



Le RGPD, la sérénité après le vent de panique ?

Le 25 mai 2018, le règlement général sur la protection des données (RGPD) est entré en vigueur afin de renforcer et d'unifier, au niveau continental, la défense des données à caractère personnel des citoyens de l'Union européenne. La Cnil, régulateur français des libertés informatiques, définit ces données comme celles « *concernant des personnes physiques, identifiées directement ou indirectement* ». En résumé, chaque organisation traitant des identifiants, des noms, des numéros d'identification en ligne, des adresses emails, des données de localisation ou d'autres éléments caractéris-

tiques d'un individu précis, est dorénavant concernée par les normes imposées par ce nouveau texte.

Nouveaux droits, nouvelles obligations

Nouveau ? Pas tant que cela pour les entreprises françaises puisque les fondements du RGPD reposent sur la loi « informatique et libertés » datant de... 1978. Le consentement de la personne concernée par les données demeure obligatoire avant toute récupération et traitement. Par ailleurs, n'importe quel individu peut disposer d'un droit d'accès, d'un droit de modification et

d'un droit d'opposition pour le traitement de ses données. Le RGPD consacre pour autant de nouveaux droits aux citoyens, à l'instar du droit à l'oubli (ou droit à l'effacement de ses données), du droit à la limitation du traitement (limitation temporelle ou thématique) ou encore du droit à la portabilité des données (pour récupérer ses données et les transmettre à l'établissement alternatif de son choix).

Alors que les citoyens se sont désintéressés du sujet dans leur grande majorité, du côté des sociétés, l'arrivée du RGPD a été accueillie par une vague d'inquiétude. S'il était déjà difficile de respecter à la lettre

les différents articles de la loi de 1978, il semblait à première vue impossible d'être conforme aux obligations supplémentaires imposées par le règlement. « Ceux qui ont eu quarante ans pour se mettre en conformité sont aujourd'hui appelés aux spécialistes des données personnelles pour des interventions au jour le jour », constate Xavier Leclerc, CEO de Data Privacy Management System (DPMS). La sécurisation des traitements (via l'anonymisation et le chiffrement), le rehaussement des niveaux de sécurité par défaut, la nomination d'un délégué à la protection des données pour les sociétés de plus de 250 salariés, ou encore l'obligation d'élaborer un registre des traitements représentaient autant d'investissements inédits pour les organisations. Le coût moyen de mise en conformité avec cette réglementation obligatoire est estimé à 8 000 euros pour les PME et 65 000 euros pour les grandes entreprises*. Ces moyennes ne reflètent pas la grande disparité qui existe entre les différents niveaux de maturité des entreprises à ce sujet. Certaines sociétés ont plus de raisons que d'autres de s'inquiéter, et plus de trésorerie à dégager... L'anxiété générale était aussi entretenue par les sanctions prévues pour les contrevenants. Les amendes peuvent s'élever à 20 millions d'euros ou, dans le cas d'une entreprise, à

4 % du chiffre d'affaires mondial total (le montant le plus élevé étant retenu).

« Nul n'est censé ignorer la loi », et pourtant...

Malgré tout cela, le niveau de réactivité des entreprises reste faible. L'étude annuelle European Payment Report 2018, réalisée par Intrum (une entreprise suédoise de gestion de créances), souligne que 27 % des entreprises en Europe et 36 % des entreprises en France ne connaissent pas cette réglementation, un mois après son entrée en vigueur. En Grèce, ce chiffre progresse même jusqu'à 69 %. Xavier Leclerc, aussi président de l'Union des Data Protection Officer (UDPO), regrette que

« les TPE et PME ne se sentent pas concernées et souffrent d'un manque criant d'information ». Si les sociétés du CAC 40 se sont organisées pour être prêtes à la date butoir, les sociétés aux moyens plus limités ne se sont pas saisies du problème réglementaire. Xavier Leclerc tire la sonnette d'alarme pour ces entreprises : « En B2B, certaines sociétés n'ayant pas à traiter des données de clients individuels estiment être à l'abri des sanctions. C'est pourtant faux car elles doivent être conformes pour leurs données internes, notamment pour la gestion des RH, mais aussi des traitements de données externes, comme les coordonnées de leurs acheteurs directs. »

Un point en particulier inquiète Elizabeth Maxwell, spécialiste certifiée de la protection des données et directrice technique EMEA chez Compuware : « Les entreprises seront dans l'incapacité de se conformer au principe du droit à l'oubli du RGPD si elles ne peuvent pas localiser les données clients. » Dans ce contexte, 27 % des entreprises françaises « ne sont pas certaines » de savoir où sont stockées toutes leurs données**. Entre les serveurs internes, le cloud et les archivages papier, le travail préalable d'identification et de cartographie des données est plus complexe que jamais et ralentit la mise en conformité des organisations, même celles armées des meilleures intentions.

Malgré l'emballage médiatique du 25 mai, Xavier Leclerc l'affirme : « Les entreprises ne sont pas informées. Tant que nous n'aurons pas de vraies sanctions, le soufflet va redescendre pour les sociétés qui se sont intéressées au sujet de manière éphémère. » Après des mois de pédagogie plus ou moins fructueux, le premier coup de bâton du régulateur pourrait mettre les entreprises au pas. Ces dernières ont été harcelées de propositions, émises par divers prestataires (ESN, cabinets d'avocats, éditeurs de logiciels, cabinets de conseil...) quand d'autres ont fini par boudier le sujet. Seule la peur du gendarme pourrait alors s'avérer être le facteur nécessaire pour engager des travaux contraignants et complexes par nature. ♦

* Selon l'étude European Payment Report 2018
** Selon une étude de l'éditeur de logiciels Senzing

LES SOCIÉTÉS EUROPÉENNES D'AVANTAGE PRÉPARÉES QUE LEURS HOMOLOGUES BRITANNIQUES ET AMÉRICAINES

Dans l'Union européenne, 27 % des entreprises considèrent être en conformité avec les obligations instaurées par le RGPD

