemple, par la possibilité prévue par le Règlement européen d'instituer des codes de conduites pour un secteur d'activité donné ou pour adapter ses préconisations aux besoins spécifiques des différentes structures organisationnelles des entreprises[62]; ou bien par la mise en place de mécanismes de certification[63] en matière de protection des données personnelles – des outils permettant à un acteur économique de valoriser sa mise en conformité pour la protection de la vie privée de ses utilisateurs, ou consommateurs. Mais d'autres instruments sont également utilisés, notamment dans le cadre d'une co-régulation interétatique, visant les cas de transfert de données transfrontaliers hors de l'Union européenne. Cependant, les autorités de protection des données personnelles en Europe restent méfiantes à l'égard des mesures américaines. Pour y remédier, d'autres outils sont mobilisés, à l'instar des règles d'entreprises contraignantes (ou *Binding corporate rules* en anglais, BCR), qui permettent à des groupes d'entreprises, notamment multinationales, d'encadrer juridiquement leurs transferts de données hors de l'Union européenne tout en leur offrant la possibilité d'engager une démarche de mise en conformité globale à l'échelle de tout le groupe[64]. Ces outils permettent d'assurer des transferts de données hors UE, transferts comportant une garantie appropriée au sens du Règlement[65] pour les ressortissants européens et également utilisés par les entreprises comme une preuve de la mise en conformité de leur organisation en la matière. Dans le même ordre d'idée, les accords transactionnels de la FTC (*Federal Trade Commission*) ne sont pas en reste. En effet,

> en plus d'augmenter les pouvoirs de sanction de la FTC, les accords transactionnels permettent à la FTC d'imposer des obligations détaillées en matière de protection des données

[61] TANGHE Hélène & Paul-Olivier GIBERT, « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales*, n°4, 2017, p. 79-93.
[62] Règlement (UE) n°2016/679 du 27 avril 2016, *op. cit.* (article 40 et s.).
[63] *Ibid* (article 42 et s.).
[64] « Ce qu'il faut savoir sur les règles d'entreprise contraignantes », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, 7 février 2020, consulté le 11 octobre 2020 : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr.
[65] Règlement (UE) n°2016/679 du 27 avril 2016, *op. cit.* (article 46.2(b)).

personnelles [dans la mesure où] un accord transactionnel avec la FTC peut devenir un mini-RGPD qui lie l'entreprise pendant 20 ans, la durée habituelle de ces accords.[66]

Par exemple, l'accord du 24 juillet 2019[67] oblige Facebook à obtenir le consentement explicite de l'utilisateur avant toute utilisation de ses données de reconnaissance faciale, ou de tout partage de son numéro mobile avec des tiers ; à mettre en place un comité d'administrateurs indépendants pour contrôler l'application de l'accord au sein de l'entreprise ; à modifier les statuts de l'entreprise pour garantir que son PDG n'a pas le pouvoir seul de licencier les personnes chargées de contrôler les obligations de Facebook à l'intérieur de l'entreprise ; à documenter l'ensemble de ses mesures prises pour réduire les risques ; et à effectuer un audit tous les deux ans par un auditeur indépendant, en plus des obligations initialement convenues à la charge de l'entreprise dans l'accord de 2012.

Mais les outils de co-régulation ne sont pas les seuls instruments de rapprochement juridique entre l'Europe et les États-Unis en matière de protection des données personnelles. Il s'avère effectivement que « des signes de convergence apparaissent également du côté des États-Unis, qui semblent vouloir développer une nouvelle approche de la vie privée, plus proche de la conception européenne »[68]. Depuis les dernières révélations qui ont fait esclandre, la sphère politique américaine s'intéresse au sujet avec une attention toute particulière. Parmi d'autres, le projet de loi fédéral *Consent Act* (*Customer Online Notification for Stopping Edge-provider Network Transgressions*) vise, par exemple, à obliger la FTC à mettre en œuvre toute mesure nécessaire pour assurer la protection de la vie privée des consommateurs américains contre l'arbitraire des plateformes numériques telle que Facebook. Un projet qui a notamment pour objet de renforcer l'obligation de recueil du consentement explicite et éclairé des internautes avant tout traitement de leurs données, à l'image du RGPD européen[69]. De plus, alors que le Congrès américain envisagerait de se doter d'une loi fédérale[70], la Californie a adopté sa propre législation inspirée du RGPD européen, alliant la reconnaissance de nouveaux droits pour les consommateurs et, *a contrario*, de nouvelles obligations pour les entreprises qui collectent des données personnelles. Le fameux « RGPD californien »[71], nommé ainsi par les journalistes et entré en application au 1er janvier 2020, reprend certains droits proches de ceux consacrés par le Règlement européen, à l'image du droit à recevoir une information, des droits d'accès, de suppression, d'opposition ou de portabilité de leurs données ; ayant pour objectif de permettre aux personnes de savoir si des

