Protection des données personnelles : l'Europe ne veut voir qu'une seule tête

Le projet de règlement européen sur la protection des données personnelles pourrait être contesté par des Etats membres, tant il remet en cause les lois Informatique et libertés nationales. Les services en ligne pan-européens, plus responsabilisés, y verront des avantages.

Par Winston Maxwell, avocat associé, Hogan Lovells

Le 25 janvier 2012, la Commission européenne a publié sa proposition de règlement concernant la protection des données personnelles dans l'Union européenne (1). S'il était adopté, ce règlement remplacerait la directive « 95/46/CE » qui régit la protection des données personnelles en Europe depuis presque 17 ans. Le nouveau règlement remplacerait non seulement la directive de 1995, mais également la législation de chaque pays membre en matière de données personnelles.

Remédier à la cacophonie réglementaire

La loi française « Informatique et libertés » de 1978 disparaîtrait d'un trait de plume (2). Le choix d'un règlement est audacieux. Contrairement à une directive – outil qui laisse une marge de manœuvre au législateur national de chaque Etat membre –, un règlement ne nécessite aucune mesure de transposition. Il remplace purement et simplement la législation nationale en la matière, ne laissant aucune autonomie au législateur national.

La Commission européenne estime qu'il existe trop de divergences dans la mise en œuvre de la directive de 1995 et que ces divergences sont préjudiciables au marché intérieur. Sur ce point, elle a certainement raison. Une société qui souhaite mettre en œuvre un traitement de données personnelles au niveau européen devra gérer les exigences de 27 Etats membres différents. Certains pays exigeront une autorisation préalable, d'autres une simple notification et d'autres encore n'exigeront aucune formalité. Il est donc très difficile aujourd'hui pour une entreprise d'adopter une politique paneuropéenne en matière de protection de données personnelles, et il en résulte un coût certain pour elle et un frein pour la compétitivité européenne. L'exécutif européen a donc raison sur le diagnostic, face auquel il impose un remède de cheval : un règlement qui rendrait tout simplement inopérante la législation nationale de chacun des Vingt-sept en matière de données personnelles. La Commission européenne s'appuie sur le nouvel article 16 du Traité de l'Union européenne pour justifier son action. Cet article permet aux institutions européennes d'adopter des mesures pour garantir la protection des données personnelles au niveau européen, mais il ne précise pas de quelles mesures il s'agit. Le choix normal aurait été une directive, qui assure un équilibre entre les institutions communautaires et l'autonomie du législateur de chaque pays membre. Cet équilibre est exigé par le protocole n°2 du Traité, lequel impose aux institutions communautaires de respecter les principes de subsidiarité et de proportionnalité. Le projet de règlement sera probablement critiqué par certains Etats membres pour cette raison, les pays européens ne souhaitant pas abandonner entièrement leurs prérogatives législatives nationales en la matière (3).

Le choix d'un règlement est en revanche une bonne nouvelle pour les entreprises dont les activités sont paneuropéennes. Ce règlement leur permettra, pour déployer un service en ligne paneuropéen, de se mettre en conformité avec une seule loi européenne, au lieu de gérer l'existence de nombreuses lois européennes ayant parfois des exigences différentes. L'autre bonne nouvelle pour les entreprises est l'abolition de l'obligation de notifier les traitements de données personnelles à une autorité de protection des données personnelles. Dorénavant, les procédures de notification et d'autorisation seraient limitées à des traitements présentant un caractère de risque particulier pour le citoyen. L'ensemble des autres traitements n'exigerait aucune formalité préalable. Ils seraient exécutés sous la responsabilité de l'entreprise qui se verrait dans l'obligation de mettre en œuvre des procédures internes (dites « accountability principle ») pour garantir la conformité de ses opérations avec la loi.

Nommer un responsable « Data Privacy »

Ainsi, les entreprises auraient moins de contraintes en termes de notifications administratives mais davantage d'obligations en matière de procédures

Notes

(1) - Communication IP/12/46 de Viviane Reding datée du 25 janvier 2012 et intitulée *« La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises »*.

(2) - Une loi française sera nécessaire pour transposer la directive sur la protection des données personnelles en matière d'infractions pénales. La loi informatique et libertés pourrait donc servir de socle pour cette transposition.

(3) - En attendant, les acteurs souhaitant avoir une influence sur cette législation concentreront leurs efforts de lobbying sur le Parlement européen.

internes, afin de garantir la protection des données personnelles. Parmi ces nouvelles obligations figurent : l'obligation de nommer un délégué aux données personnelles pour toute entreprise de plus de 250 salariés, l'obligation de maintenir une documentation permettant de contrôler *a posteriori* la conformité des traitements, l'obligation d'effectuer des analyses d'impact (« privacy impact assessments ») pour des traitements présentant des risques particuliers, l'obligation de prévoir la protection des données personnelles au stade de la conception d'un produit (« privacy by design »). Ces obligations sont conformes aux tendances internationales, qui mettent l'accent sur la prise en compte de la protection des données personnelles en amont, au stade de la conception des produits (4), et la responsabilisation accrue des entreprises.

