

A S S E M B L É E N A T I O N A L E

X I V ° L É G I S L A T U R E

Communication

Commission des affaires européennes

Mercredi 1^{er} juillet
2015
16 h 30

Communication de M^{me} Marietta Karamanli et M. Charles de La Verpillière sur la protection des données personnelles dans un cadre transatlantique



**COMMUNICATION SUR LA PROTECTION DES
DONNÉES PERSONNELLES DANS UN CADRE
TRANSATLANTIQUE**

de Mme Marietta Karamanli et M. Charles de la Verpillière

Réunion de commission du 30 juin 2015.

Comme en témoigne la diversité des projets européens touchant à sa réforme ou à son amélioration, le secteur du numérique connaît aujourd'hui une expansion sans précédent, qui est aussi vectrice de nouveaux enjeux. Car au-delà des enjeux techniques et du problème de l'unification du marché européen à travers la stratégie européenne du numérique, ce développement pose également la question du respect des droits des personnes en général et des usagers en particulier. En effet, les utilisateurs des services en ligne sur internet, des réseaux sociaux et des nombreuses plateformes d'information et de communication disponibles confient de nombreuses informations personnelles au réseau. La protection de ces données contre des utilisations abusives, frauduleuses ou tout simplement sans lien avec l'usage initial des outils ou sites numériques, ou encore disproportionnées par rapport aux nécessités des services rendus sur internet constitue un enjeu majeur. La tâche de protéger les données personnelles est compliquée par la difficulté de savoir qui les a recueillis, de localiser physiquement ces données et par les conflits entre des droits différents. Bien souvent, le caractère dématérialisé des données personnelles rend plus facile les abus. Pour parer à ceux-ci, l'Union européenne a développé dès les années 1990 une législation ambitieuse et novatrice, qui doit toutefois être conciliée avec d'autres, et principalement la législation américaine, pour être pleinement efficace. Ces deux législations sont actuellement en pleine évolution, et leurs réformes respectives apparaissent comme intrinsèquement liées.

Pour cette raison, nous avons jugé important de nous rendre aux États-Unis afin de rencontrer les interlocuteurs majeurs dans les différentes évolutions de la protection des données personnelles, qu'il s'agisse des législateurs eux-mêmes (administration et Congrès), des entreprises qui sont soumises à cette législative en mutation ou des acteurs publics qui doivent composer avec elle dans leurs activités d'intérêt général, et notamment de renseignement. Nous souhaitons donc revenir par cette communication dans un premier temps sur les informations

recueillies lors de cette mission quant aux plus récentes évolutions de la protection des données personnelles outre-atlantique, et dans un second temps, sur l'impact potentiel de celles-ci sur les changements à venir dans le cadre de l'Union européenne et des dernières négociations transatlantiques dans ce secteur.

I. UN CADRE EN PLEINE MUTATION AUX ÉTATS-UNIS

Nous voudrions d'abord souligner la diversité des interlocuteurs rencontrés, puisque nous avons eu des entretiens au sein de l'administration (Bureau du Directeur du renseignement national/ODNI, Département du *Homeland Security*, Département de la Justice, *Federal Trade Commission*), au Congrès (bureaux du Sénateur Chuck Grassley, Président de la Commission des affaires juridiques, et du Représentant Jim Sensenbrenner, notamment co-auteur des projets de loi *USA Freedom Act* et du *Judicial Redress Act*), avec l'organisme indépendant *Center for Democracy & Technology*, aux bureaux d'Apple et avec le Chef du Bureau de liaison du Parlement européen, M. Antoine Ripoll, et le numéro deux de la Délégation de l'Union, M. François Rivasseau.

Concernant l'administration, cela nous a permis d'apprécier le caractère très éclaté des acteurs ayant à composer avec le problème de la protection des données personnelles et qui sont amenés à intervenir dans les évolutions législatives. Dans le secteur du renseignement, cela représente en effet seize agences sous la supervision du Directeur du renseignement national (DNI).

A. RÉFORME DU *PATRIOT ACT*

Ces agences étaient directement touchées par l'expiration le 1^{er} juin 2015 du dispositif du *Patriot Act* relatif à la collecte de métadonnées des citoyens américains et résidents (la section 215 de l'article 2). Dans ses directives concernant la réforme des services de renseignement, le Président Obama a formulé en décembre 2013 quarante-six recommandations, avec pour objectif d'offrir plus de transparence sur l'interception et la rétention des métadonnées (telles que l'horaire ou le destinataire d'un appel, sans que le contenu de l'appel soit lui-même nécessairement analysé). Cette visée de transparence et de meilleur ciblage des contrôles opérés devait aussi selon ces directives être étendue aux personnes non américaines.