---

[66] MAXWELL Winston J., « Amende contre Facebook : comment la FTC américaine s'est transformée en super CNIL », *Institut Mines-Telecom*, 2 octobre 2019, consulté le 11 octobre 2020 : https://blogrecherche.wp.imt.fr/2019/10/02/amende-contre-facebook-ftc-super-cnil/.

[67] United States of America Federal Trade Commission, Washington, DC 20580, Déclaration du Président Joe Simons et des commissaires Noah Joshua Phillips et Christine S. Wilson In re Facebook, 24 juillet 2019 : https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf.

[68] CASTETS-RENARD Céline, « Quels liens établir avec les US et l'UE en matière de vie privée et de protection des données personnelles ? », *Dalloz IP/IT*, n°3, mars 2016, p. 115.

[69] JURILEXBLOG, « Vers un RGPD américain ? », *Haas Avocats*, consulté le 11 octobre 2020 : https://www.haas-avocats.com/actualite-juridique/vers-un-rgpd-americain/.

[70] MEDIAVILLA Lucas, « Loi sur les données personnelles : la Californie ouvre le bal aux États-Unis », *Les Échos*, 2 janvier 2020, consulté le 11 octobre 2020 : https://www.lesechos.fr/tech-medias/hightech/loi-sur-les-donnees-personnelles-la-californie-ouvre-le-bal-aux-etats-unis-1160009.

[71] RENOUARD Guillaume, « Le "RGPD californien", une loi modèle, exportable au reste des États-Unis », *La Tribune*, 22 janvier 2020, consulté le 11 octobre 2020 : https://www.latribune.fr/economie/international/le-rgpd-californien-une-loi-modele-exportable-au-reste-des-etats-unis-840240.html ; BOHIC Clément, « La Californie se dote de son RGPD sans attendre les États-Unis », *Silicon.fr*, 2 janvier 2020, consulté le 11 octobre 2020 : https://www.silicon.fr/californie-rgpd-etats-unis-331285.html.

informations personnelles sont collectées à leur sujet et surtout vendues par la suite[72]. Cela dit, la philosophie intrinsèque de la législation californienne reste relativement différente de celle du Règlement européen. Une fois de plus, le texte ne s'adresse qu'aux seuls consommateurs et ménages californiens, restreignant considérablement son champ d'application ; il ne reprend pas non plus « le principe d'*accountability*, de *privacy by design*, et ne prévoit pas d'obligation de désigner un DPO ou de tenir un registre de traitements, comme le RGPD »[73]. Ainsi, malgré une volonté manifeste de faire évoluer la protection des données personnelles aux États-Unis et l'amorce d'une convergence juridique instrumentale, le chemin à parcourir en ce sens reste encore long.

