Morgan GRIT, *doctorante, Centre européen d'Études et de Recherche Droit & Santé, UMR 5815, université de Montpellier, juriste e-santé au GIP e-santé Occitanie*

Focus sur le règlement européen relatif à la protection des données à caractère personnel

Focus on the General data protection regulation

Contexte

La protection des données à caractère personnel est déjà un objectif connu depuis plusieurs décennies. La première loi dite « Informatique et libertés » de 1978 en a posé les jalons. Aujourd'hui, devant les risques de plus en plus nombreux – comme en témoigne l'affaire *Facebook-Cambridge Analytica* – il est nécessaire d'actualiser la réglementation afin de se conformer aux nouveaux usages et d'harmoniser l'ensemble des législations des États européens. La nouvelle ère s'ouvrira donc le 25 mai 2018, date de l'entrée en vigueur des 99 articles de ce texte. Pour rappel, contrairement à une directive européenne qui nécessite un texte de transposition pour être applicable en droit français, le règlement est d'applicabilité directe.

Objectif

Le premier objectif de cette réglementation est de protéger la vie privée des personnes physiques à l'égard des traitements de données à caractère personnel. Le deuxième objectif est d'harmoniser les législations des 28 pays européens en construisant un socle minimal obligatoire de protection. Chaque État est ensuite libre de renforcer sur cette base leur législation, comme c'est le cas en Allemagne.

Champ d'application

Le RGPD dispose d'un champ d'application extrêmement large. Il s'applique à tous les traitements de données à caractère personnel, automatisés ou non, effectués dans le cadre des activités d'un établissement, responsable de traitement ou sous-traitant, sur le territoire européen, que le traitement ait lieu ou non en Europe. Ce qui veut dire que les entreprises dont le siège est hors UE seront également concernées du seul fait que les données d'un citoyen européen soient traitées. En revanche, il ne s'applique pas aux données anonymisées pour lesquelles aucune identification d'un individu n'est possible. Il en va de même pour les données concernant des individus n'habitant pas sur le territoire européen et qui ne sont pas traitées en Europe, ainsi que les données concernant les personnes morales.

Contenu

Un changement de philosophie. On passe d'une logique administrative à une logique de responsabilisation des acteurs. En effet, le régime de déclaration des traitements de données auprès de la CNIL va être abandonné au profit de la tenue d'un registre

par le responsable de traitement. À l'image d'un livre de compte en compatibilité, l'ensemble des traitements de la structure devront être compilés dans un registre des activités de traitement dont le responsable de traitement aura la responsabilité. Ce registre permettra de démontrer et prouver qu'il a tout mis en œuvre pour se conformer à la réglementation. Pour cela, des outils ont été mis en place.

Outils de conformité

Devant les enjeux à la fois de conformité au RGPD, mais aussi financier en cas de sanction et d'atteinte à l'image, les entreprises doivent mettre en place un certain nombre de mesures de sécurité. Pour cela, de nouveaux outils humains et matériels ont été développés. Sans donner de liste exhaustive, le RGPD a notamment mis en place l'obligation pour certaines structures (organisme public par exemple) de désigner un délégué à la protection des données chargé de veiller au respect du règlement. Également, les structures doivent mettre en place des études d'impact sur la vie privée, réaliser des fiches de traitement de données, élaborer un code de conduite, etc.

De nouveaux droits

Le principal apport de ce règlement est d'instaurer de nouveaux droits pour les citoyens européens. Il compte notamment renforcer le droit à l'information (art. 13 et 14) en précisant l'ensemble des informations à fournir à la personne en cas de traitement de données. Il précise également les droits d'accès (art. 15), de rectification (art. 16), droit à l'effacement appelé aussi « droit à l'oubli » (art. 17), à la limitation du traitement (art. 18), à la portabilité des données (art. 20), droit d'opposition au traitement (art. 21) et au consentement explicite préalable à tout traitement. Le texte prévoit également la possibilité pour des associations d'introduire des actions de groupe.

De nouvelles obligations des acteurs

Le règlement instaure le principe d'*accountability*, qui marque la nouvelle logique d'autocontrôle et de responsabilisation des acteurs. En ce sens, la protection des données doit être assurée dès la conception du projet de traitement (art. 25) ou si le traitement a déjà commencé, une protection par défaut. Les acteurs, en cas de contrôle, devront rendre compte des mesures de protection effectuées. La charge de la preuve appartient donc au responsable de traitement, voire au sous-traitant qui voit sa responsabilité augmenter.

Conclusion

L'atout majeur de cette nouvelle réglementation est d'offrir à l'ensemble des pays membres un cadre très protecteur de données à caractère personnel. Cependant, il semble que de nombreuses difficultés de mises en œuvre sont attendues.