Commission européenne – Réforme – Cnil

Le contrôle de la protection des données personnelles fait débat

Une proposition de réforme de la directive de 1995 sur la protection des données personnelles a été dévoilée le 25 janvier par la Commission européenne. Partiellement approuvé par la France, le projet ne suscite cependant pas le consensus.

Remis en question par le développement rapide d'Internet, le cadre réglementaire sur la protection des données personnelles instauré par la directive 95/46/EC de 1995 a besoin d'une mise à jour. C'est l'objectif principal de la réforme européenne en cours. Comme dans beaucoup d'autres secteurs économiques, l'application par les assureurs de la réglementation actuelle est loin d'être parfaite. L'anticipation des conséquences de la réforme à venir est d'autant plus capitale que cette dernière pourrait accentuer ce déphasage.

Sanctions élargies pour les autorités nationales...

Les assureurs sont très exposés aux risques résultant du traitement des données personnelles de leurs clients, tant en raison de leur volume que de leur nature. En effet, la plupart d'entre elles relèvent de la catégorie des données dites « sensibles », notamment en matière de santé. Chaque nouvelle réforme est marquée par un élargissement des pouvoirs des autorités de contrôle, ainsi que par un alourdissement des sanctions juridiques. Cela fut le cas lors de la réforme du 6 août 2004 modifiant la loi informatique et libertés [1], et cela risque d'être accentué par le projet en cours de discussion.

Par ailleurs, l'information des clients en matière de protection des données personnelles s'est considérablement améliorée, et l'utilisation devant les tribunaux de moyens tirés de violations de la loi informatique et libertés est de plus en plus fréquente, dans le but, notamment, de remettre en cause des droits ou des obligations. Particulièrement concernés, les assureurs vont devoir anticiper les nouvelles obligations et les modifications d'organisation à mettre en place.

La Commission européenne a fait également le constat que l'absence d'uniformité dans les réglementations mises en place par les États membres à la suite des transpositions nationales de la directive de 1995 a conduit à une grande complexité et à des coûts élevés pour les entreprises opérant sur les marchés de plusieurs États membres. C'est la raison pour laquelle un changement majeur est envisagé : la réforme prendrait la forme non pas d'une directive, mais d'un règlement. Ce dernier présente l'avantage d'être uniformément et immédiatement applicable dans l'ensemble de l'Union européenne.

Les autorités françaises soutiennent le principe d'une réforme de la réglementation en matière de protection des données personnelles, mais annoncent qu'elles s'opposeront à certaines de ses dispositions.

■ PAGES COORDONNÉES PAR EMMANUELLE BERNARD

... dont le rôle serait réduit au bénéfice de la Commission

En France, la Commission nationale informatique et libertés (Cnil) soutient le principe d'une réforme de la réglementation, pour que soient prises en compte les évolutions technologiques intervenues jusqu'à ce jour et afin d'introduire de nouveaux droits pour les citoyens : reconnaissance d'un droit à l'oubli, d'un droit à la portabilité de leurs données, et clarification des règles relatives au recueil du consentement et à l'exercice de leurs droits.

La Cnil approuve également l'objectif de réduction des formalités administratives des entreprises, dans la

Si le principe d'une réforme est salué, les critiques fusent sur les pouvoirs excessifs accordés à la Commission.

LES PROPOSITIONS FRANÇAISES DE MODIFICATION DU PROJET DE RÈGLEMENT

Les autorités françaises proposent, alternativement aux dispositions contestées dans le projet de la Commission européenne :

- qu'en cas de traitement de données ciblant spécifiquement la population d'un État membre, soit maintenue la compétence de l'autorité de contrôle de cet État, quel que soit le lieu d'établissement principal du responsable de traitement ;
- un rééquilibrage des compétences, qu'il est prévu de concentrer sur la Commission européenne, au profit des autorités de contrôle nationales, qui bénéficient non seulement de l'expertise technique et de l'expérience requises, mais également d'une plus grande proximité avec les citoyens ;
- un maintien des pouvoirs de contrôle et d'autorisation des transferts internationaux de données par les autorités nationales de contrôle.

mesure où ces dernières seront, par ailleurs, soumises à des obligations accrues en matière de protection des données : désignation obligatoire de correspondants informatique et libertés, mise en place de procédures internes pour assurer la mise en œuvre des principes de protection (notions d'*« accountability »* et de *« privacy by design »*, à savoir la mise en place d'audits et de registres, ainsi que la prise en compte de la protection des données dans les produits et services des entreprises dès leur conception, etc.), notification des violations de sécurité des données personnelles [2]...