B – Les tentatives d'adoption d'un régime bilatéral

Si les dernières évolutions législatives américaines sont notables, et porteuses d'espoir dans le domaine, considérant qu'une majeure partie des superpuissances actuelles du numérique sont localisées sur ce territoire, il s'avère qu'au regard des Européens, des failles majeures et non tolérables persistent dans la législation américaine. À vrai dire, si l'Europe s'intéresse de près aux tenants et aux aboutissants de la protection des données personnelles dans le monde, s'estimant précurseur en la matière, sa priorité reste la protection de ses ressortissants et de leurs informations personnelles, sur son territoire comme en dehors de ses frontières. Ainsi, « la sauvegarde des droits des personnes concernées en cas de transfert de leurs données en dehors de l'UE permet à la protection conférée par le droit de l'UE de rester attachée aux données à caractère personnel en provenance de l'Union »[74]. Matériellement, en dehors de l'Union européenne, les transferts de données doivent respecter le principe selon lequel le pays destinataire des données doit garantir un « niveau adéquat de protection[75]» alors que, pour leur part, les États-Unis n'ont pas limité les transferts externes de données personnelles collectées sur leur territoire à l'extérieur de leurs frontières. Bien que l'actualité relative au réseau social TikTok, filiale de l'entreprise chinoise ByteDance, menacée d'interdiction aux États-Unis par le gouvernement Trump, soulève la problématique de la protection des données américaines vis-à-vis d'une utilisation par des organismes étrangers. Le niveau d'adéquation se mesure

> à la lumière de toutes les circonstances encadrant les opérations de transfert ou à une catégorie de transfert de données [; notamment,] sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont appliquées.[76]

---

[72] ZUBCEVIC Oriane, « Le "California Consumer Privacy Act" est-il le RGPD américain ? », *Éditions législatives*, 28 janvier 2020, consulté le 11 octobre 2020 : https://www.editions-legislatives.fr/actualite/le-«california-consumer-privacy-act»-est-il-le-rgpd-americain.

[73] *Idem.*

[74] Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, « *Manuel de droit européen ... », op. cit.*

[75] 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, J.O. n° L 281 du 23/11/1995 (art. 25 §1) ; Règlement (UE) n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), JOUE L127 2 du 23/05/2018 (art. 43 et s.).

[76] CASTETS-RENARD Céline, « Société de l'information », *Cahiers Droit, Sciences & Technologies*, n°8, 2019, p. 233-243.

Ne pouvant directement apporter des modifications législatives dans les pays collectant les données personnelles des européens, les États membres de l'UE doivent ainsi prendre les mesures nécessaires visant à empêcher tout transfert vers des pays tiers qui n'offriraient pas un niveau de protection adéquat. Les flux transfrontaliers de données personnelles étant quasiment inévitables à l'ère de l'économie numérique mondialisée, des accords bilatéraux se sont révélés nécessaires, bien que la question ne soit pas, encore aujourd'hui, totalement solutionnée.

L'histoire commence au milieu des années 1990, avec la directive CE 95/46[77], l'Europe ayant considéré que les États-Unis ne garantissaient pas un niveau de protection suffisant aux données personnelles européennes transférées. Pour y remédier, la Commission européenne, en concertation avec le département du Commerce des États-Unis, a adopté un cadre juridique spécifique, la « sphère de sécurité » (ou « *Safe Harbor* ») fondé sur la décision 2000/520/CE du 26juillet 2000. Le *Safe Harbor* consistait en un

> ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne [permettant ainsi d'assurer] un niveau de protection suffisant pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis.[78]

Une garantie de protection minimale, du moins en théorie. Effectivement le 6 octobre 2015, la Cour de justice de l'Union européenne a invalidé cette décision d'adéquation, à l'occasion de l'arrêt *Schrems I*[79]. Le requérant, un ressortissant autrichien résidant en Autriche, est un utilisateur du réseau social Facebook, dont la requête consistait, en substance, en l'interdiction à Facebook Ireland de transférer ses données à caractère personnel vers les États-Unis. Celui-ci faisait valoir que le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données à caractère personnel conservées sur le territoire américain, notamment suite aux révélations de l'affaire *Snowden*, contre les activités de surveillance qui y étaient pratiquées par les autorités publiques. La Cour estima que les vérifications et contrôles du respect des dispositions du *Safe Harbor* par les autorités américaines, notamment le Département du commerce et la FTC, étaient insuffisants. Mais également que

> si des ingérences peuvent être apportées aux droits fondamentaux protégés par la Charte de l'UE (art. 7 et 8) pour des motifs de sécurité nationale, encore faut-il que ces ingérences soient limitées et soumises en particulier aux principes de nécessité et proportionnalité [, incompatibles avec l'existence de programmes de surveillance de masse].[80]

Par ailleurs, l'accord *Safe Harbor* ne permettait pas aux justiciables d'exercer leurs droits d'accès, de rectification et d'effacement, en violation également du droit à un recours effectif et d'accéder à un tribunal impartial. Une décision qui ne fut pas sans conséquences pour la mise en conformité des traitements de données européennes transférées aux États-Unis et pour les quelques milliers de sociétés américaines qui l'appliquaient[81].

