ARTICLE

M-11 : ÊTES-VOUS CONCERNÉ PAR LE RGPD ?

IT et données personnelles ANNULE - Concurrence, régulation européenne et FDI Contrats commerciaux et internationaux | 26/06/17 | Florence Chafiol

TECH & DIGITAL PROTECTION DES DONNÉES PERSONNELLES

Le **Règlement européen 2016/679** du 27 avril 2016 sur la protection des données personnelles (« RGPD ») entrera en application le 25 mai 2018. Parmi les principaux changements dus à l'entrée en application du RGPD figure son champ d'action extraterritorial. En effet, le RGPD étend et clarifie le champ d'application territorial de la législation européenne en matière de protection des données personnelles grâce à la mise en place de nouveaux critères d'applicabilité. Alors qu'à l'heure actelle la **loi Informatique et Libertés prévoit deux critères d'applicabilité que sont le critère de l'établissement** (c-à-d le fait que le responsable de traitement soit établi sur le territoire français) et **le critère des moyens** (c-à-d que le responsable de traitement, sans être établi sur le territoire de l'Union européenne (ci-après « UE »), utilise des moyens de traitement sur le territoire français), le **RGPD prévoit quant à lui deux critères différents que sont le critère de l'établissement et le critère du ciblage**.

Nous vous proposons d'analyser ci-dessous plus en détail les nouvelles questions à vous poser pour déterminer si le traitement que vous souhaitez mettre en œuvre relève ou non des dispositions du RGPD.

QUELLES SONT LES DONNEES CONCERNEES ?

Toutes les **données personnelles se rapportant à des personnes physiques identifiées ou identifiables directement ou indirectement**, notamment grâce à un identifiant.

> Sur ce point, le RGPD est similaire à la loi Informatique et Libertés.

QUELS SONT LES TRAITEMENTS VISES ?

Les **traitements automatisés et les traitements non automatisés (manuels) appelés à figurer dans un fichier.**

> Pas de distinction selon qu'il s'agit d'un traitement mis en œuvre par une personne physique ou une personne morale de droit public ou de droit privé.

A l'inverse, les traitements mis en œuvre par une personne physique à but exclusivement privé (activité strictement personnelle et domestique) ainsi que certains traitements mis en œuvre par les Etats Membres et les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales **ne sont pas concernés** par les dispositions du RGPD (d'autres textes européens leur sont applicables).

QUI DOIT RESPECTER LE REGLEMENT ?

2 critères : **le critère de l'établissement et le critère du ciblage :**

- Tous les **responsables de traitement** et tous les **sous-traitants établis** sur le territoire de **l'UE que le traitement ait lieu ou non dans l'UE** (critère de l'établissement) ;
- Tous les **responsables de traitement ou sous-traitants mettant en œuvre des traitements visant à fournir des biens et services à des personnes au sein de l'Union (y compris à titre gratuit) ou à suivre leurs comportements au sein de l'Union** (critère du ciblage).

> Peu importe la nationalité de la personne concernée, seul compte l'établissement des acteurs impliqués dans le traitement et le territoire dans lequel est fourni le bien ou le service.

QU'EST-CE QUI CHANGE EN PRATIQUE ?

> Le Règlement s'applique aux **responsables de traitements mais également aux sous-traitants** qui sont directement visés par certaines des dispositions du RGPD.

- Dans ce contexte, (i) la responsabilité du sous-traitant pourra être directement engagée par la personne concernée par le traitement, (ii) les **autorités de protection pourront également directement sanctionner les sous-traitants** dans les limites fixées par le RGPD (jusqu'à 2 à 4% du chiffre d'affaires annuel mondial ou 10 à 20 millions d'euros).
- Pour rappel, dans le cadre de la loi Informatique et Libertés, seule la responsabilité du responsable de traitement peut être engagée et lui seul peut être sanctionné par les autorités de protection des données et ce, même si le manquement est dû au sous-traitant.

> Le Règlement s'appliquera chaque fois qu'une **personne au sein de l'UE sera directement visée par un traitement de données à caractère personnel** (y compris par internet), **même si le responsable de traitement ou ses sous-traitants sont basés hors de l'UE.**

En réalité, ce nouveau critère permet de clarifier le champ d'application de la législation en matière de données à caractère personnel. Le critère du ciblage consacre finalement la doctrine et la jurisprudence extensives qu'avaient adoptées les autorités de protection des données (notamment la CNIL dans les sanctions prononcées à l'encontre de Facebook en 2017, de Google en 2011 et en 2014) et la Cour de Justice de l'UE (dans l'Affaire Google Spain) pour considérer que les dispositions européennes s'appliquaient à des responsables de traitement, notamment américains, qui estimaient qu'ils n'étaient pas établis au sein de l'UE, et n'utilisaient pas de moyens de traitement au sein de l'UE au sens de l'article 5 de la loi Informatique et Libertés, et qui considéraient donc que la règlementation européenne ne leur était pas applicable.

- Les responsables de traitement et sous-traitants qui ne sont pas établis au sein de l'UE ne pourront plus considérer que les dispositions du RGPD leur sont inapplicables à partir du moment où ils traitent des données à caractère personnel dans le cadre d'une offre de biens ou de services destinée à des personnes concernées au sein de l'UE ou suivent le comportement de ces personnes.

