Le RGPD organise la transparence en matière de violation de données personnelles

Par Thierry Dor, associé, Gide

Après Uber, c'est Facebook qui fait la une des journaux pour une affaire de faille de sécurité, concernant des millions d'utilisateurs, révélée très tardivement. La question est à la fois celle de la sécurité et de la confidentialité des données des utilisateurs mais aussi celle de la transparence vis-à-vis de ces utilisateurs lorsque les mesures de sécurité et de confidentialité n'ont pas permis d'éviter une faille entraînant la violation de leurs données.

Pour remédier à cette situation, de nombreux Etats américains dès 2001, l'Australie depuis le 22 février 2018 et maintenant l'Union européenne, ont décidé de mettre en place différents régimes organisant la transparence en matière de violation des données personnelles.

En France, il existait déjà dans la loi Informatique et Libertés une obligation générale de sécurité et de confidentialité des données personnelles. Ainsi, dans sa délibération remarquée sanctionnant un opérateur télécom en 2014, l'autorité française de protection des données (la CNIL) rappelait à l'opérateur son obligation de « *mettre en œuvre des moyens propres à assurer la sécurité des données de ses clients et notamment des mesures adaptées pour que ces données ne soient pas communiquées à des tiers non autorisés.* »

Désormais, avec le Règlement Général sur la Protection des Données ("RGPD"), applicable à partir du 25 mai 2018 dans l'ensemble des pays de l'Union européenne, il conviendra aussi de communiquer en présence d'une violation de données avérée.

L'article 4-12 du RGPD définit de façon large ce type d'atteinte comme toute « *violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.* »

Que les données n'existent plus, aient été corrompues, divulguées ou ne soient plus sous le contrôle du responsable de traitement, les articles 33 et 34 du RGPD introduisent non seulement une obligation de notification à l'autorité de protection des données compétente, mais également une obligation d'information des personnes dont les données ont été compromises, obligations lourdement sanctionnées.

Notification à l'autorité de protection des données compétente

Cette notification doit être effectuée « *dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.* » L'article 33 précise également que les informations caractérisant cette violation peuvent être communiquées de manière échelonnée, si l'analyse de l'incident se révèle complexe.

Le G29, qui regroupe les autorités européennes de protection des données, a publié des lignes directrices (Guidelines on Personal data breach notification under Regulation 2016/679, adoptées le 6 février 2018) afin d'aider les entreprises à se préparer à une situation de violation de données.

Concernant les délais de notification à l'autorité, selon le G29, un responsable du traitement doit se considérer comme ayant pris connaissance de la violation dès lors qu'il a une certitude raisonnable qu'un incident de sécurité s'est produit entraînant une atteinte aux données personnelles.

Cette notification à l'autorité de protection des données doit inclure une description de la nature de la violation, les catégories et le nombre approximatif de personnes concernées, le nombre d'enregistrements de données impactés, ainsi que les conséquences potentielles de la violation et les mesures prises ou envisagées pour y remédier ou en atténuer les éventuelles conséquences négatives. Le nom et les coordonnées du délégué à la protection des données, s'il en existe un, ou de tout autre point de contact, doivent également être fournis.

Sur l'auteur

Thierry Dor est avocat associé de Gide, en charge du droit des nouvelles technologies et des données. Thierry possède une expérience approfondie en matière de données personnelles, de projets informatiques, d'Internet, de commerce électronique, de logiciels et de bases de données. Il conseille notamment les clients français et internationaux du cabinet dans le cadre de la mise en œuvre de traitements de données complexes et de transferts internationaux de données personnelles. Il les assiste également dans leurs litiges liés aux technologies de l'information. Thierry a travaillé onze ans en entreprise en qualité de directeur juridique au sein de groupes internationaux confrontés aux questions relatives à la protection des données personnelles.

Enfin, même si aucune notification n'est faite à l'autorité de protection des données, l'entreprise se doit de documenter toute violation identifiée.

Communication aux personnes concernées

L'article 34 du RGPD prévoit que « *lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.* »

Le contenu de cette communication est similaire à celui de la notification à l'autorité de protection des données, à l'exception des informations concernant le nombre de personnes et d'enregistrements de données concernés.

Le RGPD prévoit des exceptions à cette obligation de communication aux personnes concernées. En effet, l'article 34-3 indique que cette communication n'est pas nécessaire si le responsable du traitement a mis en œuvre des mesures de protection techniques et organisationnelles appropriées, telles que le chiffrement des données, qui rendent les données inaccessibles pour toute personne non autorisée. De même, dès lors que le responsable du traitement a pris des mesures ultérieures suffisantes afin de limiter le risque pour les droits et libertés des personnes concernées, la communication à celles-ci n'est pas exigée. Enfin, lorsque cette communication requiert du responsable du traitement des efforts disproportionnés, il est possible de procéder à une communication publique (journaux, radios, internet…) ou à toute mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

L'autorité de protection des données peut toutefois ordonner au responsable du traitement de communiquer la violation aux personnes concernées après avoir examiné la notification de violation de données reçue du responsable du traitement.

A noter : dans le cadre de la modification de la loi Informatique et Libertés, en cours de discussion parlementaire, destinée à préparer l'entrée en application du RGPD, il est prévu une limitation à cette obligation de transparence lorsqu'elle est susceptible de « *représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique.* » Les traitements concernés par cette limitation feront l'objet d'un décret en Conseil d'État.

Sanctions

Le non-respect des obligations prévues par le RGPD en matière de mesures de confidentialité et de sécurité et en cas de violation de données à caractère personnel fait l'objet « *d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.* »

***

Cette nouvelle exigence de transparence vis-à-vis de l'autorité de protection des données et des personnes concernées s'ajoute donc aux impératifs déjà existants en termes de sécurité et de confidentialité des données personnelles. Les entreprises devront se préparer à cet exercice de transparence délicat, notamment compte tenu des délais très courts prévus par le RGPD. Ainsi, il est recommandé non seulement de prévoir des procédures de gestion de crise en matière de violation de données personnelles, mais aussi de les tester, en particulier au sein des groupes multinationaux, qui devront tenir compte du RGPD et des autres réglementations applicables. ■