Au moment de notre mission, deux projets de lois concurrents avaient été introduits au Congrès. L'un prolongeait tel quel le dispositif actuel du *Patriot Act*. L'autre (le *USA Freedom Act* présenté le 28 avril par J. Sensenbrenner avec le soutien de l'administration) proposait une réforme des pratiques dans le prolongement des engagements pris par le Président Obama, avec la fin de la collecte de masse par l'administration et obligation pour les agences de renseignement de davantage cibler leurs demandes d'accès aux données. Depuis notre déplacement, c'est finalement ce second projet qui a été adopté, et cela, sans surprise, car dans l'ensemble, nos interlocuteurs américains s'étaient montrés

confiants sur le passage d'une loi d'ici le 1^{er} juin, compte tenu du risque d'absence de base juridique auquel les services de renseignement américains seraient confrontés dans le cas contraire.

Il faut toutefois relativiser les changements qu'entraînera la mise en œuvre de cette législation. Les think tanks tels que le *Center for Democracy & Technology* aussi bien que le General Counsel de l'ODNI estimaient que le texte qui serait adopté ne modifierait pas fondamentalement les pratiques des agences de renseignement. Le stockage des métadonnées par les opérateurs téléphoniques plutôt que par le gouvernement n'empêchera pas les services de renseignement d'y accéder, et les grands opérateurs de l'internet devraient rester peu concernés par ce texte dans la gestion des données recueillies sur le réseau.

Mais cette volonté d'un plus grand contrôle sur les activités des services de renseignement pourrait également avoir des répercussions sur le droit de la protection des données personnelles des Européens.

B. UN NOUVEAU DROIT DE RECOURS POUR LES CITOYENS NON-AMÉRICAINS

En effet, une autre réforme concerne plus précisément les citoyens non-américains et semble faire l'objet d'une réflexion très actuelle. En juin 2014, l'Attorney General, Eric Holder, avait promis qu'un projet serait présenté permettant dans une certaine mesure un accès pour les citoyens n'étant ni américains, ni résidents des États-Unis, à des recours judiciaires contre l'usage fait par les autorités américaines de leurs données personnelles. Cette promesse s'est traduite par un projet de loi introduit mi-avril à la Chambre par le Représentant Sensenbrenner, le *Judicial Redress Act*.

Les collaborateurs du Représentant Sensenbrenner, que nous avons rencontrés, nous ont indiqué qu'aucun calendrier pour les discussions et le vote du projet n'était prévu à ce stade, les efforts de pédagogie en direction des élus n'étant qu'à leurs débuts. Pour leur part, le Chef du Bureau du Parlement européen et le numéro deux de la Délégation de l'Union à Washington ont mis en avant à la fois les efforts des institutions européennes, et la forte pression des industriels américains sur le Congrès en faveur de ce projet de loi. Les élus américains devraient *in fine* comprendre l'intérêt commercial indirect de l'adoption de cette loi (comme prérequis implicite, côté européen, à la finalisation des négociations du Safe Harbor). Les interlocuteurs au Département de la Justice se montrent confiants pour ces mêmes raisons (« *Il y a eu beaucoup de lobbying des entreprises, y compris européennes, au Congrès en faveur de ce texte* »).

II. DES IMBRICATIONS CROISSANTES ENTRE LA PROTECTION DES DONNÉES PERSONNELLES AUX ÉTATS-UNIS ET DANS L'UNION EUROPÉENNE

Alors que l'Union européenne finalise les négociations autour du paquet « protection des données personnelles », notre mission nous a permis de constater que les progrès et évolutions se répondaient de plus en plus des deux côtés de l'Atlantique. Au Département de la Justice et au département du *Homeland Security*, les interlocuteurs rencontrés insistent, s'agissant des négociations sur « l'accord parapluie », sur le caractère central de l'adoption de la loi étendant aux Européens le bénéfice du recours judiciaire.

L'accord parapluie, que la Commission avait reçu mandat de négocier avec les États-Unis, concerne la protection des données personnelles pour tous les échanges entre l'UE et les États-Unis dans le domaine de la coopération policière et de la coopération judiciaire pénale. Il a quatre objectifs : garantir un niveau élevé de protection des libertés, apporter un cadre juridique cohérent et contraignant des normes régissant la protection des données, assurer un degré élevé de protection des données, favoriser la coopération judiciaire et policière entre les États-Unis et l'Union. Alors qu'elles semblaient être au point mort depuis quelques mois, et sous réserve de l'adoption de la loi, Sensenbrenner nos interlocuteurs ont estimé que les négociations pourraient être finalisées à brève échéance. Cette analyse est confirmée à la Délégation de l'Union européenne de Washington. L'Accord parapluie permettrait de prévoir un ensemble cohérent et harmonisé de normes en matière de protection des données. Il énoncerait notamment des principes fondamentaux comme la proportionnalité, la limitation de l'étendue et de la durée de conservation des données au strict nécessaire et la stricte limitation des finalités de celle-ci. Cet accord pourrait donc conduire à faire converger les législations dans le sens d'une protection transatlantique plus proche des standards européens.