> Le Règlement réintroduit **la notion de « co-responsable de traitement »**, qui existait dans la Directive 95/46 mais qui n'avait pas été transposée au sein de la loi Informatique et Libertés.

- En pratique, cette notion pourra être utile dans certains cas de figure où les notions de « responsable de traitement » et de « sous-traitant » ne correspondent pas à la réalité des rôles de chacune des parties dans le traitement mis en œuvre.

ARTICULATION RGPD ET DISPOSITIONS LOCALES

- Le RGPD est d'application directe dans tous les Etats Membres. Toutefois, il prévoit 57 renvois au droit national, c'est-à-dire que les Etats Membres peuvent adopter sur 57 points précis, par le biais de lois ou textes locaux, des dispositions spécifiques qui s'appliqueront en plus de celles prévues par le RGPD. Ceci pourrait donc aboutir à des spécificités locales plus ou moins importantes selon les Etats Membres.

- La loi Informatique et Libertés et l'ensemble des dispositions françaises s'appliquant à des traitements réalisés dans certains secteurs spécifiques n'ont pas encore été modifiées suite à l'adoption du RGPD. Un projet de loi est attendu dans les prochains mois.

- A noter que le RGPD prévoit notamment (au titre des 57 renvois) que des dispositions nationales peuvent être adoptées pour la prise en compte des besoins des TPE/PME, pour le traitement du NIR, pour les traitements dans le cadre de relations de travail, etc.

LE RGPD EST-IL APPLICABLE ?

QUELQUES EXEMPLES PRATIQUES

Un responsable de traitement au sein de l'UE - Citoyen Américain - livraison d'un bien hors UE

Un **citoyen américain** commande une balance connectée via le **site internet d'une startup française.** Il fournit ses données personnelles (nom, prénom, adresse, informations de la carte de crédit américaine) pour pouvoir être **livré aux Etats-Unis.**

- **le RGPD est applicable,** le responsable de traitement est établi au sein de l'UE.

Un responsable de traitement hors UE - personne concernée au sein de l'UE - une livraison d'un bien au sein de l'UE

Un **citoyen européen** commande sur un **site internet d'ameublement américain** des meubles pour son appartement. Il procède à la commande en ligne et fournit des données personnelles (adresse personnelle, informations de la carte de crédit française) afin de se faire **livrer chez lui en France.**

- **le RGPD est applicable** car même si le responsable de traitement n'est pas établi dans l'UE, il met en œuvre des traitements visant à fournir des biens à des personnes situées au sein de l'UE.

Un responsable de traitement hors de l'UE - personne concernée au sein de l'UE - profilage au sein de l'UE

Un **citoyen européen** télécharge **une application mobile américaine gratuite** permettant de calculer ses performances sportives. Pour utiliser l'application, il doit s'inscrire en rentrant ses données personnelles (nom, prénom, âge, adresse email, préférence, centres d'intérêts etc.).

- **le RGPD est applicable** car même si le responsable de traitement n'est pas établi dans l'UE, il met en œuvre des traitements visant à suivre le comportement d'une personne située au sein de l'UE.

Un responsable de traitement hors UE - personne concernée au sein de l'UE - livraison en dehors de l'UE

Un **citoyen américain** en voyage en France commande (à partir d'un aéroport au sein de l'UE) sur un site internet d'ameublement américain des meubles pour son appartement. Il procède à la commande en ligne et fournit des données personnelles (nom, prénom, adresse personnelle, informations de la carte de crédit américaine) afin de se faire livrer chez lui aux Etats-Unis.

- **le RGPD n'est pas applicable** car le responsable de traitement n'est pas établi sur le territoire de l'UE et ne fournit pas de biens à des personnes situées au sein de l'UE.

Un responsable de traitement hors de l'UE - personne concernée au sein de l'UE - service hors de l'UE

Un **citoyen européen** en voyage aux Etats-Unis souhaite réserver une voiture de location à partir du **site internet d'une société américaine.** Il fournit ses données personnelles (nom, prénom, informations de la carte de crédit française etc.) afin d'obtenir le service sur le territoire américain.

- **le RGPD n'est pas applicable** car le service n'est pas fourni au sein de l'UE, et le responsable de traitement n'est pas établi au sein de l'UE.

ACTIONS DE MISE EN CONFORMITE

- Identifier les différents traitements de données personnelles mis en œuvre et les **analyser au regard des nouveaux critères d'applicabilité**, notamment au sein des groupes de sociétés implantés dans différents pays dans le monde ;
- **Pour les responsables de traitement et les sous-traitants établis en dehors de l'UE, analyser si le critère du ciblage** (offre de biens et de services dans l'UE ou au suivi du comportement des personnes au sein de l'UE) **est applicable au traitement mis en œuvre** ;
- **Identifier les différents rôles** (responsable de traitement / sous-traitant/ coresponsable de traitement) ;
- En cas de responsable de traitement ou sous-traitant situés hors UE, effectuer les démarches pour désigner un **représentant au sein de l'UE** et plus généralement entamer une mise en conformité globale au RGPD.