Réforme du cadre européen relatif à la protection des données personnelles : les propositions de la Commission Européenne

[DONNEES PERSONNELLES]
Commission Européenne, proposition de règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, 25 janvier 2012

Le 25 janvier 2012, la Commission a rendu publique sa proposition globale fixant un nouveau cadre législatif à la protection des données au sein de l'Union Européenne.

Les propositions de la Commission se trouvent ainsi traduites, d'une part, dans un projet de règlement européen (texte d'application directe) qui abrogerait la directive 95/46/CE relative à la protection des données personnelles et, d'autre part, dans une proposition de directive portant spécifiquement sur la protection des données traitées à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites, ainsi que d'activités judiciaires connexes.

Le choix de la Commission en faveur d'un règlement pour fixer le nouveau cadre général résulte du constat (peu contestable) que les disparités des lois nationales ayant transposé la directive de 1995 étaient source de confusion et d'insécurité juridique tant pour les personnes physiques dont les données personnelles sont traitées que pour les organisations mettant en œuvre les traitements.

Les mesures phares de la proposition de règlement s'articulent autour de trois grands objectifs rappelés par la Commission dans sa communication du 25 janvier 2012 : unifier et améliorer la protection des données des particuliers dans tous les domaines d'action (1), réduire les formalités administratives pesant sur les entreprises responsables de traitement (2), garantir la libre circulation desdites données au sein de l'UE (3).

Au plan économique, la Commission souligne l'importance de susciter la confiance des consommateurs dans les services numériques pour permettre à l'économie numérique de se développer dans l'ensemble du marché intérieur, et donner un « coup de fouet salutaire » à la croissance en Europe (considérant 6 du projet de Règlement).

L'adaptation de la réglementation à l'ère numérique apparaissait, en tout état de cause, indispensable étant rappelé que la directive 95/46/CE avait vu le jour à une époque où l'Internet n'en était qu'à ses premiers balbutiements.

1/ Protection renforcée des données personnelles des particuliers

Le considérant premier du projet de règlement réaffirme que la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. Cette disposition rappelle le principe posé à l'article 8 de la Charte des droits fondamentaux selon lequel toute personne a droit à la protection, dans tous les aspects de sa vie, des données à caractère personnel la concernant.

Pour garantir ce droit fondamental, plusieurs mesures sont proposées : consécration de l'opt in, droit à l'oubli numérique, droit à la portabilité des données, renforcement des sanctions applicables aux responsables de traitement.

Il s'agit tout d'abord d'imposer aux sites marchands, réseaux sociaux ou moteurs de recherche, l'obtention d'un consentement explicite des internautes en vue de l'utilisation de leurs données. C'est la version actualisée de « l'opt in » défini dès 1995 par opposition à « l'opt out », en vigueur aux Etats-Unis où les données sont présumées utilisables tant que la personne ne s'y est pas explicitement opposée. L'article 4 du projet définit le consentement comme « *toute manifestation de volonté, libre, spécifique, informée et* ***explicite*** *par laquelle la personne concernée accepte, par une déclaration ou* ***par un acte positif univoque****, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Le considérant 25 suggère, par exemple, que la personne manifeste son consentement en cochant une case lorsqu'elle consulte un site internet.

L'article 17 du texte prévoit de rendre possible un véritable « droit à l'oubli numérique » qui permettrait aux internautes d'obtenir la suppression de l'intégralité des données les concernant si le responsable de traitement n'a pas de motif légitime pour les conserver. Ainsi, un internaute qui voudrait résilier son compte sur un réseau social devrait théoriquement pouvoir obtenir du site qu'il détruise toutes les données personnelles le concernant. L'on sait que cette disposition vise notamment à protéger les mineurs des risques inhérents au traitement des données qu'ils communiquent, souvent trop facilement, sur les réseaux sociaux.

Un droit à la portabilité des données est consacré à l'article 18 du projet de règlement : « *la personne concernée a le droit d'obtenir auprès du responsable de traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée* ». La personne concernée devrait être autorisée à transférer ces données, qu'elle a fournies, d'une application automatisée (telle qu'un réseau social) à une autre.

Le renforcement de la protection se traduit également par une augmentation significative des sanctions pouvant être prononcées par les autorités nationales de protection, sur le territoire de l'Etat dont elles relèvent. Ces autorités pourraient ainsi infliger des amendes qui pourront atteindre 1 million d'euros ou 2% du chiffre d'affaires annuel mondial, s'il s'agit d'une entreprise.

Enfin, le nouveau cadre législatif prévoit que les principes généraux en matière de protection des données s'appliqueront à la coopération policière et à la coopération judiciaire en matière pénale, tout en respectant les spécificités de ces domaines. Ces spécificités sont prises en compte par le projet de directive proposé par la Commission européenne. Son objectif est de faciliter l'échange d'informations entre les autorités policières et judiciaires nationales et, de ce fait, d'améliorer la coopération dans la lutte contre les formes graves de criminalité en Europe, tout en garantissant un niveau élevé de protection des données personnelles dans ce domaine.