Le vote du Judicial Redress Act, revendication de l'Union pour offrir un recours judiciaire aux Européens, conditionnerait donc la conclusion de l'Accord parapluie, qui serait elle-même un prérequis pour la renégociation du Safe Harbor. L'accord de Safe Harbor sur les données personnelles dans la sphère commerciale, permet à de nombreuses entreprises américaines, sous réserve d'une certification par la *Federal Trade Commission*, de bénéficier de la présomption d'un traitement des données personnelles en accord avec les standards européens de la directive de 1995. Il a donc de profondes ramifications commerciales pour les grandes entreprises américaines du secteur de l'internet, qui bénéficient d'un régime relativement favorable dans l'accès aux données européennes. Les révélations de l'Affaire Prism avaient toutefois conduit la Commission à émettre treize recommandations pour réformer le Safe Harbor, des dysfonctionnements ayant été avérés. Il existe aujourd'hui un fort enjeu pour les entreprises américaines, qui poussent pour une renégociation favorable à leurs intérêts économiques, et se font donc ici les alliées de l'Union dans la recherche d'avancées.

Les entreprises des nouvelles technologies sont très impliquées sur ces sujets et n'hésitent pas à développer une réflexion novatrice en matière de protection des données personnelles. Vos rapporteurs ont ainsi pu rencontrer les représentants de l'entreprise Apple.

Dernier exemple notable du dialogue transatlantique accru en matière de données personnelles : la réussite que constitue pour le département de sécurité intérieure (Homeland Security) l'accord sur les données des passagers (PNR). Selon le Homeland Security, le PNR permet notamment de développer le « scenario-based targeting », le repérage des ruptures dans les habitudes de déplacement d'une personne suspecte et ainsi de déjouer véritablement des projets d'attentat, mais constitue également un instrument dans la lutte contre la propagation de pandémies du type Ebola, en offrant la vision du trajet complet d'un voyageur arrivant aux États-Unis (par exemple d'Afrique de l'Ouest *via* l'Europe), et pas seulement depuis sa dernière escale. Le *Center for Democracy & Technology* s'est montré plus circonspect sur le caractère jugé trop invasif des croisements de fichiers générés grâce au PNR, mais a estimé que le temps du débat était passé sur ce sujet aux États-Unis.

*

* *

La mission effectuée aux États-Unis par vos rapporteurs du 27 au 29 avril a donc permis de constater chez notre partenaire transatlantique un véritable foisonnement législatif autour des questions de la protection des données personnelles (d'autres initiatives sur le cryptage des données ou la lutte contre les cyberattaques ont été évoquées lors des entretiens mais n'ont pu être détaillées dans la présente communication). Ce foisonnement n'est pas sans conséquences sur les droits exercés par les Européens, et à ce titre, les négociations entre les deux acteurs majeurs que sont l'Union et les États-Unis dans la collecte et le traitement des données devront continuer à faire l'objet d'un suivi attentif. Cela d'autant plus que la protection des données personnelles voit son cadre profondément renouvelé avec l'élaboration d'un nouveau paquet dans l'Union, dont la conclusion est espérée dans les mois à venir.

Enfin, même si tel n'était pas l'objet de notre déplacement aux États-Unis, la question de la protection des données personnelles se pose fortement dans le cadre du projet de traité transatlantique. En effet, la question des données n'est pas mentionnée dans le mandat européen de négociation du TTIP, les États-Unis poussent à un renforcement de la libre circulation des données entre les entreprises européennes et américaines – « cross-border data flows ». Une telle libéralisation suppose l'abaissement des barrières réglementaires, principalement européennes, encadrant et restreignant notamment la transmission des données à caractère personnel vers des pays tiers. En effet, les différences de législation entre l'Union européenne et les États-Unis entraînent des coûts d'adaptation pour les entreprises

qui affectent la fluidité commerciale entre les deux parties. Des restrictions pourraient en effet être justifiées par un impératif de protection des intérêts économiques ou de l'intérêt général (vie privée, sécurité publique, santé publique ...).

C'est pourquoi, compte tenu des révélations récentes sur la surveillance massive des citoyens européens, ainsi que de leurs dirigeants au plus haut niveau, qui ont entraîné une crise de confiance entre l'Union européenne et les États Unis, il nous incombe d'être particulièrement vigilant sur le traitement de la question des données personnelles dans le cadre des négociations en cours. Tout comme le Parlement européen, qui a exprimé sa position sur le sujet dans un rapport d'initiative en mars dernier, je pense que l'Union européenne doit être particulièrement attentive à cet égard, dans le cadre des négociations en cours, afin que tout transfert de données personnelles d'une rive à l'autre de l'Atlantique soit soumis au respect de la législation communautaire.