Par Frédéric Forster, Alain Bensoussan Avocats Lexing [1]

LA SÉCURITÉ EUROPÉENNE N'EST PAS NÉGOCIABLE

Cinq mois après l'entrée en application du Règlement général européen sur la protection des données, quel bilan tirer en matière de mise en conformité des entreprises sur le terrain de la sécurité, et quelles actions prioriser ?

Le règlement européen 2016/679 relatif à la protection des données à caractère personnel (RGPD) est entré en application le 25 mai 2018. Il renforce les droits des personnes dont les données sont collectées et traitées ; il met en place un système de conformité que le responsable de traitement doit documenter. Si les droits des personnes sont ainsi renforcés, les obligations corrélatives des entités, privées ou publiques, sont considérablement étoffées, créant des programmes de mise en conformité au règlement un chantier inévitable. Sur le plan technique, le RGPD focalise toute sa puissance sur, d'une part, la protection de la confidentialité des données personnelles et, d'autre part, la sécurité : fiabilité de la collecte, des traitements réalisés, des échanges de données, sûreté contre les intrusions et les vols ou la corruption d'information, etc. Ces enjeux ne sont pas inédits car la loi Informatique et Libertés les incluait déjà. Néanmoins, le RGPD en augmente l'importance dans le dispositif global de conformité des organisations, et accroît considérablement le montant des sanctions. Sur le plan de la conformité, beaucoup d'entreprises n'ont pas attendu le 25 mai 2018 pour mettre en place des logiques de sécurité, le plus souvent pilotées par le RSSI ou le DSI. Mais, pour un nombre significatif d'entre elles, il est grand temps de se pencher sur ce sujet. Et plus généralement, toutes doivent intégrer dans leur *roadmap* de la conformité les principes issus du RGPD.

L'analyse d'impact pour prendre conscience des risques

Citons d'abord l'analyse d'impact relative à la protection des données (*privacy impact assessment* ou PIA), conçue comme un outil de prise de conscience, objectivée et systémique, des risques que pourraient subir les données personnelles détenues par les organisations, et des mesures afin d'amoindrir voire de supprimer les risques identifiés. Rappelons que le RGPD prévoit (art. 35) la conduite d'une telle analyse d'impact lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Par ailleurs, le RGPD rend obligatoire, dans la quasi-totalité des cas, la révélation, non seulement à la Cnil mais aussi aux personnes physiques touchées, de failles de données, c'est-à-dire d'atteintes à la sécurité ayant entraîné – ou pouvant entraîner – une altération des données à caractère personnel. Enfin, les données personnelles collectées, stockées et échangées peuvent être d'une particulière sensibilité, telles les informations médicales ou biométriques. Plus question de laisser celles-ci circuler librement, de réseau en réseau, d'ordinateur à ordinateur, sans que leur sécurité et leur protection soient garanties.

Défis techniques, juridiques et organisationnels

Cela suppose de lancer des chantiers techniques (implémentation d'outils logiciels, renforcement des mesures d'accès physique, mise en œuvre des mesures pour la suppression des risques révélés par une PIA, etc.), juridiques (renforcement des clauses avec les sous-traitants) et organisationnels (déploiement de PIA, cellules de veille interne, procédures d'alerte vers la Cnil et les personnes physiques, désignation de *data protection officers).* Il n'est pas peu dire que les organisations ne doivent sous-estimer ni la charge de travail associée au volet sécurité de leur conformité ni la rupture que le RGPD a marquée dans la sensibilisation des personnes aux questions de protection de leurs données. Ainsi, quelques mois seulement après l'entrée en application du RGPD, la Cnil vient d'annoncer que le nombre de plaintes qu'elle a reçues a bondi de 56 %. ■

« Ne pas sous-estimer le travail associé au volet sécurité de la conformité, et la rupture que le RGPD a marquée dans la sensibilisation des personnes »

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

Suite du dossier p. 114