French Treasury in the U.S.
Le Service Economique Régional de l'Ambassade de France aux Etats-Unis
MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
TRÉSOR DIRECTION GÉNÉRALE

VERS UNE LOI FEDERALE DE PROTECTION DES DONNEES PERSONNELLES AUX ETATS-UNIS ?

Par Oualid Bachiri
Le 15 février 2019

Sauf dispositions spécifiques à certains secteurs ou publics vulnérables, le cadre américain de la protection des données personnelles se limite principalement à des exigences de transparence, tout en laissant aux acteurs privés le soin d'établir leurs règles de confidentialité et les modalités de contrôle offertes aux utilisateurs. A la différence de l'Union européenne, la protection des données personnelles vis-à-vis des entités privées n'est pas considérée comme un droit fondamental au niveau fédéral. Au contraire, les acteurs économiques qui collectent et/ou contrôlent les données mettent en avant l'intérêt économique de la libre circulation de l'information pour défendre un modèle flexible. De ce fait, la protection des données personnelles est principalement traitée par les autorités en charge de la protection des consommateurs. Les récents scandales liés à des fuites de données (Equifax, Cambridge Analytica, Google+, Marriott, etc.) ont toutefois renforcé la sensibilité des citoyens vis-à-vis du traitement de leurs données par des acteurs privés, lesquels sont désormais de plus en plus disposés à accepter les termes d'un régime fédéral de protection des données personnelles.

LES GRANDES CARACTERISTIQUES DE LA PROTECTION DES DONNEES AUX ETATS-UNIS

1. Au niveau fédéral, il n'existe pas de règlementation générale sur la protection des données personnelles. La Cour suprême des Etats-Unis appréhende le respect de la vie privée en ce qui concerne le rapport entre les citoyens et les autorités, sur le fondement du 4ème Amendement de la Constitution américaine (ex. : décisions *Katz v. United States*, *Carpenter v. United States*). Sur ce plan, au pénal, la protection des données personnelles des citoyens américains est donc plus forte qu'en France où les procureurs et autorités judiciaires peuvent accéder aux données des citoyens sans mandat de perquisition sur simple décision d'un procureur.

2. Il existe toutefois un encadrement fédéral des données personnelles dans les secteurs traitant des données sensibles (données financières, données médicales, données des mineurs, données des étudiants). Cet encadrement se limite souvent à des exigences de transparence (ex. : droit d'accès à ses données, charte sur la vie privée, notification des usagers en cas de fuites de données sensibles), sauf dans le cas des mineurs de moins de 13 ans, protégés par le *Children's Online Privacy Protection Act* (COPPA Act) de 1998. Ce texte de loi fédéral est l'un des plus stricts en matière de protection

des données personnelles aux Etats-Unis, soumettant par exemple certaines collectes d'informations à l'accord explicite des parents. Il a conduit certains services (ex. : Facebook, Gmail, Twitter) à refuser l'inscription des mineurs de moins de 13 ans.

3. Le modèle américain est souvent appelé celui du « *notice and choice* » : ***a)*** les usagers doivent, a minima, être informés du fait que leurs données sont collectées et utilisées ; ***b)*** les entreprises ont une grande latitude sur la manière de présenter et rendre accessibles ces informations ; ***c)*** elles peuvent aussi décider du régime du consentement qui est, en général, celui du *opt-out*, c'est-à-dire que les utilisateurs acceptent implicitement la collecte et l'utilisation faite de leurs données dès lors qu'ils utilisent les services d'une entreprise, laquelle doit cependant prévoir des possibilités (ex. : retirer son courriel d'une liste de diffusion) afin d'être en conformité avec le CAN-SPAM Act (2003) qui encadre les messages électroniques commerciaux non-sollicités par les usagers.

4. Les attentes en matière de vie privée sont mises en regard avec l'intérêt économique de la libre circulation des données. Cet objectif justifie, selon l'approche américaine actuelle, la flexibilité accordée aux acteurs privés qui doivent néanmoins rendre compte de leurs propres engagements et sont soumis aux règlements sectoriels et aux législations des Etats fédérés. Il est à relever que les impératifs économiques étant moindres, les agences fédérales font l'objet d'un encadrement plus strict, notamment pour sécuriser l'accès aux données (cybersécurité), ce qui est censé inspirer les opérateurs privés.

