Publié dans TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad
Février-mai 2014

Rétablir la confiance de part et d'autre de l'Atlantique[*]

Peter Hustinx[**]
Contrôleur européen de la protection des données (CEPD)

Le flot récent de révélations concernant la surveillance de masse sur l'internet par les services de sécurité américains et d'autres pays a suscité une onde de choc dans le monde entier, mais a également révélé un grave problème multidimensionnel entre l'UE et les États-Unis. Non seulement, nous avons appris l'existence d'une surveillance excessive, à grande échelle et structurelle, de tous les citoyens vaquant à leurs occupations quotidiennes, mais, qui plus est, cette surveillance de masse se fonde sur une infrastructure de services gratuits, souvent dominée par des sociétés américaines, dans laquelle les données à caractère personnel des citoyens sont constamment surveillées et transformées en importants bénéfices publicitaires sur l'internet. Cette infrastructure s'est progressivement développée au cours de la dernière décennie, en bénéficiant d'un soutien évident du public, lequel a toutefois très peu conscience des conséquences, désormais évidentes. En outre, il est tout aussi important de constater un inquiétant déséquilibre entre les cadres juridiques applicables de part et d'autre de l'Atlantique.

La Commission européenne vient de présenter un plan d'action destiné à rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis

---

[*] Publié dans TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad, nr. 97, février-mai 2014, p. 80-82.
[**] M. Hustinx est le Contrôleur européen de la protection des données (CEPD). Courriel: edps@edps.europa.eu; site Web: www.edps.europa.eu

d'Amérique[1]. Ce plan d'action invite également le gouvernement américain à participer au rétablissement de la confiance et à combler le fossé actuel. Il est toutefois important de comprendre que les problèmes survenus sont profondément enracinés dans l'histoire et dans la culture juridique et que leur résolution s'inscrira dans le cadre d'un processus à long terme. En tout état de cause, il est préférable de traiter la question de l'«espionnage excessif» séparément des autres problèmes à caractère plus structurel, même si nous devons garder à l'esprit leurs interactions.

L'UE et les États-Unis présentent aussi des points communs. Les premières idées sur la protection des données à caractère personnel ont vu le jour, tant dans l'UE qu'aux États-Unis, au même moment, soit au début des années 1970. Les principes définis dans la Convention du Conseil de l'Europe sur la protection des données (1981) reposaient en fait sur les principes d'équité en matière d'informations appliqués aux États-Unis[2], qui ont également inspiré les lignes directrices de l'OCDE régissant la protection de la vie privée (1980). La situation a ensuite évolué différemment: les États-Unis se sont essentiellement basés, outre certaines lois spécifiques, sur l'autorégulation, tandis que l'UE a continué d'investir dans un cadre de lois nationales, dans l'esprit de la directive 95/46/CE. Le droit à la protection des données à caractère personnel a finalement été reconnu comme un droit fondamental distinct, inscrit à l'article 8 de la Charte des droits fondamentaux, devenue contraignante avec l'entrée en vigueur du traité de Lisbonne à la fin de l'année 2009.

Cette différence d'infrastructure juridique dissimule toutefois une importante différence constitutionnelle. Le 4e amendement de la Constitution des États-Unis, qui interdit les perquisitions et saisies non motivées[3], a une portée bien plus restreinte que le droit au respect de la vie privée, tel que défini à l'article 7 de la Charte européenne[4]. En conséquence, il ne s'applique qu'au *contenu* et non à d'autres données de communication, telles que l'appelant, l'heure et l'endroit, et ne protège en principe que les citoyens américains. En outre, les informations confiées à un prestataire de

[1] Communication de la Commission au Parlement européen et au Conseil, *Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique*, 27 novembre 2013, COM(2013) 846 final

[2] Ministère américain de la Santé, de l'éducation et des services sociaux, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens* (Rapport du Comité consultatif du Secrétaire sur les systèmes automatisés de traitement des données à caractère personnel: enregistrements, ordinateurs et droits des citoyens) (Washington DC 1973)

[3] Quatrième amendement de la Constitution des États-Unis: «*Le droit des citoyens d'être garantis dans leurs personnes, domiciles, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir.*»

[4] Article 7 de la Charte: «*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications*».

services ne bénéficient plus de sa protection, alors que le point de départ de la législation de l'UE réside toujours dans la confidentialité des communications.

Au fil des années, des solutions créatives ont été trouvées pour combler l'écart entre la législation de l'UE et l'autorégulation américaine. Citons notamment la décision relative à la sphère de sécurité[5], qui autorise le transfert de données de l'UE vers des entreprises établies aux États-Unis qui se sont engagées à respecter les principes de la sphère de sécurité, relevant de la compétence de la Commission fédérale du commerce (Federal Trade Commission) en vertu de la loi américaine sur le commerce équitable (Fair Trade Act). Bien que plus de 3 000 sociétés adhèrent actuellement à cet accord, certains problèmes majeurs subsistent, et la Commission[6] a identifié treize points d'amélioration et annoncé un réexamen approfondi d'ici à l'été 2014.

Entre-temps, l'UE s'est énormément investie dans le réexamen approfondi de son cadre juridique actuel concernant la protection des données afin de le renforcer et d'améliorer son efficacité au vu des défis posés par les nouvelles technologies et la mondialisation.[7] Ce nouveau cadre renforcera les droits des personnes concernées, les obligations des responsables du traitement des données, ainsi que la supervision et la mise en pratique par des autorités indépendantes. La proposition de règlement général sur la protection des données[8], qui serait directement contraignant dans tous les États membres, garantira une meilleure homogénéité des pratiques et règles juridiques à l'échelle de l'Union européenne. Il est désormais plus que jamais nécessaire de mettre en place un cadre solide, assorti de règles claires également applicables dans des situations de transfert de données à l'étranger.

