LYSIOS
PUBLIC AFFAIRS

31 octobre 2014

L'Union européenne et la protection des données personnelles

La protection des données personnelles figure parmi les 10 priorités que le nouveau président de la Commission Jean-Claude Juncker s'est fixées pour les premiers mois de son mandat. Avec l'apparition de moteurs de recherche de plus en plus puissants, du « cloud computing » et le développement du commerce électronique, les données personnelles ont pris une valeur marchande considérable. Par ailleurs, la révélation en juin 2013 de l'existence du programme Prism de surveillance électronique généralisé mis en place par l'Agence nationale de sécurité américaine (NSA) a mis en en évidence l'enjeu de la protection des données personnelles en matière de libertés publiques et de respect de la vie privée. La législation de l'Union européenne (UE) relative à la protection des données personnelles résulte d'une réflexion propre à l'UE (I) mais elle a aussi été influencée par les pratiques des Etats-Unis et l'évolution des négociations avec ce pays (II).

I. La protection des données personnelles dans l'UE

1. La directive sur la protection et la libre circulation des données

Texte fondateur, la directive de 1995[1] répond à un double objectif : garantir le droit fondamental des personnes à la protection de leurs données et permettre la libre circulation de ces données entre Etats membres.

Elle établit les principes de licéité du traitement des données (type, qualité, exactitude des données ; traitement loyal et licite à des fins déterminées ; légitimation par consentement ou par nécessité) et garantit leur protection (confidentialité et sécurité du traitement ; non-retraitement par un sous-traitant sauf sur instruction du responsable du traitement ; notification à l'autorité de contrôle). Elle octroie des droits aux personnes : information et opposition au traitement ; accès, rectification et effacement des données non conformes ; recours juridictionnel. Elle créé le « groupe de l'article 29 » qui réunit des représentants des autorités nationales de contrôle, afin de favoriser une interprétation commune de la directive et de contribuer à l'élaboration de normes européennes de protection.

2. Un niveau élevé de protection pour certains acteurs et certains secteurs

En 2001, l'UE a adopté un règlement[2] relatif à la protection des données traitées par ses institutions et les organes qui en dépendent. Il oblige ces organismes à désigner un délégué chargé de cette protection et institue une autorité indépendante chargée de la bonne exécution du règlement : le contrôleur européen de la protection des données (CEPD).

[1] Directive 95/46/CE 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.
[2] Règlement 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et la libre circulation de ces données.

Depuis 2002, la directive « vie privée »[3] encadre le traitement des données lors de la fourniture de services de communication.

En 2006, à la suite des attentats de Madrid et de Londres (2004 et 2005), l'UE adopte la directive « conservation des données »[4] qui oblige les opérateurs à garder pendant 6 à 24 mois les métadonnées[5] de la communication.

En 2008, la protection des données dans les domaines de la coopération policière et judiciaire en matière pénale fait l'objet d'une décision-cadre[6].

Le Traité de Lisbonne donne en 2009 une base juridique solide à la protection des données[7].

Enfin, en 2011, la Commission présente la proposition de directive « utilisation des données des passagers aériens (PNR) » dans l'UE. Mais la commission Libertés Civiles du Parlement européen a rejeté la proposition en avril 2013. Le dossier est depuis lors bloqué bien que le Conseil ait appelé en juin 2014 à une décision avant la fin de l'année 2014.

3. L'actuelle révision du cadre européen de la protection des données

Adoptée à une époque où moins de 1% des Européens utilisaient Internet[8], la directive de 1995 ne répond qu'imparfaitement aux enjeux actuels. La commissaire à la Justice, Viviane Reding a été conduite à présenter en janvier 2012 un « paquet législatif » composé de deux propositions :

a) **Une proposition de règlement[9] qui vise à renforcer les droits des personnes** en précisant les définitions du « consentement éclairé » (les responsables du traitement doivent les informer et recueillir leur accord au traitement) et du droit à l'oubli (le premier responsable du traitement informe les responsables suivants que la personne souhaite effacer ses données, et surveille leur suppression). Elle introduit le droit de portabilité des données et elle règlemente le profilage. En outre, les responsables du traitement doivent prendre en compte la protection des données dès la conception (« privacy by design »[10]). Le secteur public et les entreprises (sauf les PME) nomment un délégué à la protection des données. Les Etats