Principales lois fédérales :

Health Insurance Portability and Accountability Act (HIPAA, 1996)
Financial Services Modernization Act (Gramm–Leach–Bliley Act, 1999)
Children's Online Privacy Protection Act (COPPA, 1998)
Electronic Communications Privacy Act (ECPA, 1986)

Source : SER

5. Les Etats fédérés peuvent compléter le cadre fédéral. L'Etat de Californie dispose du régime le plus protecteur. La Californie a notamment inscrit le droit à la vie privée dans le premier article de sa constitution. Le California Online Privacy Protection Act de 2003 oblige par ailleurs les entreprises de services en ligne à soumettre à leurs utilisateurs une charte de confidentialité les informant de la nature des données récoltées, leurs usages et les destinataires. De plus, la Californie requiert des entreprises qu'elles communiquent publiquement lorsque leurs bases de données ont été piratées. Cette mesure a été suivie par tous les autres Etats fédérés, avec toutefois des définitions et conditions qui peuvent varier d'un Etat à l'autre.

6. Plus récemment, la California a adopté le California Consumer Privacy Act (CCPA) en juin 2018. Sans évolution inattendue, les dispositions du texte devraient entrer en application en juillet 2020, elles se rapprochent conceptuellement du modèle européen (cadre général, sanctions financières, affirmation des droits des consommateurs) mais elles ne consacrent pas l'*opt-in* (obligation d'obtenir un consentement explicite avant toute collecte ou tout traitement de données personnelles) et se limitent aux entreprises qui génèrent plus de 25 M USD de CA ainsi qu'aux *data brokers* (entreprises dont le *business model* est la revente de données à des fins de ciblage publicitaires, ex. : Acxiom, Bluekai).

COMPARAISON AVEC LE CADRE EUROPEEN

La protection des données personnelles est un droit fondamental garanti par la *Charte européenne des droits fondamentaux*. Dans le but d'assurer l'effectivité de ce droit dans l'ensemble de l'U.E., le règlement général de protection des données (RGPD) encadre la collecte et le traitement des données personnelles et défend un certain nombre de principes (consentement explicite ou opt-in, portabilité, droit à l'oubli, obligation d'audit, etc.). Le RGPD implique l'harmonisation des cadres nationaux existants (ex. : loi Informatique et Libertés en France). A noter que le texte intègre des dispositions spécifiques selon la nature des données personnelles, les modalités de traitement ou le public affecté (décisions automatisées, consentement des mineurs, données sensibles). Le modèle européen entend également concilier l'essor de l'économie numérique avec la protection des données personnelles mais cet objectif est censé s'atteindre par l'harmonisation des cadres nationaux et la préservation de la confiance des usagers grâce à des garanties fortes.

LES AUTORITES COMPETENTES : POUVOIRS ET INDEPENDANCE

7. En théorie, quand il existe une autorité sectorielle de protection des consommateurs, celle-ci est chargée de faire respecter les lois en vigueur dans le secteur en question, notamment lorsque le secteur est concerné par des dispositions spécifiques liées à la protection des données. Par exemple, dans le cadre du respect du *Gramm–Leach–Bliley Act* (1999), une loi fédérale qui encadre le secteur financier, la *Securities and Exchange Commission*

(SEC) peut prononcer des amendes (ex. : 1 M à l'encontre de cas Morgan Stanley en 2016).

8. Dans la pratique, la *Federal Trade Commission* (FTC) s'affirme de plus en plus comme l'autorité compétente, y compris dans les cas couverts par des dispositions sectorielles (ex. : cas de la fuite de données de la société financière Equifax en 2017). De façon générale, on peut considérer que la FTC est la première autorité compétente chargée de prévenir les atteintes à la vie privée des consommateurs.

9. Le FTC Act de 1914 donne un cadre à la FTC pour agir sur un large spectre de l'économie, puisqu'elle peut s'autosaisir dès lors qu'elle suspecte des pratiques commerciales déloyales ou trompeuses pour le consommateur. La FTC est composée de 5 membres nommés par le président avec l'accord du Sénat (3 du camp de la majorité au pouvoir, 2 de l'opposition). La FTC peut ordonner une amende seulement si une entreprise fautive récidive malgré un engagement écrit visant à rectifier sa conduite. Par exemple, Uber a accepté de payer 148 millions USD pour clôturer une investigation liée à la fuite des données de millions d'utilisateurs et de milliers de conducteurs en 2014 et en 2016. L'amende a pu être imposée car l'entreprise était soumise à un « *consent decree* » suite à une fuite des données en 2014. Dans le cadre de l'affaire Cambridge Analytica, la FTC enquête actuellement quant à savoir si Facebook a violé un accord à l'amiable signé en 2011. Si tel était le cas, le réseau social s'exposerait à une amende pouvant atteindre jusqu'à 40 000 USD par violation (c'est-à-dire par utilisateur affecté), soit un montant total nettement supérieur à la pénalité payée par Uber du fait de l'ampleur des fuites de données en question (87 M d'usagers Facebook affectés).