---

[77] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, *op. cit.*

[78] « Le Safe Harbor », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, consulté le 11 octobre 2020 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf.

[79] CJUE, 6 octobre 2015, aff. C-362/14, Maximilian Schrems c. Data Protection Commissioner (« Schrems »).

[80] CASTETS-RENARD Céline, « Société de l'information », *op. cit.*

[81] TAMBA Julie & Anne-Laure VILLEDIEU, « La CJUE remet en cause les modalités de transfert des données vers les Etats-Unis – la fin du Safe Harbor », *LEXplicite*, 10 novembre 2015, consulté le 11 octobre 2020 :

Après l'invalidation du *Safe Harbor*, un nouvel accord devait être négocié entre l'Union européenne et les États-Unis. Une négociation matérialisée par l'obtention d'un accord intitulé « bouclier de protection de données UE-États-Unis » qui permettait aux entreprises du numérique de transférer légalement les données personnelles de citoyens européens aux Etats-Unis. Issu de la décision du 12 juillet 2016[82], le bouclier de protection des données était

> un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis[83].

Il prévoyait de nouvelles garanties juridiques pour les individus, l'existence d'un organe indépendant de résolution des litiges destiné à recevoir les plaintes et fournir des voies de recours appropriées, un contrôle plus régulier et rigoureux du Département du commerce, mais également des limitations d'accès par les autorités publiques aux données personnelles pour des raisons de sécurité nationale[84]. Mais une fois encore, le 16 juillet 2020, la Cour de justice de l'Union européenne est intervenue, dans le cadre de *l'affaire Schrems II*, et a invalidé le régime de transferts de données entre l'Union européenne et les États-Unis dit *Privacy shield* adopté en 2016, celui présentant toujours des faiblesses non négligeables. Selon la Cour, entre autres motifs,

> les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité.[85]

En revanche, si la situation semble poser quelques difficultés vis-à-vis des autorités publiques américaines, la Cour valide la légalité des clauses contractuelles en matière de transfert de données confirmant que les entreprises peuvent se conformer à la loi européenne en s'engageant, individuellement, à respecter certaines précautions quant à l'usage des données de leurs utilisateurs européens[86]. En conséquent, il semblerait donc que la question d'un transfert des données européennes aux États-Unis garantissant un niveau de protection adéquat ne soit pas totalement résolue et fasse encore l'objet de nombreux débats. Dans le dessein d'apporter de nouvelles solutions et d'alimenter le dialogue en la matière :

> la Commission européenne considère que l'implémentation pratique du Privacy Shield peut être améliorée et fait pas moins de 10 recommandations à cet effet […] demande de clarifier l'information concernant la certification des compagnies américaines et de renforcer le contrôle et la coopération des autorités américaines en charge de l'application [souhaitant] que

---

https://www.lexplicite.fr/la-cjue-remet-en-cause-les-modalites-de-transfert-des-donnees-vers-les-etats-unis-la-fin-du-safe-harbor/.

[82] Décision de la Commission (EU) 2016/1250 du 12 juillet 2016 reposant sur la Directive 95/46/CE du Parlement européen et du Conseil sur l'adéquation de la protection fournie par le EU-U.S. Privacy Shield, OJL207, 1er août 2016, p. 1.

[83] « Le Privacy Shield », *Site officiel de la Commission Nationale de l'Informatique et Libertés*, 24 mai 2017, consulté le 11 octobre 2020 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf.

[84] CASTETS-RENARD Céline, « Société de l'information », *op. cit.*

[85] CJUE, 16 juillet 2020, aff. C-311/18, Data Protection Commissioner/Maximilian Schrems et Facebook Ireland (« Schrems 2 »).

[86] LELOUP Damien & Grégor BRANDY, « L'accord sur le transfert de données personnelles entre l'UE et les États-Unis annulé par la justice européenne », *Le Monde*, 16 juillet 2020, consulté le 11 octobre 2020 : https://www.lemonde.fr/pixels/article/2020/07/16/la-justice-europeenne-annule-l-accord-sur-le-transfert-de-donnees-personnelles-ue-etats-unis_6046344_4408996.html.