[3] Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
[4] Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.
[5] Les métadonnées incluent par exemple la date et la durée de l'appel, l'appareil utilisé ou sa localisation.
[6] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.
[7] Article 16 du Traité sur le fonctionnement de l'UE.
[8] Source : Commission, communiqué IP/12/46.
[9] Proposition de règlement du Parlement européen et du Conseil COM(2012)0011 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[10] Les responsables du traitement doivent conserver une trace documentaire de leurs opérations, notifier les violations et effectuer une analyse d'impact relative préalable aux traitements présentant le plus de risques.

définissent les sanctions pénales en cas d'infraction et installent des autorités nationales de contrôle qui doivent répondre à des conditions d'indépendance et coopérer entre elles. La Commission introduit la désignation d'une « autorité chef de file » unique, celle de l'État où se situe l'établissement principal du responsable du traitement, qui contrôlera le traitement des données dans tous les États. Les directeurs des autorités nationales et le CEPD se réunissent au sein d'un nouveau comité européen de la protection des données qui remplace le « groupe de l'article 29 » de la directive de 1995.

Cette proposition est en cours d'examen au Parlement et au Conseil. En mars 2014, le Parlement a élargi son champ d'application au traitement des données européennes en dehors de l'UE. Il a clarifié les conditions du consentement, du droit à l'effacement et de l'opposition au profilage. Début octobre, le Conseil a adopté une position sur les obligations des responsables du traitement et des sous-traitants. La question de l'autorité nationale de contrôle n'a en revanche pas été tranchée, certains Etats (dont la France) défendant plutôt une codécision des autorités nationales.

b) **Une proposition de directive concernant la protection des données traitées à des fins répressives**[11]. Elle étend le champ d'application de la décision de 2008 aux traitements effectués au niveau national par les autorités policières et judiciaires. Elle renforce les conditions d'autorisation du transfert de données vers un Etat tiers et prévoit des mécanismes de coopération internationaux. Le Parlement s'est prononcé en mars dernier mais le Conseil n'a pas encore entamé le débat de fond.

4. Invalidation de la directive « conservation des données »

En avril 2014, la Cour de justice de l'UE (CJUE) a rendu un arrêt qui invalide la directive « conservation des données » de 2006[12]. Permettant la création d'un profil trop précis de la personne, cette directive laissait les Etats libres de définir et d'établir les garanties d'accès aux données collectées. La CJUE a estimé que la vie privée des personnes était insuffisamment protégée. Cependant l'invalidation de la directive n'invalide pas pour autant les lois nationales qui découlent de sa transposition. Cet arrêt rarissime n'a pu que renforcer les velléités de réforme affichées par la Commission.

II. La protection des données personnelles de l'UE transférées aux Etats-Unis

1. Les données transférées à des fins commerciales

[11] Proposition de directive du Parlement européen et du Conseil (COM(2012)0010) relative à la protection des personnes à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[12] Cet arrêt répond aux demandes d'examen en validité introduites par la Cour suprême irlandaise et par la Cour constitutionnelle autrichienne.

La directive de 1995 autorise les transferts de données à des fins commerciales d'un État membre vers un Etat tiers qui assure un niveau de protection adéquat, ce que la Commission reconnait en adoptant une décision d'adéquation (« adequacy decision »). En 2000, la Commission a reconnu l'adéquation de la protection de la vie privée offerte par les principes américains « Safe Harbour ». Cela autorise le transfert de données des Etats de l'UE vers les entreprises américaines qui ont souhaité adhérer à ces principes auprès du Département du Commerce américain.

2. Les données transférées à des fins répressives

Après les attentats du 11 septembre 2001, les accords de coopération policière et judiciaire entre l'UE et les Etats-Unis se sont multipliés.