Point important, cette proposition s'adressera à toutes les sociétés présentes sur le marché européen, quel que soit leur lieu d'activité d'origine. Le nouveau cadre s'appliquera donc également aux sociétés établies aux États-Unis ou dans d'autres pays tiers qui ne sont pas soumises à des règles similaires dans leur pays. Il concernera aussi probablement des opérateurs internet bien connus, susceptibles d'avoir fait l'objet d'une surveillance de masse lors de la fourniture de services aux consommateurs de l'UE. Ces nouvelles règles prévoiront un instrument contre les pratiques excessives des sociétés, désormais engagées dans la surveillance

[5] Décision de la Commission 2000/520/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, JO L 215, 25.8.2000, p. 7.
[6] Voir la communication mentionnée dans la note de bas de page 1.
[7] Voir le train de réformes présenté par la Commission européenne en janvier 2012.
[8] Commission européenne, proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final

systématique et l'exploitation du comportement des consommateurs. La taille même du marché européen permettra d'en faire une option réaliste.

Les nouvelles règles pourraient également prévoir un mécanisme[9] afin de gérer l'éventualité d'un conflit législatif (inter)national, au cas où les juridictions auraient des avis divergents sur leurs intérêts publics. Le principe de base sous-tendant ce mécanisme serait que tous les flux de données doivent être conformes à la législation de l'UE, sauf si un accord international contraignant prévoit le contraire ou si une autorité judiciaire ou de surveillance a octroyé une dérogation. Ce type de mécanisme pourrait s'avérer utile dans différentes situations, notamment celles désormais éventuellement concernées par la surveillance de masse.

Dans ce contexte, il est important que le plan d'action récemment présenté par la Commission européenne prévoie également des mesures dans le cadre d'accords internationaux avec les États-Unis.[10] Outre les principes de la «sphère de sécurité», déjà brièvement évoqués, la Commission entend renforcer les garanties pour la protection des données traitées à des fins répressives. La réalisation de cet objectif suppose de conclure un accord de transfert de données dans le cadre d'une coopération policière et judiciaire et de veiller à garantir un niveau élevé de protection des citoyens de part et d'autre de l'Atlantique. Cela signifie également que les citoyens européens, qui ne résident pas aux États-Unis, devraient bénéficier de mécanismes de recours judiciaire. Le transfert de données à des fins répressives devrait passer par des canaux officiels. Les demandes de données effectuées directement auprès de sociétés de l'UE ne devraient être possibles que dans des cas exceptionnels clairement définis et susceptibles de faire l'objet d'un contrôle juridictionnel.

La Commission européenne a également insisté sur le fait que les préoccupations européennes devaient trouver un écho dans le processus de réforme actuellement en cours aux États-Unis. Celui-ci porte sur le réexamen des activités des autorités américaines chargées de la sécurité nationale, y compris le cadre juridique applicable, comme l'a annoncé le Président Barack Obama. Les principaux changements envisagés par la Commission concerneraient l'application aux citoyens de l'UE ne résidant pas aux États-Unis des mêmes garanties que celles dont bénéficient les ressortissants et résidents américains, l'amélioration de la transparence des activités de renseignement et le renforcement du contrôle de ces activités. Il conviendrait également de tenir compte de la nécessité et de la proportionalité des programmes de surveillance actuels.

[9] Voir les modifications adoptées par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen en date du 21 octobre 2013.
[10] Voir la communication mentionnée dans la note de bas de page 1.

La Commission européenne a également mentionné le besoin croissant de normes internationales en matière de vie privée, notamment sur l'internet. Dans ce contexte, elle a fait référence à plusieurs initiatives récentes, dont le projet de résolution pour l'Assemblée générale des Nations unies proposé par l'Allemagne et le Brésil, qui s'appuie sur l'article 17 du Pacte international relatif aux droits civils et politiques (1966) et demande la protection de la vie privée en ligne et hors ligne.

Les échanges transatlantiques de données et autres échanges internationaux de données bénéficieraient également grandement d'un renforcement du cadre juridique national américain, et de l'adoption de la «Consumer Privacy Bill of Rights» (déclaration de droits sur la protection de la vie privée des consommateurs) présentée par le Président Barack Obama en février 2012 dans le cadre d'un projet global destiné à améliorer la protection de la vie privée des consommateurs.[11] Des règles solides et opposables en matière de protection des données, inscrites à la fois dans le droit de l'UE et dans la législation américaine, constitueraient en effet une base plus solide pour les flux transfrontaliers de données.

Enfin, il ne faut pas oublier que les États membres de l'UE peuvent avoir joué ou continuer à jouer un rôle important en matière de surveillance de masse. Le fait que la sécurité nationale reste de la seule responsabilité[12] de chaque État membre ne constitue en aucun cas une raison suffisante pour éviter de poser les bonnes questions et de prendre les bonnes mesures, le plus tôt possible et aux niveaux appropriés.

[11] Voir: *"Consumer Data Privacy in a Networked World: a framework for protecting privacy and promoting innovation in the global digital economy"* (Confidentialité des données des consommateurs dans un monde interconnecté: un cadre pour la protection de la vie privée et la promotion de l'innovation dans l'économie numérique mondiale), février 2012, Washington DC.
[12] Voir article 4, paragraphe 2, du traité sur l'Union européenne (TUE)