Protection des données personnelles : Etats-Unis et Europe convergent sur tout, ou presque

L'administration Obama veut renforcer le pouvoir du régulateur du commerce, la FTC, en matière de protection des données personnelles sur Internet et converger avec les règles proposées par la Commission européenne. Mais les deux exécutifs divergent sur le droit à l'oubli.

Par Winston Maxwell (photo) et Christopher Wolf*, avocats associés, Hogan Lovells LLP.

Les Etats-Unis et l'Europe préparent en même temps d'importantes réformes en matière de protection des données personnelles. La Commission européenne a proposé le 25 janvier 2012 (1) un règlement et une directive qui seront débattues au sein du Parlement européen et du Conseil européen dans les 24 prochains mois. L'administration Obama, elle, a lancé le 23 février 2012 (2) une initiative intitulée « The Consumer Privacy Bill of Rights ». La proposition de la Maison Blanche vient d'être suivie par celle de la Federal Trade Commission (FTC), qui propose une série de mesures pour améliorer la protection du consommateur en matière de données personnelles (3).

Google et Facebook sous surveillance

Depuis longtemps, les Européens considéraient les Américains comme les parents pauvres de la protection des données personnelles. Certes, dans certains secteurs, les Etats-Unis disposent d'une législation forte en la matière (4), mais il leur manque une loi transversale qui accorde aux consommateurs des droits minimums de protection, quel que soit le prestataire. Même si la FTC disposait de pouvoirs généraux pour sanctionner des pratiques trompeuses, certains en Europe estimaient que ces pouvoirs n'étaient pas exercés de manière suffisamment forte, notamment vis-à-vis d'Internet. Mais, au cours de ces douze derniers mois, la FTC a montré qu'elle était capable de tenir tête aux plus grands acteurs de l'Internet. Elle a conclu à l'automne dernier deux accords transactionnels avec respectivement Google (5) et Facebook (6). Accusés de ne pas avoir respecté leurs propres engagements à l'égard des consommateurs, notamment au titre de leurs Privacy Policies (protection des données personnelles) et Safe Harbor (partenariat Etats-Unis/Europe), Google et Facebook ont fait l'objet d'une plainte par l'EPIC *(Electronic Privacy Information Center)*, une association de défense des consommateurs et droits civiques. La FTC a lancé une enquête et a assigné les deux géants du Net en justice pour violation de l'article 5 de la loi américaine sur la protection des consommateurs (section 5 du FTC Act). Google et Facebook ont contesté ces accusations, mais ont choisi de conclure un accord transactionnel avec la FTC, plutôt que de se battre devant les tribunaux. D'une durée de 20 ans, ces accords imposent un régime strict de protection de données personnelles au sein de chaque entreprise – un régime digne de ce qu'aurait pu imaginer une autorité européenne telle que la Cnil (7) en France ! Ces accords imposent des obligations d' « accountability » *(voir plus loin)* similaires à celles envisagées par la proposition de règlement européen. La FTC devient un gendarme redoutable en matière de données personnelles, ses amendes dépassant de loin celles imposées par les autorités européennes.

L'administration Obama souhaite aller encore plus loin : le plan dévoilé le 23 février imposerait aux Etats-Unis un régime similaire à celui envisagé en Europe. Les points de convergence entre le plan américain et la proposition de règlement européen sont nombreux.

- **Principe de la transparence :** les propositions américaines et européennes soulignent, toutes les deux, la nécessité de donner aux consommateurs des informations plus claires et lisibles sur le traitement de leurs données personnelles. La pratique actuelle consiste à insérer les dispositions sur les données personnelles, au sein de conditions générales de vente longues et difficilement compréhensibles. Cette pratique doit cesser, aussi bien en Europe qu'aux Etats-Unis. Les entreprises doivent présenter des informations courtes et pertinentes, au bon endroit et au bon moment, pour que le consommateur soit réellement informé.
- **Principe du consentement :** pour qu'un consentement soit valable, celui-ci doit être explicite et précis. Un consentement global aux conditions générales ne suffira plus. Il faudrait prévoir des consentements ciblés, proposés au bon endroit et au bon moment. Cette obligation pèse déjà sur les prestataires d'Internet en matière de *cookies*.

Consentement explicite. Et implicite ?

Les révisions de 2009 au Paquet Télécom exigent dorénavant un consentement explicite du consommateur,

Notes

(1) - Lire Winston Maxwell dans *EM@ n°51*.

(2) - *« The White House, Consumer Data Privacy in a Networked World »*, février 2012

(3) - *« Protecting Consumer Privacy in an Era of Rapid Change »*, FTC, mars 2012

(4) - Santé, services financiers, télécoms, administration, protection des enfants, législation sur les violations de données personnelles (« data breach »).

(5) - Communiqué de la FTC sur Google, 24 octobre 2011.

(6) - Communiqué de la FTC sur Facebook, 29 novembre 2011.

(7) - Commission nationale informatique et libertés (Cnil).

(8) - Une seule visite à un site web peut en effet activer des centaines de *cookies*.

(9) - Initiative *« Do not track »* du consortium W3C, évoquée récemment par le groupe « article 29 » dans sa lettre du 1er mars 2012 à l'IAB Europe et l'EASA.

avant le déploiement de ces *« témoins électroniques »* sur son terminal. Même si le principe semble clair, sa mise en œuvre s'avère complexe. Si on appliquait la règle à la lettre, le consommateur devrait donner des centaines de consentements (8) à chaque visite d'un site web !