> des actions soient prises pour renforcer le Privacy Shield, afin de limiter les risques d'invalidation par la Cour de justice de l'Union européenne.[87]

Cependant, en dépit des efforts déployés par chacune des parties, le régime juridique des flux de données transatlantiques, et par voie de conséquence le niveau de protection des informations transférées, restent incertains dans un contexte politique troublé.

*

* *

En conclusion, entre attribut propre à l'individu et marchandise commercialisable, que ce soit d'un côté ou de l'autre de l'Atlantique, les données personnelles ont un statut particulier à la fois en tant qu'élément personnel et comme carburant du développement économique des nouvelles technologies. Alors que l'Europe confère une protection attentive aux données personnelles, tout du moins en théorie, *via* un système de régulation global, les États-Unis ont une approche plus libérale du sujet, faisant l'objet au cas par cas d'une protection sectorisée. Malgré cette divergence culturelle de la gestion institutionnelle de la protection des données personnelles, les choses ne sont pas si tranchées qu'auparavant et tendent à converger autour d'un objectif commun de protection de la vie privée, que ce soit celle de l'individu européen ou celle du consommateur américain, plutôt que de seulement pointer du doigt des divergences méthodologiques. Si l'on opte pour l'option de voir le verre à moitié plein, il est possible d'observer un changement de paradigme qui n'est pas anecdotique. D'un côté comme de l'autre, dans une conjoncture numérique mondialisée, les différentes philosophies aspirent à se rejoindre. L'Union européenne, avec l'adoption du RGPD se met à la portée des acteurs économiques qui collectent et utilisent les données personnelles, pendant que les États-Unis prennent peu à peu conscience de l'importance croissante des aspects sociaux et juridiques que soulève cette problématique. Les plus fervents défenseurs de la protection des données personnelles ne peuvent, en revanche, s'empêcher de voir les risques que comportent la partie à moitié vide du verre. Des inquiétudes mises en avant par les difficultés rencontrées dans la conclusion d'un accord bilatéral transatlantique, ces derniers étant successivement invalidés par la Cour de justice de l'Union européenne, qui relève des failles dans les garanties apportées aux données européennes transférées aux États-Unis et n'apportant pas un niveau de protection jugé adéquat. Plaignant dans les affaires à l'origine des invalidations de la Cour, Max Schrems s'exprimait en déclarant que « les États-Unis vont devoir sérieusement changer leurs lois sur la surveillance si leurs entreprises veulent continuer à jouer un rôle sur le marché européen »[88]. Une perspective qui reste à approfondir, laissant la problématique de la protection des données personnelles vacillante, dans un contexte politique international globalement tumultueux.

[87] CASTETS-RENARD Céline, « Société de l'information », *op. cit.*, p. 233-243.
[88] LELOUP Damien & Grégor BRANDY, « L'accord sur le transfert de données personnelles… », *op. cit.*

BIBLIOGRAPHIE

Ouvrages

Agence des droits fondamentaux de l'Union européenne et du Conseil de l'Europe, *Manuel de droit européen en matière de protection des données personnelles*, Luxembourg, Office des publications de l'Union européenne, éd. 2018, 2019, 450 p.

BANCK Aurélie, *RGPD : la protection des données à caractère personnel, 19 fiches pour réussir et maintenir votre conformité*, Paris, Lextenso, 2020, 79 p.

GUINCHARD Serge & Thierry DEBARD (dir.), *Lexique des termes juridiques*, Paris, Dalloz, 2014, 1057 p.

G'SELL Florence (dir.), *Le big data et le droit*, Paris, Dalloz, 2020, 300 p.

HOMÈRE, *L'Odyssée*, trad. du grec ancien par Victor Bérard, Paris, Gallimard, 1993, 1136 p.

ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, New York, Zulma, 2020, 864 p.

Chapitre ou partie d'un ouvrage collectif

DELMAS-LINEL Béatrice & Grégoire DUMAS, « L'impact du RGPD sur les innovations en matière d'IA », dans G'SELL Florence (dir.), *Le big data et le droit*, Paris, Dalloz, 2020, p. 207-217.