10. L'approche du régulateur américain en matière de protection des données est principalement basée sur des outils d'*enforcement*, activés à la suite d'une analyse coût-bénéfices [en savoir plus sur la *cost-benefit analysis* de la FTC] intervenant à posteriori d'une situation suspectée d'avoir causé un tort significatif aux consommateurs. On est ici dans le cadre d'une approche règlementaire *ex-post* qui privilégie une réparation a posteriori des torts relatifs à une situation donnée. La FTC considère que son approche au « *cas par cas* » contribue également à envoyer des consignes à l'ensemble des opérateurs privés.

COMPARAISON AVEC LE CADRE EUROPEEN

A contrario, le RGPD est la résultante d'une approche *ex-ante* qui encadre les opérateurs privés afin de prévenir des situations pouvant causer du tort aux consommateurs. Seuls les échanges de données personnelles conformes au RGPD sont considérés légaux. Il est toutefois à noter que le CCPA californien s'inspire, dans une certaine mesure, de l'approche européenne.

11. Au niveau des Etats fédérés, les procureurs généraux sont compétents pour poursuivre les acteurs économiques qui contreviendraient à un règlement local de protection des données ou bien qui seraient suspectés de pratiques commerciales déloyales ou trompeuses en utilisant des données personnelles. Une violation des règles de protection des données personnelles conduit à une amende sauf dans les cas où la violation a conduit à des activités criminelles. Dans la plupart des cas, les procédures de conciliation permettent d'aboutir à un accord à l'amiable entre les parties. Par exemple, en 2017, Target a été poursuivi par 47 Etats fédérés après la fuite des numéros de cartes de crédit de 40 millions de consommateurs en 2013. Une entente entre les parties a conduit Target à accepter de payer une amende de 18,5 M USD.

12. Par ailleurs, les tribunaux des Etats fédérés réceptionnent la plupart des plaintes collectives (*class-action*) des consommateurs qui s'estiment affectés par les pratiques d'une entreprise. Ces recours sont généralement intentés à la suite de fuites de données personnelles sensibles (ex. : n° de carte de crédit). Par exemple, depuis fin 2018, le groupe Marriott fait l'objet de plusieurs *class-actions* (ex. : dans l'Etat du Maryland) à la suite de la fuite des données de près de 500 millions de clients de la chaîne d'hôtels. Les *class-actions* peuvent être traitées par le système judiciaire fédéral dès lors que les plaignants sont dans plusieurs Etats fédérés et que le montant des dommages estimés est supérieur à 5 M USD. Il est à noter que les tribunaux américains apprécient la recevabilité d'une plainte à la lumière du préjudice estimé, dont l'appréciation peut être différente d'une Cour à l'autre. Certaines Cours pourront avoir des exigences plus strictes sur la nature et la « sensibilité » des données concernées ainsi que la réalité des risques encourus (usurpation d'identité, transactions frauduleuses, etc.). *[Pour plus de précisions, lire cette analyse de l'American Bar Association].*

COMPARAISON AVEC LE CADRE EUROPEEN

Chaque Etat membre dispose d'une autorité de protection des données personnelles, laquelle est chargée de faire respecter le RGPD. Ces autorités se réunissent au sein du *Comité européen de la protection des données* qui assure la cohérence de l'application du RGPD au sein de l'U.E. Les autorités de protections des données sont indépendantes et

peuvent prononcer des sanctions administratives pouvant aller jusqu'à une amende de 10 M EUR ou 2% du CA annuel mondial pour les entreprises (20 M EUR ou 4% du CA en cas d'atteinte aux droits des personnes). Les Etats ont la possibilité d'adopter d'autres sanctions, y compris pénales. Mais il existe des variations en termes de ressources et expertise entre autorités nationales. En janvier 2019, sous le régime du RGPD, la CNIL a infligé une première amende de 50 M EUR à Google pour des « *manquements graves* » au règlement européen.