- Fin 2001, Europol et les Etats-Unis acceptent d'échanger des informations stratégiques et techniques pour prévenir et enquêter sur les crimes internationaux.
- En 2009, le Conseil de l'UE adopte une décision relative à l'entraide judiciaire et à l'extradition des criminels.
- Le New York Times ayant révélé en 2006 que les Etats-Unis espionnent les données bancaires européennes stockées sur le réseau de l'entreprise Swift, ce pays propose à l'UE de négocier un accord pour régulariser cette situation. L'accord sur le « Traitement et transfert des données de messagerie financière pour le programme de financement du terrorisme » (TFTP) est adopté en juillet 2010.
- Enfin, l'utilisation et le transfert des données des passagers aériens (PNR)[13] fait l'objet d'un accord fin 2011.

Au-delà de ces accords spécifiques, l'UE et les Etats-Unis ont entamé en mai 2011 des négociations sur un accord-cadre sur les principes de traitement des données échangées. Ces négociations, toujours en cours, achoppent notamment sur la garantie de recours juridictionnel. L'UE souhaite en effet que ses citoyens qui ne résident pas aux Etats-Unis disposent des mêmes garanties de protection que les citoyens américains.

3. L'affaire Prism et la remise en question des accords avec les Etats-Unis

A la suite de l'affaire Prism, de nombreuses voix se sont exprimées en Europe pour demander la suspension et/ou la révision de l'accord « Safe Harbour ». Le 4 juillet 2013, le Parlement européen a adopté une résolution en faveur d'une révision de l'accord. La Vice-Présidente Viviane Reding a répondu le 19 juillet en annonçant que la Commission allait réexaminer cet accord et en novembre 2013, elle a publié trois documents :

a) Le rapport du groupe de travail UE-Etats-Unis, créé en 2013 pour établir les effets des programmes de surveillance américains sur la protection des données européennes, qui révèle que certaines lois américaines permettent la collecte et le traitement des données à

[13] L'UE en a également adopté un avec l'Australie en 2011 et un avec le Canada en 2014.

des fins de surveillance étrangère, sans donner aux personnes des droits d'accès, de rectification et d'effacement de leurs données, ni de recours.

b) Une communication sur le transfert des données transatlantiques qui présente les enjeux liés à la collecte de renseignements par les Américains. Elle invite les institutions à adopter au plus tôt le paquet sur la protection des données personnelles, à renforcer l'accord du « Safe Harbour » et à exiger du gouvernement américain l'extension aux citoyens européens des garanties accordées aux données de leurs citoyens.

c) Enfin, une communication analysant le fonctionnement du « Safe Harbour » qui se conclut par une liste de 13 recommandations adressées à la Commission fédérale du Commerce américain. Elles visent à renforcer la transparence des données échangées et à encadrer leur accès par les autorités américaines. Elles garantissent les possibilités de recours et l'application de l'accord.

La Commission a clairement laissé entendre que si ces recommandations n'étaient pas prises en compte, l'accord « Safe harbour » pourrait se trouver en danger. Le 28 janvier dernier, la Vice-Présidente Viviane Reding a ainsi jugé que l'accord présentait des failles et menacé de le suspendre si les Etats-Unis n'y mettaient pas bon ordre.

III. Conclusion

La nouvelle Commission souhaite aller rapidement de l'avant. Dans ses lettres de mission adressées au Vice-Président chargé du Marché numérique, Andrus Ansip, et à la commissaire à la Justice, Vera Jourova, le Président Jean-Claude Juncker a demandé de veiller à l'adoption du paquet « protection des données » et de clore l'examen du « Safe Harbour » dans les six mois suivant l'entrée en fonction de la nouvelle Commission. Sur le plan strictement européen, l'adoption du paquet législatif « données personnelles » en six mois est sans conteste un objectif ambitieux. L'examen du « Safe Harbour » devrait par contre être achevé dans les délais prévus, mais il n'est pas sûr que les Etats-Unis suivent les recommandations de la Commission. Dans ce cas, la question de la suspension de l'accord se poserait très rapidement. Par ailleurs, des interférences avec les négociations sur le « Partenariat transatlantique de commerce et d'investissement» ne sont pas à exclure. Nul doute que la protection des données personnelles se situera à un niveau élevé dans l'agenda européen au cours des prochains mois.