FAUVARQUE-COSSON Bénédicte & Winston J. MAXWELL, « Protection des données personnelles », *Recueil Dalloz*, décembre 2016 - mai 2018, p. 1033.

NETTER Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », dans NETTER Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, Amiens, Centre de droit privé et de sciences criminelles d'Amiens – CEPRISCA, 2019, p. 5-31.

MAXWELL Winston J., « La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne », *Le cloud computing*, p. 71-78.

Articles

BLONDEEL Jean, « La Common Law et le droit civil », *Revue Internationale de Droit Comparé*, Vol. 3, n°4, octobre-décembre 1951, p. 585-598.

BIGNAMI Francesca & Giorgio RESTA, « Transatlantic Privacy Regulation: Conflict and Cooperation », *Law and Contemporary Problems*, Vol. 78, n°2015-52, 2015, p. 231-266.

CASTETS-RENARD Céline, « Quels liens établir avec les US et l'UE en matière de vie privée et de protection des données personnelles ? », *Dalloz IP/IT*, n°3, mars 2016, p. 115.

CASTETS-RENARD Céline, « Société de l'information », *Cahiers Droit, Sciences & Technologies*, n°8, 2019, p. 233-243.

CASTETS-RENARD Céline, « L'intelligence artificielle, les droits fondamentaux et la protection des données personnelles dans l'Union européenne et les États-Unis », *Revue de Droit International d'Assas*, n°2, 2019, p. 158-174.

PETINIAUD Louis, « Cartographie de l'affaire Snowden », *Hérodote*, Vol. 152-153, n°1, 2014, p. 35-42.

TANGHE Hélène & Paul-Olivier GIBERT, « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales*, n°4, 2017, p. 79-93.

Ressources numériques

« Le Privacy Shield », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, 24 mai 2017, consulté le 11 octobre 2020 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf.

« Ce qu'il faut savoir sur les règles d'entreprise contraignantes », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, 7 février 2020, consulté le 11 octobre 2020 : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr.

« La protection des données dans le monde », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, consulté le 11 octobre 2020 : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

« Le Safe Harbor », *Site officiel de la Commission Nationale de l'Informatique et des Libertés*, consulté le 11 octobre 2020 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf.

« L'IA : C'est quoi ? », *Portail du Conseil de l'Europe*, consulté le 11 octobre 2020 : https://www.coe.int/fr/web/artificial-intelligence/what-is-ai.

« Protection des données personnelles », *Unité de la Presse – Cour européenne des droits de l'homme*, septembre 2020, consulté le 11 octobre 2020 : https://www.echr.coe.int/documents/fs_data_fra.pdf.

« Protection des données », *Le contrôleur européen de la protection des données*, consulté le 11 octobre 2020 : https://edps.europa.eu/data-protection_fr.

« La protection des données à caractère personnel », *Fiches techniques sur l'Union européenne*, 2020 : https://www.europarl.europa.eu/ftu/pdf/fr/FTU_4.2.8.pdf.

AMNESTY INTERNATIONAL, « La surveillance intrusive exercée par Facebook et Google : un danger sans précédent pour les droits humains », *Amnesty International*, 21 novembre 2019, consulté le 11 octobre 2020 : https://www.amnesty.org/fr/latest/news/2019/11/google-facebook-surveillance-

privacy/.

AUDUREAU William, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », *Le Monde*, 22 mars 2018, consulté le 11 octobre 2020 : https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html.

AVGOUSTI Christina, « Common law ou droit civil, est-ce que cela importe ? », *Le Petit Juriste*, 8 juillet 2015, consulté le 11 octobre 2020 : https://www.lepetitjuriste.fr/common-law-ou-droit-civil-est-ce-que-cela-importe/.

BELLANOVA Rocco & Paul DE HERT, « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », *Cultures & Conflits*, n°74, Été 2009, 28 octobre 2010, consulté le 11 octobre 2020 : http://journals.openedition.org/conflits/17429.