A l'heure actuelle, le traitement de ces données est essentiellement régi par la décision cadre de 2008 dont le champ d'application est limité aux traitements à caractère transfrontière. Il en résulte une transposition disparate au sein de l'Union ainsi que des difficultés pratiques pour les autorités de police et judiciaires à déterminer si un traitement de données est purement national ou transfrontière. L'article 2 du projet étendrait le champ d'application de la directive à l'ensemble des traitements effectués par des autorités compétentes.

Ainsi, s'il existe un droit des personnes physiques à être informées lorsque les autorités de police ou judiciaires traitent ou consultent des données les concernant, l'article 11 du texte prévoit que ce droit pourra être limité lorsque ces limitations sont « *nécessaires et proportionnées, dans une société démocratique, à l'exercice des tâches des autorités compétentes* ».

2/ La réduction des obligations administratives des entreprises

La proposition de règlement prévoit que l'obligation de notification qui incombe actuellement aux entreprises sera supprimée. Cette mesure devrait représenter une économie annuelle de quelques 2,3 milliards d'euros. En contrepartie, le règlement impose toutefois davantage d'obligations aux responsables de traitement et accroit leur responsabilité.

Les articles 31 et 32 du règlement imposent aux organisations d'informer les personnes intéressées et l'autorité nationale compétente dans les meilleurs délais – et dans la mesure du possible dans les 24 heures – en cas de violation des données, c'est-à-dire si des données sont accidentellement ou illégalement détruites, perdues, altérées, consultées par des personnes non autorisées ou divulguées à de telles personnes.

Mais la mesure la plus emblématique serait de soumettre exclusivement les responsables de traitement à l'autorité de protection située dans l'état où ils ont leur « établissement principal ». Le considérant 98 évoque ainsi un système de « guichet unique » qui suscite des réactions contrastées.

Cette dernière proposition est en effet vivement critiquée par la CNIL. Etant rappelé que les grands acteurs de l'internet implantés en Europe ont rarement leur établissement principal en France, la CNIL craint de voir nombre de procédures échapper ainsi à son contrôle. L'Assemblée nationale, qui a adopté une proposition de résolution européenne, s'oppose également à ce critère de l'établissement principal, qui serait porteur, selon elle, de conséquences économiques, politiques et juridiques extrêmement préjudiciables pour les droits des citoyens mais aussi pour l'économie de la France et de l'UE. Le Sénat a adressé des critiques similaires sur ce point et saisi le Ministre de la justice qui soutient la position du Parlement français. L'on notera en revanche que l'ICO (Information Commissionner's Office – équivalent britannique de la CNIL), dans un esprit plus libéral, n'émet pas d'avis défavorable.

3/ La libre circulation des données personnelles et ses défis

La question des flux internationaux de données constitue également une préoccupation importante pour la Commission. La proposition de règlement prévoit ainsi que le droit de l'Union serait applicable aux responsables de traitements établis hors des frontières européennes, *chaque fois que des produits et services seront proposés à des personnes physiques dans l'UE ou que leur comportement est analysé*. Actuellement, au plan français, la loi Informatique et Libertés s'applique à un responsable de traitement établi dans un pays hors UE uniquement dans l'hypothèse où ce dernier utilise des moyens de traitement situés sur le territoire français.

A l'article 41 du règlement, la Commission propose enfin une procédure rationalisée qui permettra la libre circulation des informations entre les Etats membres et les pays tiers. Elle rendra des décisions d'adéquation qui constitueront la reconnaissance du niveau adéquat de protection des données assuré par un pays non-membre de l'Union, du fait de sa législation nationale ou de ses engagements internationaux . Ces décisions d'adéquation seront rendues au niveau européen sur la base de critères explicites qui s'appliqueront aussi à la coopération en matière de police et de justice pénale. Dans le règlement, au considérant 82, la Commission prévoit d'interdire le transfert de données personnelles à un pays dont elle aurait préalablement constaté qu'il n'offre pas le niveau adéquat de protection.

Toujours pour favoriser la libre circulation des données, le règlement prévoit que les règles relatives aux transferts internationaux de données seront simplifiées : lorsque les transferts seront couverts par des règles d'entreprise contraignantes ou par des clauses contractuelles type de la Commission, l'autorisation préalable de l'autorité nationale compétente sera supprimée.

Le Parlement européen et les Etats membres, réunis en Conseil des ministres, doivent à présent examiner ces propositions qui feront probablement l'objet de débats houleux et de nouvelles prises de position par les autorités nationales de protection. Sous réserve d'adoption, le règlement entrerait en vigueur dans un délai de deux ans.

Jade TELLINI et Hélèna DELABARRE