Édito

L'Europe redéfinit la protection des données personnelles

Le 25 janvier 2012, la Commission européenne a entrepris de remettre en chantier une réforme globale de la protection des données personnelles en proposant à la fois un règlement européen pour la protection des données personnelles d'ordre commercial et leur circulation et une directive pour les données relatives aux affaires de justice et de police, d'enquêtes et de sanctions pénales. La précédente directive européenne, datant de 1995, a été diversement transposée dans les différents pays de l'Union. En particulier, cette directive ne l'a été qu'en 2004 en France, remettant partiellement en cause un certain nombre d'acquis de la loi Informatique et Libertés de 1978.

Quelles sont les raisons poussant la Commission européenne, suivie en cela par le Parlement européen qui a approuvé dans un rapport du 6 juillet 2011 la démarche de la Commission ?

Celle-ci avance trois arguments majeurs motivant cette évolution :

- le développement de l'Internet qui était balbutiant en 1995,
- la facilitation des échanges et du commerce des données personnelles pour favoriser la fluidité des marchés et leur développement,
- l'unification des législations européennes car la directive de 1995 avait été diversement transposée au sein des différents pays de l'Union.

Le but principal de la Commission européenne est de faciliter le marché unique numérique en développant le paiement électronique et de gagner la confiance des consommateurs dans ces systèmes. L'interopérabilité entre les différentes administrations nationales et les grandes entreprises est une nécessité sur le plan technique. Ce marché étant devenu mondial, l'échange des données hors de l'Europe avec les autres pays développés est devenu également une question cruciale.

Le projet de règlement supprime la déclaration des traitements automatisés par les entreprises. Cette mesure était réclamée à la fois par les adminis-

trations nationales et par les grandes entreprises et il est vrai que les moyens mis aux dispositions des différentes autorités de contrôle ne permettaient pas de traiter la masse des informations reçues. Comme contrepartie, le nouveau règlement prévoit un renforcement du pouvoir de sanction de la part des autorités de contrôle comme la Cnil en France, en cas de manquement grave à la législation sous forme de fortes amendes[1] et rend les responsables du traitement susceptibles d'être sanctionnés.

Le texte réaffirme également pour toute personne le droit fondamental à la protection des données personnelles la concernant. Cela se traduit par le fait d'imposer le choix de *« l'opt in »* aux sites marchands ou aux moteurs de recherche, c'est-à-dire un consentement explicite des internautes à l'utilisation de leurs données personnelles *« par un acte positif univoque »* comme le fait de cocher une case lorsqu'ils consultent un site Web. Souvent ce consentement n'est donné qu'en échange de services (informations et/ou logiciels gratuits).

Un autre point positif est consacré au droit à la portabilité (article 18 du règlement) présenté comme *« le droit d'obtenir auprès du responsable du 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... »* Ce qui devrait permettre au consommateur/internaute de faire jouer plus facilement la concurrence entre les prestataires de services.

Le droit à l'oubli fait également l'objet de l'article 17, mais cette intention louable de protéger les mineurs des informations qu'ils mettent en ligne sans réfléchir et de leur donner la possibilité d'exiger le retrait et la destruction de certaines de ces données se heurte à la réalité de l'Internet où l'effacement est quasi impossible en réalité. On ne peut jamais certifier que toutes les copies et toutes les références à un document ont bien été effacées.

Les insuffisances de certaines propositions du règlement et de la directive de la Commission ont été soulevées par la Cnil et le Groupe de l'article 29[2] :

* La directive dans le domaine de la police et de la justice manque d'ambition ; pour le G29 les protections devraient être de même niveau que dans le règlement et ne pas constituer des reculs pour certains pays.

* Des restrictions subsistent dans la définition des données à caractère personnel notamment sur la notion d'identifiant potentiel (par exemple l'adresse IP d'une machine personnelle).

1. « Les États membres devraient veiller à ce que les sanctions soient effectives, proportionnées et dissuasives, et prendre toutes mesures nécessaires à leur application. »
2. Groupe des réprésentants des autorités de contrôle (telle la CNIL) au niveau de l'Union européenne créé en 1996.

* Des exceptions sont accordées au service public.

* Un traitement ultérieur à des fins non compatibles avec la finalité initiale reste possible lorsque celui-ci peut trouver une autre base juridique.

Quels sont les recours possibles d'un internaute face à des violations de cette loi (informations personnelles divulguées, piratées, modifiées voire détruites accidentellement ou non). Alors que l'on pouvait s'attendre à ce que l'autorité de contrôle du pays où a eu lieu l'infraction soit l'organisme où la plainte puisse être déposée et traitée, la Commission européenne a tranché en faveur du « guichet unique » : les requêtes doivent être déposées auprès de l'autorité de contrôle dans le pays dans lequel le responsable du traitement a son « principal établissement ».

Comme beaucoup d'entreprises multinationales ont leur « établissement principal » hors de France (souvent en Irlande pour les entreprises informatiques), la Cnil a vivement réagi à cette mesure qui prive les citoyens de la protection de l'autorité de contrôle de leur pays et d'un accès simplifié aux autorités judiciaires.

Même le Groupe de l'article 29 demande *« un exercice effectif des droits de recours des citoyens, leur donnant la possibilité de se défendre devant le tribunal de leur résidence quelle que soit la procédure civile, pénale ou administrative choisie »*. On peut comprendre le choix de la Commission européenne de ne pas compliquer l'installation des entreprises multinationales en Europe dans le domaine des TIC pour relancer nos économies en difficulté, mais cela se fait au détriment de l'image de l'Europe vécue par les citoyens comme une entité bureaucratique lointaine.

Dans le cadre de la libéralisation du commerce électronique qui ne se limite pas aux frontières de l'Europe, la Commission européenne a choisi, en poursuivant la politique déjà engagée dans ce domaine avec les États-Unis[3], de définir elle-même le niveau adéquat de protection des données qui doit être assuré par un pays non membre de l'Union pour permettre les échanges. Le Groupe de l'article 29 *« considère que le champ d'application des dérogations aux règles d'encadrement des transferts est trop large et souhaite les limiter aux transferts non massifs et non répétitifs »*.

Enfin, comment ne pas s'étonner de l'importance donnée à la Commission européenne pour un grand nombre de décisions à prendre dans le domaine de la protection des données personnelles ? Le Comité européen de la protection des données regroupant les autorités de contrôle « indépendantes » prenant la suite du Groupe de l'article 29 est dirigé par le contrô-

3. Dossier des données passager (Passenger Name Record) : accord UE-USA.

leur européen de la protection des données[4] qui rend compte à la Commission européenne. Il semble que l'on veuille mettre en place une surveillance accrue du domaine de la protection des données personnelles qui est considéré comme ayant un impact important dans l'économie et le commerce électronique. Mais cela va de pair également avec des dispositions de plus en plus contraignantes dans le champ social (contrôle aux frontières…) et dans celui des libertés individuelles. ■

Jacques Vétois

4. Nommé par décision conjointe du Parlement européen et du Conseil européen pour un mandat de 5 ans. En place depuis 2001.