BOHIC Clément, « La Californie se dote de son RGPD sans attendre les États-Unis », *Silicon.fr*, 2 janvier 2020, consulté le 11 octobre 2020 : https://www.silicon.fr/californie-rgpd-etats-unis-331285.html.

DELTORN Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », *Revue des Droits et Libertés Fondamentaux*, 2017, consulté le 11 octobre 2020 : http://www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/.

HAAS AVOCATS, « Vers un RGPD américain ? », *Haas-avocats.com*, consulté le 11 octobre 2020 : https://www.haas-avocats.com/actualite-juridique/vers-un-rgpd-americain/.

LAUSSON Julien, « RGPD : vers une loi de protection des données personnelles aux USA ? », *Numerama*, 22 juin 2018, consulté le 11 octobre 2020 : https://www.numerama.com/politique/388051-rgpd-vers-une-loi-de-protection-des-donnees-personnelles-aux-usa.html.

LAZAREGUE Alexandre, « RGPD : Les Américains considèrent la donnée personnelle comme un simple bien commercialisable », *Le Monde*, 20 janvier 2020, consulté le 11 octobre 2020 : https://www.lemonde.fr/idees/article/2020/01/20/rgpd-les-americains-considerent-la-donnee-personnelle-comme-un-simple-bien-commercialisable_6026550_3232.html.

LELOUP Damien & Grégor BRANDY, « L'accord sur le transfert de données personnelles entre l'UE et les États-Unis annulé par la justice européenne », *Le Monde*, 16 juillet 2020, consulté le 11 octobre 2020 : https://www.lemonde.fr/pixels/article/2020/07/16/la-justice-europeenne-annule-l-accord-sur-le-transfert-de-donnees-personnelles-ue-etats-unis_6046344_4408996.html.

MARTIN Alexandre, « Privacy Shield : Comment protéger les données de votre entreprise aux États-Unis », *Village de la Justice*, 28 novembre 2019, consulté le 11 octobre 2020 : https://www.village-justice.com/articles/privacy-shield-comment-proteger-les-donnees-votre-entreprise-aux-etats-unis,33067.html?page=article&id_article=33067.

MAXWELL Winston J., « Amende contre Facebook : comment la FTC américaine s'est

transformée en super CNIL », *Institut Mines-Telecom*, 2 octobre 2019, consulté le 11 octobre 2020 : https://blogrecherche.wp.imt.fr/2019/10/02/amende-contre-facebook-ftc-super-cnil/.

MEDIAVILLA Lucas, « Loi sur les données personnelles : la Californie ouvre le bal aux États-Unis », *Les Échos*, 2 janvier 2020, consulté le 11 octobre 2020 : https://www.lesechos.fr/tech-medias/hightech/loi-sur-les-donnees-personnelles-la-californie-ouvre-le-bal-aux-etats-unis-1160009.

MOURON Philippe, « Une amende record de 5 milliards de dollars prononcée par la FTC contre Facebook », *La revue européenne des médias et du numérique*, automne 2019, consulté le 11 octobre 2020 : https://la-rem.eu/2019/12/une-amende-record-de-5-milliards-de-dollars-prononcee-par-la-ftc-contre-facebook/.

POZZO DI BORGO Valérie & Jérôme COUZIGOU, « Données personnelles aux États-Unis et dans l'UE : vers une convergence des règles de protection ? », dans « RGPD : quelques mois pour se mettre en conformité ! », *Revue Banque.fr*, n°810, 28 juin 2017, consulté le 11 octobre 2020 : http://www.revue-banque.fr/risques-reglementations/article/donnees-personnelles-aux-etats-unis-dans-ue-vers-u.

RENOUARD Guillaume, « Le "RGPD californien", une loi modèle, exportable au reste des États-Unis », *La Tribune*, 22 janvier 2020, consulté le 11 octobre 2020 : https://www.latribune.fr/economie/international/le-rgpd-californien-une-loi-modele-exportable-au-reste-des-etats-unis-840240.html.

TAMBA Julie & Anne-Laure VILLEDIEU, « La CJUE remet en cause les modalités de transfert des données vers les Etats-Unis – la fin du Safe Harbor », *LEXplicite*, 10 novembre 2015, consulté le 11 octobre 2020 : https://www.lexplicite.fr/la-cjue-remet-en-cause-les-modalites-de-transfert-des-donnees-vers-les-etats-unis-la-fin-du-safe-harbor/.

UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, Washington, DC 20580, Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, July 24, 2019 : https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf.

VACHON Loïc, « Protection des données : Une mosaïque de réglementations, d'Europe au Canada, de Californie au Brésil », *Le Monde*, 20 avril 2019, consulté le 11 octobre 2020 : https://www.lemonde.fr/idees/article/2019/04/20/protection-des-donnees-une-mosaique-de-reglementations-d-europe-au-canada-de-californie-au-bresil_5452844_3232.html.

VERMERSCH Léa, « La protection des données personnelles aux États-Unis, une approche différente de l'Europe », *Économie numérique*, 18 février 2019, consulté le 11 octobre 2020 : http://blog.economie-numerique.net/2019/02/18/la-protection-des-donnees-personnelles-aux-etats-unis-une-approche-differente-de-leurope/.

ZUBCEVIC Oriane, « Le "California Consumer Privacy Act" est-il le RGPD américain ? »,

Éditions législatives, 28 janvier 2020, consulté le 11 octobre 2020 : https://www.editions-legislatives.fr/actualite/le-«california-consumer-privacy-act»-est-il-le-rgpd-americain.

Thèses de doctorat

MERABET Samir, *Vers un droit de l'intelligence artificielle*, Thèse de doctorat, Aix-en-Provence, Université d'Aix-Marseille, 2018, 558 p.

OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse de doctorat, Paris, Université Paris 1 Panthéon-Sorbonne, 2014, 763 p.

Rapport

DÉTRAIGNE Yves & Anne-Marie ESCOFFIER, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », *Senat.fr*, 27 mai 2009, consulté le 11 octobre 2020 : https://www.senat.fr/rap/r08-441/r08-44128.html.

FOYER Jean, *Projet de loi relatif à l'informatique et aux libertés*, Rapport n° 3125 (1977-1978), JO du 4 octobre 1977, p. 5782.

Textes juridiques

Congrès des Etats-Unis, Bill of Rights (déclaration des droits), 1789.

Privacy Act (loi sur la protection de la vie privée), 5 U.S.C. § 552a, 1974.

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, J.O. n° L 281 du 23/11/1995.

Règlement (UE) n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), JOUE L127 2 du 23/05/2018.

Décision de la Commission (EU) 2016/1250 du 12 juillet 2016 reposant sur la Directive 95/46/CE du Parlement européen et du Conseil sur l'adéquation de la protection fournie par le EU-U.S. Privacy Shield, OJL207, 1.8.2016, p.1.

Décisions juridiques et jurisprudence

SUPREME COURT OF THE UNITED STATES, *Schmerber c. Californie*, 384 U.S. 757, 767, 1966.

CEDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, Requêtes nos 30562/04 et

30566/04.

FEDERAL TRADE COMMISION - United States of America, Decision and Order in the matter of Facebook Inc., August 10, 2012, n° C-4365.

CJUE, 6 octobre 2015, aff. C-362/14, Maximilian Schrems c. Data Protection Commissioner (« Schrems »).

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA, Stipulated Order for Civil Penalty, Monetary Judgment, and Injuctive Relief, United States vs Facebook Inc., July 24, 2019, n° 19-cv-2184.

CJUE, 16 juillet 2020, aff. C-311/18, Data Protection Commissioner/Maximilian Schrems et Facebook Ireland (« Schrems 2 »).

Documentaires

ORLOWSK Jeff (réalisateur), « *The Social Dilemma* », 2020.

POITRAS Laura (réalisatrice), *Citizenfour*, 2015.

Pour citer cet article : DARNAULT Cécila, « La protection des données personnelles : présentation des approches européennes et américaines », *Cahiers Tocqueville des Jeunes Chercheurs*, Vol. 3, n°1, juillet 2021, p. 153-176.

Cécilia Darnault est élève-avocate à l'École de Formation des Avocats Centre Sud située à Montpellier et chercheuse indépendante, après l'obtention d'un doctorat en droit privé à l'Université d'Aix-Marseille portant sur la gouvernance et la résolution alternative des risques juridiques.