Par Frédéric Forster, avocat, directeur du pôle Télécoms du cabinet Lexing Alain Bensoussan Avocats

LE COMPTE À REBOURS DU RGPD EST LANCÉ

Le Règlement général sur la protection des données personnelles entrera en application dans un an. La pression s'accentue donc pour les entreprises encore loin d'un état de conformité de type RGPD.[1]

Avocat à la Cour d'appel de Paris, Frédéric Forster dirige le pôle Télécoms du cabinet Lexing Alain Bensoussan Avocats depuis 2006. Il était précédemment directeur juridique du groupe SFR. Il est également vice-président du réseau international d'avocats Lexing.

Le Règlement général sur la protection des données a été adopté le 27 avril 2016 et publié au Journal officiel de l'Union européenne le 4 mai 2016. S'il est déjà entré en vigueur, il n'entrera cependant en application que le 25 mai 2018. Il a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel afin de prendre en compte les avancées technologiques, notamment numériques, et de réduire voire de supprimer les écarts juridiques entre les législations des États membres de l'Union européenne. Les entreprises ont donc un peu plus d'un an pour repenser leur gouvernance de protection des données personnelles et pour déployer l'ensemble des actions leur assurant une conformité totale avec le RGPD. Une gageure. En effet, il s'agit d'un texte complexe et technique qui va imposer de nouvelles obligations aux sociétés telles que :

- la réalisation d'analyses d'impact avant la mise en œuvre d'un traitement de données pouvant présenter des risques pour les droits et libertés des personnes ;
- la prise en compte de la protection de la sécurité des données dès la conception du traitement d'informations concerné ;
- l'obligation d'être, à tout moment, en mesure de démontrer la conformité du traitement avec le RGPD.

La quasi-totalité des entreprises traitant des données personnelles de citoyens européens est donc concernée par le Règlement.

Une exigence inédite qui implique d'être conforme en permanence à la loi

Le RGPD porte en germe près de 400 obligations, dont le contenu est précisé dans 99 articles, contextualisés dans près de 200 considérants. Les contraintes sont donc étoffées par le nouveau dispositif, et le rôle des intervenants à la collecte et aux traitements de données à caractère personnel souvent modifiés par rapport à ce qui prévalait sous l'empire de la directive de 1995 et de la loi française de 1978. Plus question, par exemple, pour l'entreprise qui réalise des prestations d'hébergement de données à caractère personnel pour le compte de ses clients de se retrancher derrière le statut de « sous-traitant » pour échapper aux obligations. Plus question non plus de parier sur la pratique décisionnelle de la Cnil, puisque les sanctions pourront atteindre 20 M€ ou de 4 % du C. A. mondial. Plus question enfin, de se contenter de réaliser les formalités déclaratives préalables auprès de la Cnil pour se considérer au meilleur niveau de conformité légale puisque la démarche est permanente. Elle doit correspondre à un état d'esprit général dans l'entreprise, qui doit réfléchir « protection des données » à toutes les étapes de son processus de gestion et de commercialisation. Ce processus, aussi désigné *« privacy by design »*, nécessite donc que la prise en compte du meilleur degré de protection des données à caractère personnel se fasse dès la conception des outils de l'entreprise. Ce principe s'accompagne de celui dit du *« security by default »*, au titre duquel les données à caractère personnel doivent, à tout moment de leur traitement, être gérées avec le plus haut niveau de sécurité possible, appliqué tant au plan physique que logique. L'un des corollaires de ces nouvelles règles est l'obligation de documenter l'ensemble des actions menées dans le cadre de ces deux obligations particulières, quitte à réaliser des analyses d'impact sur la sécurité des données, afin d'identifier et de suivre la mise en œuvre des décisions qui réduiraient voire supprimeraient ces risques. Les failles de sécurité seront également à notifier, non seulement à la Cnil, mais aussi aux personnes concernées et victimes, avérées ou potentielles, de ces failles. Les clients seront donc informés de ces lacunes, par la société elle-même. Enfin, beaucoup d'entreprises devront désigner un délégué à la protection des données chargé de la mise en œuvre de la conformité au RGPD. En somme, le compte à rebours a commencé, et force est de constater que l'entrée en vigueur du RGPD n'a pas nettement provoqué une prise de conscience des nouvelles obligations. D'ici à l'entrée en application, douze mois ne seront pas de trop pour s'atteler à une tâche qui sera, à n'en pas douter, immense pour beaucoup. ■

Les obligations des entreprises sont considérablement étoffées par le nouveau dispositif, et les rôles des intervenants à la collecte ou aux traitements de données à caractère personnel souvent modifiés.

[1] Lire également à propos du Règlement général sur la protection des données, la rubrique Avis d'experts, pp. 120 et 121.