Le nouveau Règlement européen sur la protection des données personnelles : nouveautés et enjeux

publié le **31/08/2016**, vu **2453 fois**, Auteur : Maître Claire VINH SAN

Issu de la Directive Protection des données personnelles de 1995, le cadre juridique européen relatif à la protection des données à caractère personnel nécessitait d'être réformé afin de s'adapter aux nouveaux usages des technologies de l'information. Après quatre années de discussions et de négociations, c'est enfin chose faite suite à l'adoption du texte de Règlement européen sur la protection des données personnelles par le Parlement le 14 avril dernier.

Issu de la Directive Protection des données personnelles de 1995, le cadre juridique européen relatif à la protection des données à caractère personnel nécessitait d'être réformé afin de s'adapter aux nouveaux usages des technologies de l'information. Après quatre années de discussions et de négociations, c'est enfin chose faite suite à l'adoption du texte de Règlement européen sur la protection des données personnelles par le Parlement le 14 avril dernier.

Après le dépôt d'un premier projet Règlement européen sur la protection des données personnelles en 2012 et un nombre record d'amendements déposés – 3.999 amendements au total, soit un record – un texte de compromis a finalement été adopté au printemps 2016. **Le Règlement européen sur la protection des données personnelles - ou GDPR (pour *General Data Protection Regulation*) - sera ainsi applicable dès le 25 mai 2018.**

Il est donc nécessaire que les entreprises se mettent au plus vite en conformité avec ce nouveau texte, d'autant plus que les sanctions en cas de violation pourront aller jusqu'à **20.000.000 euros ou 4% du chiffre d'affaires annuel mondial en cas de violation pour le responsable d'un traitement de données.**

- *Sur le champ d'application territorial du texte :*

Il s'avère que les discussions autour du GDPR ont tenu compte des difficultés apparues pour appliquer la législation relatives à la protection des données aux responsables de traitement situés en dehors de l'Union européenne.

Ainsi, le GDPR sera applicable :

- aux traitements de données à caractère personnel liés **aux activités d'un responsable de traitement de données ou d'un sous-traitant sur le territoire de l'Union**, peu importe que le traitement de données à caractère personnel ait lieu sur le territoire de l'Union ;
-

aux traitements de données à caractère personnel **concernant des personnes localisées sur le territoire de l'Union**, peu importe leur nationalité ou leur lieu de résidence, notamment lorsqu'il s'agit de surveiller le comportement d'une personne pour autant que ce comportement ait lieu sur le territoire de l'Union.

1. **Sur les droits des personnes concernées par un traitement de données :**

L'ambition de ce texte est notamment d'imposer un droit plus protecteur en matière de données à caractère personnel.

A ce titre, le texte reconnaît textuellement le **droit à l'oubli numérique et à l'effacement** qui avait été précédemment admis par la Cour de Justice de l'Union européenne dans une décision du 13 mai 2014 et organise la mise en œuvre de celui-ci ainsi que ses exceptions.

Le GDPR créé le **droit à la portabilité des données,** permettant que les données soient transmises à un autre responsable de traitement à la demande de la personne concernée. Ce nouveau droit est d'ailleurs assez révélateur de la volonté de l'Union européenne de permettre aux personnes concernées par un traitement de reprendre « possession » de leurs données et de leur offrir un rôle plus actif dans la gestion de leurs données à caractère personnel.

On peut également évoquer le **droit à ne pas être soumis à une décision automatisée** , modifié par le GDPR. Il s'agit d'interdire toute décision fondée exclusivement sur un traitement automatisé de données à caractère personnel et produisant des effets juridiques ou affectant la personne de manière significative – on peut par exemple penser au fichier S. Le texte prévoit toutefois les exceptions à cette interdiction et notamment lorsque le traitement s'avère nécessaire pour des « *motifs d'intérêt public important* ».

Enfin, le GDPR prévoit que le **consentement d'un mineur sera licite à partir de 16 ans** , les Etats membres pouvant également prévoir un abaissement jusqu'à l'âge de 13 ans – cette disposition venant répondre à une réelle difficulté concernant l'usage des réseaux sociaux par les mineurs.

2. **Sur les obligations des responsables de traitement :**

Ce texte pose également de nouvelles obligations pour les responsables de traitement de données à caractère personnel.

Ainsi deux nouveaux principes font leur entrée :

- **le principe de protection des données dès la conception** (*data protection by design*) : qui oblige le responsable du traitement à prendre des mesures de protection dès la conception du produit ou du service impliquant un traitement de données – par exemple en collectant le minimum de données ou encore en prévoyant l'utilisation de pseudonymes ;

- **le principe de protection des données par défaut** (*data protection by default*) : qui oblige le responsable du traitement à prévoir, par défaut, les mesures les plus protectrices quant à la collecte des données à caractère personnel.

Ces principes sont toutefois limités par « *l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques »* mais ils montrent la volonté du législateur européen d'imposer aux entreprises une réflexion orientée vers la protection des données dans le développement de leurs produits et services.

En ce sens, les responsables d'un traitement de données seront soumis à un réel **devoir de transparence**, puisqu'ils devront par exemple notifier toute atteinte à l'autorité de contrôle compétente et informer les personnes concernées.

Certaines sociétés ont déjà donné l'exemple, comme la société LinkedIn qui a communiqué par mail à ces utilisateurs quant à un vol de données dont elle a été victime. Ce type de communication a d'ailleurs un impact positif à l'égard des utilisateurs de plus en plus sensibles à la question de la sécurité de leurs données personnelles qui sont ainsi tenus informés.

3. **Les nouveautés en matière de procédure :**

Les procédures entre les acteurs concernés (les personnes concernées par le traitement, le responsable du traitement, le sous-traitent ou encore l'autorité de contrôle) ont été davantage encadrées voire simplifiées dans une volonté de faciliter les rapports entre eux.

Ainsi, en cas de violation par le responsable d'un traitement de ses obligations, les personnes concernées pourront saisir l'autorité de contrôle de leur propre pays, quel que soit l'État membre dans lequel le responsable du traitement est établi. En conséquence, un utilisateur de Facebook en France pourra saisir directement la CNIL si Facebook ne respecte pas ses obligations en matière de protection des données.

Le texte met en place une nouvelle procédure dite de *« guichet unique »* qui permettra à une entreprise ayant plusieurs établissements dans différents États membres de n'avoir à traiter qu'avec l'autorité de contrôle de l'État membre dans lequel elle a son établissement principal pour l'ensemble de ses traitements.

Le texte vient également organiser la relation entre le responsable du traitement de données, son sous-traitant et le sous-traitant secondaire le cas échéant (ce qui règle les difficultés en cas de sous-traitance confiée à un tiers, fréquent en pratique).

Enfin, le CIL (Correspondant Informatique et Liberté) devient le **DPO** (pour *Data Protection Officer*) et voit son indépendance et son statut renforcés afin de remplir les différentes missions qui lui sont confiées. Sa désignation devient une obligation pour les entreprises appartenant au secteur public, les entreprises qui réalisent un suivi régulier et systématique des personnes *« à grande échelle »* du fait de leur activité principale ainsi que les entreprises amenées à traiter des données « sensibles » ou relatives à des condamnations, également *« à grande échelle »*.

La protection des données à caractère personnel doit véritablement être perçue comme une valeur ajoutée pour un produit ou un service – voire devenir un véritable outil marketing pour l'entreprise. Il est donc essentiel de travailler avec des juristes et avocats compétents en matière de protection des données à caractère personnel et d'anticiper cette nouvelle règlementation.