Les prestataires de l'Internet et des organisations comme le W3C (9) travaillent avec les autorités de régulation en Europe, afin de trouver des solutions pragmatiques à ce problème épineux. Le groupe des « Cnil » européennes, dit « Article 29 », s'apprête à publier un avis sur sujet. Les propositions américaines, elles, admettent que le consentement peut être implicite dans certains cas où de toute évidence le consommateur s'attend à ce que ses données personnelles soient utilisées (10). La FTC souhaite, par ailleurs, une loi spécifique pour encadrer l'activité des « data brokers », ces marchands peu visibles qui achètent des listes de données, notamment pour les revendre aux prestataires de la publicité en ligne.

- **Principe d'** ***« accountability »*** **:** difficilement traduisible en français, ce concept signifie l'obligation pour chaque entreprise d'organiser son propre audit interne de conformité. Ces programmes de contrôle, dits de *« compliance »*, sont fréquents en matière comptable, anti-corruption et concurrence, surtout depuis l'affaire « Enron ». L'existence d'un tel programme constitue une circonstance atténuante pour les autorités américaines lorsqu'elles appliquent des sanctions. La proposition européenne et l'initiative Obama obligeraient les entreprises à prendre en compte la protection des données personnelles lors de l'élaboration de leurs produits ou services, tout comme elles prennent en compte les normes anti-pollution (11), et de prouver ensuite qu'elles ont mis en place des mesures de protection et que ces mesures de protection sont régulièrement mises à jour et testées pour garantir leur efficacité.

Autre point de convergence entre Américains et Européens : la notion même de données personnelles. Longtemps adeptes du concept de PII (Personally identifiable information), les Américains semblent maintenant rejoindre la notion plus large (12) de données personnelles chère aux Européens. Même l'adresse IP d'une machine constituerait une donnée personnelle, selon la proposition de la FTC (13).

Web, Cloud,... : libre circulation des données

Un autre point de convergence consiste en la recherche d'un régime international qui permettrait aux données de circuler librement sans frontières, tout en assurant une protection adéquate pour le citoyen. Cet objectif a été à l'origine même de la directive européenne de 1995 sur la protection des données personnelles (14) et a été fixé ensuite dans les accords « Safe Harbor » de 2000, entre les Etats-Unis et la Commission européenne. Mais l'ampleur des flux internationaux de données et la notion de *« cloud computing »* rend la recherche de nouvelles solutions indispensable. La recherche d'interopérabilité entre les régimes américain et européen de protection de données personnelles a fait l'objet d'une réunion à Washington le 19 mars 2012 (15). Cela passerait par la généralisation de codes de conduite ayant force de loi. En Europe, ces codes sont connus sous le nom *Binding Corporate Rules* (BCR). La Cnil en France et les autres autorités européennes mettent en avant les BCR comme le moyen le plus approprié pour fluidifier les transferts de données à travers le monde, au sein d'une même organisation. Aux Etats-Unis, l'initiative Obama prévoit la mise au point de codes de conduite ayant force de loi au sein de différents secteurs de l'industrie. Cette démarche sera supervisée par la NTIA (16), une agence au sein du département du Commerce américain. Si les codes de conduite américains commencent à ressembler aux BCR européens, la fameuse interopérabilité pourrait enfin devenir une réalité. @

** Christopher Wolf est également le fondateur du « Future of Privacy Forum » (www.futureofprivacy.org) à Washington DC.*

Notes

(10) - Si le vendeur transmet les données personnelles du consommateur au transporteur pour la livraison, consentement implicite ; si le vendeur cède sa liste de clients à une entreprise de marketing direct, consentement explicite.

(11) - Concept *« Privacy by Design »* préconisé depuis longtemps par les autorités canadiennes.

(12) - Le PII se limite généralement aux nom ou adresse d'une personne.

(13) - Rapport FTC de mars 2012, p. 18.

(14) - Directive 95/46/CE

(15) - *« EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson »*, 19 mars 2012.

(16) - *National Telecommunications and Information Administration* (NTIA).

FOCUS

Point d'achoppement Etats-Unis/Europe : le droit à l'oubli

Si les positions américaine et européenne s'accordent désormais sur l'essentiel, elles achoppent sur un point sérieux : le droit à l'oubli. Selon la Commission européenne, le droit à l'oubli consiste seulement à rendre plus clairs des droits qui existent déjà – et notamment le droit d'exiger l'effacement de données, lorsque celles-ci ne sont plus nécessaires. Pour certains Américains, le droit à l'oubli est l'une des plus grandes menaces à la liberté d'expression sur l'Internet de notre époque. Selon le professeur Rosen (1) à la George Washington University, le droit à l'oubli ouvre la porte à de nombreuses actions par des individus contre des plateformes d'accès à l'information, telle que Wikipedia et Google, afin de bloquer l'accès à des informations peu flatteuses (2). Les Américains voient dans le « droit à l'oubli » une dérive dangereuse vers la censure et la réécriture de l'histoire (3).

1 - Voir notamment J. Rosen, The Right to be Forgotten, 64 Stan. L. Rev. Online 88, 13 février 2012. • 2 - Ch. Wolf, The Problem with Europe's Strict Privacy Laws, 14 mars 2012. • 3- Sur cette question, voir le livre blanc publié par la American Chamber of Commerce in France: « Le droit à l'oubli: un "droit" complexe », mars 2012.