LE CAS DE L'INTERCEPTION DES TELECOMMUNICATIONS PAR LES AUTORITES

13. Historiquement, le débat américain sur la vie privée, y compris sur le plan juridique, s'attarde sur l'équilibre entre les droits des individus et les impératifs de sécurité nationale dans l'objectif de protéger les citoyens contre l'intrusion des autorités exécutives dans leur espace privé. C'est notamment sous ce prisme que la Cour suprême entend défendre le principe de vie privée.

14. L'Electronic Communications Privacy Act (ECPA), et en particulier son Titre 2 (aussi appelé Stored Communications Act) encadre les pratiques des services de police dans le cadre d'enquêtes judiciaires en précisant que l'interception de communications électroniques privées ne peut être effectuée qu'avec le mandat d'un juge. Il est à noter que ***(i)*** les communications stockées sur un serveur pendant plus de 180 jours ne sont pas protégées (les données type emails non-lus sont alors considérées comme « abandonnées ») ; ***(ii)*** les données de géolocalisation détenues par un fournisseur d'accès à internet requiert un mandat de perquisition (arrêt Carpenter de la Cour suprême, juin 2018) tandis que les autres métadonnées détenues par des tierces parties font l'objet d'un niveau de protection inférieure (ordonnance d'un juge ou *Court Order*) mais qui reste exigeant (obligation de justifier que la collecte d'informations est nécessaire à l'investigation en cours) ; ***(iii)*** les données électroniques stockées à l'étranger par des entreprises américaines sont également soumises à l'ECPA depuis le vote du *Clarifying Lawful Overseas Use of Data Act* de 2018 (CLOUD Act).

15. Dans le cadre des activités de contre-espionnage des services de renseignement américains (NSA, CIA, FBI, etc.), les étrangers suspectés d'espionnage ou d'atteinte à la sécurité nationale peuvent faire l'objet de surveillance, selon les modalités inscrites dans Foreign Intelligence Surveillance Act (FISA). Ces opérations de surveillance nécessitent l'autorisation d'une Cour spéciale (la Cour FISA), composée de juges : 99% des demandes sont acceptées.

QUELLES PERSPECTIVES POUR LE MODELE AMERICAIN DE PROTECTION DES DONNEES PERSONNELLES ?

16. Le modèle américain de la protection des données personnelles est régulièrement critiqué pour son manque de clarté et les faibles garanties apportées aux consommateurs. Ces critiques ont été amplifiées depuis le printemps 2018 du fait d'un renouveau du débat américain sur la protection des données, alimenté par deux actualités majeures : ***(i)*** la multiplication des fuites de données et le scandale Facebook/Cambridge Analytica révélé en mars 2018 ont marqué l'opinion publique ; ***(ii)*** l'entrée en vigueur fin mai 2018 du RGPD européen a, d'une part suscité l'inquiétude des entreprises américaines présentes en Europe sur les coûts de mise en conformité, d'autre part nourri un mouvement de critiques à l'encontre du modèle de régulation limitée (*light-touch regulation*) du secteur.

17. L'opportunité d'établir un cadre fédéral général sur la protection des données personnelles bénéficie à la fois d'un consensus bipartisan au Congrès et du soutien des opérateurs privés, comme en témoignent les différentes auditions organisées au cours du dernier semestre 2018 (ex. : ici et là). Plusieurs éléments expliquent le regain d'intérêt des parlementaires américains : ***(i)*** la multiplication des fuites de données est perçue comme un frein au développement de l'économie numérique (risque de baisse de confiance des usagers) car la sensibilité des citoyens américains s'est accrue en matière de protection des données ; ***(ii)*** les entreprises sont en demande d'un cadre harmonisé qui réduirait les coûts de mise en conformité liés à une multiplication des initiatives des Etats fédérés (ex. : US Chamber of Commerce, Internet Association, Software Alliance, Google) ; ***(iii)*** il existe un enjeu de réputation et d'influence lié à la difficulté de rendre visible, à l'international, le modèle américaine de protection des données, ceci à l'avantage du RGPD (cf. les contributions adressées à la *National Telecommunications and Information Administration – NTIA* - lors d'une consultation publique sur les priorités internationales américaines en matière de numérique).

