

L'ABCD du RGPD : (R)évolution ?

Le règlement européen N°2016/679 du 27 avril 2016 relatif à la protection des données personnelles (RGPD) entrera en vigueur le 25 mai 2018.

Il vient remplacer la Directive de 1995 en renforçant encore le régime que nous connaissons déjà de la protection des données issu de la loi du 6 janvier 1978 qui avait, entre autre, donné naissance à la CNIL.

Assurément à l'aire de la dématérialisation, de la relation 2.0 entre professionnels et particuliers et de la nébuleuse cloud, le RGPD vise surtout à défendre les droits des citoyens, à mieux les cyber protéger se dressant comme un pare feu réglementaire contre les GAFA et autres hébergeurs de la nébuleuse cloud.

Comment ?

A - En confirmant le droit d'accès aux données personnelles, le droit de rectification et encore le droit de s'opposer à un traitement des données.

B - En créant un droit à la portabilité des données qui permettra à tout consommateur de récupérer les données qu'il a fournies pour les réutiliser ou les transmettre à un tiers, et un droit à l'oubli par l'effacement des données.

C - En renversant la charge de la preuve puisqu'il appartiendra désormais aux opérateurs de données de prouver qu'ils respectent les dispositions du règlement selon un principe nouveau de responsabilisation et transparence qui vient renforcer le dispositif de formalités préalables, et en introduisant tout un aéropage de sanctions telles que la mise en demeure de l'entreprise, la suspension des flux de données ou des amendes s'élevant jusqu'à 4% de son chiffre d'affaires annuel mondial et la réparation du dommage matériel et/ou moral du citoyen.

D – En s'imposant à toute entreprise utilisant des données personnelles, quelle que soit sa taille, même si d'évidence les banques et les assureurs sont les premiers concernés.

L'ubérisation des rapports conduit aujourd'hui le RGPD à responsabiliser et sanctionner tant les entreprises exploitant elle—mêmes les données que leurs hébergeurs et fournisseurs de services, tous étant responsables de la sécurité des données.

Le chantier est colossal et c'est en ce qu'il suppose une mise en conformité des moyens logistiques et informatiques qu'il est révolutionnaire, il ne se contente plus de protéger moralement mais bien matériellement.

Tous les acteurs ne seront prêts pour le printemps 2018, on estime aujourd'hui à 1/3 seulement les entreprises qui ont mis en marche la mutation nécessaire de leurs services et moyens internes.

Elles sont pourtant nombreuses à être concernées puisqu'il suffit de collecter, classer et analyser des données relatives à un consommateur ou un salarié pour y être éligible.

Certes les contraintes elles-mêmes sont grandes, avant de traiter des données dites « à risque », les entreprises devront accompagner leur déclarations auprès de la CNIL d'une étude d'impact en matière de protection de la vie privée, elles devront reconfigurer leurs systèmes informatiques tout en se préservant d'un bug.

Si l'on peut imaginer que les PME puissent être accablées par cette nécessaire mise en conformité, celles-ci semblent pourtant les premières à entrevoir dans cette protection accrue du consommateur une opportunité concurrentielle.

D'une contrainte, il faut donc y avoir un avantage compétitif induit de la restauration du lien de confiance.

Voeu pieux ?

A n'en pas douter, cet ambitieux règlement qui se veut plus contraignant et coercitif que la précédente Directive se devait d'être pour sécuriser l'infini virtuel, mais ne devra son succès qu'à l'exercice de ses sanctions.

Le compte à rebours est lancé.

Il nous concerne tous.

Carine DETRE
Avocate