Sites web non-européens visés.

Le projet de règlement communautaire change en outre les règles en matière de loi applicable aux sites non-européens. Actuellement, la directive de 1995 permet à certains sites web non-européens d'échapper à l'application des lois européennes sur la protection des données personnelles, puisque ces sites n'utilisent pas des « moyens » en Europe. La Commission nationale de l'informatique et des libertés (CNIL) et d'autres autorités de protection des données personnelles ne partagent pas ce point de vue, estimant que l'utilisation de « cookies » par un site web non-européen est suffisante pour faire appliquer la législation locale.

Le projet de règlement mettrait fin à ce débat, en introduisant une règle selon laquelle un acteur non-européen serait soumis à la loi européenne dès lors qu'il offre des biens ou des services à un public en Europe (5), ou bien qu'il observe leur comportement.

Le nouveau règlement imposerait à toutes les entreprises une obligation de signaler les pertes de données personnelles. Il s'agit d'une obligation identique à celle qui pèse actuellement sur les opérateurs de communications électroniques. Il faudra informer la CNIL en France, mais également chaque personne concernée si la perte peut avoir un impact défavorable sur cette personne. Une obligation de ce type existe depuis plusieurs années aux Etats-Unis (6). Le texte proposé par la Commission européenne reste néanmoins controversé. En particulier, le délai de 24 heures suggéré par la Commission semble trop court compte tenu des expériences américaines en la matière.

Et ce n'est pas tout. Le règlement confèrerait aux citoyens un droit à l'oubli. Pour les juristes, ce droit à l'oubli est source de consternation. Premièrement, en quoi ce droit est-il différent du droit actuel ? La directive de 1995 confère à un citoyen le droit d'exiger la suppression des données le concernant. De plus, les entreprises ont déjà l'obligation d'effacer toutes les données personnelles dès lors qu'elles ne sont plus nécessaires pour l'objectif d'origine pour lequel elles ont été recueillies. Le droit à l'oubli semble redonder avec les dispositions actuelles. Deuxièmement, le droit à l'oubli rentre en collision avec d'autres droits fondamentaux, notamment lorsque le droit à l'oubli est utilisé par une personne qui souhaite effacer une partie de son histoire. Dans certains cas, ce souhait d'effacer son histoire est légitime et sera reconnu par la loi et les tribunaux (7). Dans d'autres cas, ce sera une violation de la liberté d'expression. Les tribunaux doivent les gérer au cas par cas, comme c'est prévu actuellement, et la création d'un nouveau droit ne semble pas opportune.

Un autre droit nouveau proposé par la Commission européenne est celui de la portabilité des données. La portabilité est bien connue des opérateurs télécoms qui doivent assurer la portabilité des numéros de téléphone. Le texte proposé va beaucoup plus loin, car il exigerait la restitution des données « dans un format structuré qui est couramment utilisé », et ce pour que la personne puisse transmettre ces données à un autre système. Il s'agit d'une mesure visant à réduire les coûts de changement (« switching costs ») entre prestataires et ainsi accroître la fluidité de la concurrence. Alors que cette mesure semble surtout avoir un objectif lié à la concurrence, la Commission européenne n'a entrepris aucune analyse de marché, et n'a constaté aucune défaillance du marché concurrentiel.

Portabilité pour plus de concurrence

La portabilité constitue une limitation forte à la liberté d'entreprise et pourrait avoir des effets dans beaucoup de secteurs : elle pourrait s'étendre aux banques, lesquelles auraient une obligation de restituer toutes les données du compte et notamment les informations sur les prélèvements dans un format permettant au consommateur de « porter » ces données à une banque concurrente. Il semble étonnant qu'une mesure aussi structurante pour la concurrence soit glissée dans un projet de règlement sur la protection des données personnelles. @

Notes

(4) - *« Privacy by Design »* est un concept créé par le commissaire à la protection des données personnelles à Ontario, Canada, Ann Cavoukian *(www.privacybydesign.ca).*

(5) - Il s'agit d'une règle similaire à celle utilisée par les tribunaux pour déterminer si la loi française en matière de propriété intellectuelle s'applique à un site web étranger.

(6) - Outre-Atlantique, on constate que l'obligation d'effectuer des notifications de perte de données crée une incitation forte pour les entreprises de mettre en œuvre des programmes efficaces de sécurité.

(7) - Des mesures particulières existent, par exemple pour garantir la confidentialité de certaines condamnations pour les mineurs.