Le renforcement des pouvoirs de sanction des autorités de protection nationales (amendes pouvant atteindre 2 % du chiffre d'affaires mondial de l'entreprise en infraction) et l'obligation d'une coopération accrue de ces autorités au niveau européen sont également accueillis favorablement par la Cnil.

Toutefois, toutes les propositions ne font pas consensus. En effet, la France s'oppose à la réduction envisagée du rôle des autorités de contrôle nationales et à l'accroissement des pouvoirs de la Commission européenne. La Cnil [3] mais également le Parlement [4] et le gouvernement français ont d'ores et déjà tenu à annoncer que certaines dispositions importantes seraient totalement contre-productives et qu'ils s'y opposeraient, à savoir :

– le principe retenu par le projet de règlement selon lequel l'autorité de contrôle compétente en matière d'application de la réglementation serait uniquement celle de l'État membre où se situe « l'établissement principal » de l'entreprise, quel que soit le public ciblé par son activité ;

– les mécanismes de coopération entre les autorités de contrôle nationales tels qu'ils sont actuellement prévus, qui sont trop lourds et trop limités (les notifications de failles de sécurité ou de traitements à risques à l'autorité nationale du lieu du principal établissement d'une entreprise ne seraient pas nécessairement communiquées aux autorités des autres États membres concernés par ces événements) ;

– la trop grande concentration de pouvoirs prévue par le projet de règlement au profit de la Commission européenne, au détriment des autorités de contrôle nationales. En effet, la Commission serait seule compétente pour élaborer les lignes directrices en matière de protection des données personnelles et pour définir les modalités précises d'application des nouvelles dispositions ;

– la simple procédure d'auto-évaluation par un responsable de traitement des conditions des transferts internationaux de données, qui échapperaient donc au contrôle des autorités nationales de protection.

Selon les autorités françaises, les risques soulevés par de telles dispositions seraient le trop grand éloignement des citoyens des autorités de protection nationales et les risques de pratiques dites de *« forum shopping »*. En l'occurrence, les entreprises seraient incitées, comme elles le font déjà au plan fiscal au sein de l'Union européenne, à privilégier une installation de leur principal établissement dans les États membres les moins exigeants, notamment en matière de contrôle et de sanction.

Même le Contrôleur européen exprime des réserves

Des autorités de contrôle d'autres pays membres ont également émis des réserves à la suite de la publication du projet de règlement, même si toutes saluent le principe d'une réforme. Dans un communiqué du 7 mars 2012, le Contrôleur européen de la protection des données personnelles (CEPD) a aussi fait part de nombreuses réserves sur ce projet. En particulier, il a critiqué « les pouvoirs excessifs accordés à la Commission dans le mécanisme destiné à garantir la cohérence au niveau des différentes autorités de contrôle ».

Les débats et actions de *lobbying* concernant le projet de règlement risquent donc de redoubler d'intensité au cours de l'année à venir, délai que Viviane Reding, vice-présidente de la Commission européenne, s'est fixé pour l'adoption de la réforme par les instances européennes.

■ THIERRY BERNARD, AVOCAT ASSOCIÉ DE LA SOCIÉTÉ D'AVOCATS QUADRIGE

À RETENIR

- La directive de 1995 sur la protection des données personnelles doit être réformée pour intégrer l'évolution des technologies.
- L'essentiel de la nouvelle réglementation relèvera d'un règlement, applicable en termes identiques dans tous les États membres.
- La France est favorable à la reconnaissance de nouveaux droits accordés aux citoyens, mais s'oppose à ce que le contrôle du respect de la réglementation par les entreprises soit uniquement du ressort de l'autorité de contrôle du pays où est implanté leur « établissement principal ».
- L'adoption définitive du règlement est attendue d'ici à fin 2012, pour une entrée en vigueur deux ans après.

1. Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

2. Généralisation de l'obligation s'imposant déjà aux fournisseurs de services de communications électroniques (article 34 bis de la loi n° 78-17 du 6 janvier 1978 modifiée) et aux hébergeurs de données de santé (article R. 1111-14, 1°, e du code de la santé publique), et qui fait déjà l'objet d'une proposition de loi adoptée par le Sénat le 23 mars 2010.

3. Communiqué de la Cnil du 26 janvier 2012.

4. Résolution européenne adoptée le 7 février 2012 par l'Assemblée nationale et le Sénat.