18. En revanche, l'intérêt de principe pour un règlement général de protection des données n'élude pas des divergences sur les modalités, qui opposent entreprises et associations de protection des consommateurs comme l'illustrent les contributions adressées à la NTIA lors d'une

consultation publique sur la question de la vie privée. Opérateurs privés et associations se disent favorables à une loi fédérale qui imposerait des exigences de transparence (ex. : règles d'utilisation compréhensibles, notification des usagers en cas de fuite) et renforcerait les droits des consommateurs (ex. : consentement en cas de partage des données, droit d'accès et de correction des données, portabilité), mais le consensus s'estompe lorsqu'il s'agit d'apprécier l'intérêt d'adopter une législation similaire au RGPD en Europe ou au CCPA en Californie.

19. Dans leur grande majorité, les opérateurs privés plaident pour une règlementation sous la forme de principes généraux, pour ne pas faire de distinction entre les *business models* et, si possible, pour empêcher les Etats fédérés d'adopter des règles plus strictes. Les opérateurs privés souhaitent le maintien d'un certain niveau de flexibilité afin d'amoindrir les incertitudes juridiques et de limiter les coûts de mise en conformité. Ils considèrent par ailleurs que si elles existaient, les défaillances de marché seraient limitées car les scandales sur la protection de données pénaliseraient leur capitalisation boursière et la confiance des usagers.

20. A contrario, la société civile (ex. : le *Center for Democracy & Technology*) soutient une législation adaptée au contexte américain mais aussi ambitieuse que le RGPD, avec des sanctions lourdes en cas de manquement aux obligations, grâce à un renforcement des organes de contrôle (*Federal Trade Commission* et Procureurs généraux). A ces divergences s'ajoutent des désaccords sur la définition même de données personnelles (voire de données « sensibles »), les modalités de consentement (opt-in / opt-out), et l'opportunité d'interdire aux Etats fédérés de maintenir leur régime local.

21. L'administration actuelle soutient le point de vue des opérateurs privés, mais la membre du *National Economic Council* en charge du sujet Gail Slater a soutenu l'idée de renforcer le rôle de la FTC, notamment en lui permettant de sanctionner une entreprise dès la première infraction.

22. En l'absence d'un cadre fédéral contraignant, l'administration entend privilégier des dispositifs règlementaires auxquels les acteurs économiques pourront adhérer sur la base du volontariat. Cela peut prendre différentes formes, comme promouvoir : ***(i)*** l'adhésion à des principes et objectifs (non finalisés) de protection de la vie privée mis en place par le *Department of Commerce* ; ***(ii)*** l'utilisation d'outils, méthodes et bonnes pratiques mis à la disposition des entreprises et conçus par le *National Institute of Standards and Technology* (NIST) ; ***(iii)*** l'adhésion aux principes et mécanismes du Privacy Shield pour les entreprises américaines présentes en Europe (pour rappel, le *Privacy Shield* instaure depuis 2016 un mécanisme d'auto-certification pour les entreprises américaines et européennes souhaitant transférer des données personnelles depuis l'Europe vers les Etats-Unis et vice-versa) ; ***(iv)*** l'adhésion à l'APEC *Cross-Border Privacy Rules (CBPR) System*, un mécanisme de certification externe relatif à la protection des données personnelles et actuellement disponible aux Etats-Unis, au Mexique, au Canada, à Singapore et en Corée du Sud.

******

Alors que la 116ème session du Congrès a démarré en janvier 2019 avec une majorité démocrate à la Chambre des Représentants et une majorité républicaine au Sénat, les chances d'aboutir à un cadre fédéral en matière de protection des données dépendront de la priorité donnée au sujet par les deux partis et de leur capacité à dépasser des points de divergences pour en faire une loi bipartisane. Mais la perspective de l'élection présidentielle de 2020 pourrait soit mettre le sujet en arrière, soit en faire un élément de clivage politique, à l'instar de la neutralité du net.

Editeur :
Service Economique Régional des Etats-Unis
Ambassade de France aux Etats-Unis
4101 Reservoir Road, Washington, DC 20007
1700 Broadway, 30th fl, New York, NY 10019
88 Kearny Street, Suite 600, San Francisco, CA 94108
777, Poat Oak Blvd, Suite 600, Houston, TX 77056
www.frenchtreasuryintheus.org

Directeur de la publication : Renaud Lassus
Rédacteur en chef : Sabine Lemoyne de Forges
Revu par : Jonas Anne-Braun