CYBER-SECURITE : CLE DE VOUTE DU RGPD

La cyber-sécurité est au cœur de la réglementation européenne en matière de données personnelles depuis le 27 avril 2016, et ce dans son intitulé même : RGPD - Règlement Général sur la « *Protection* » des Données ; cette préoccupation concerne au premier chef les données des personnes physiques, mais la réglementation a également pour objectif de « *garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micro, petites et moyennes entreprises* » (cons. 13 RGPD).

Ainsi une section entière du RGPD est-elle consacrée à la sécurité des données personnelles, dont l'article introductif 32.1 dispose notamment que « *compte tenu... des risques* » (1) le responsable du traitement met en œuvre « *les mesures techniques et organisationnelles appropriées* » (2).

1. CYBER-RISQUES LIÉS AUX TRAITEMENTS

La détermination des mesures de sécurité à mettre en œuvre nécessite une analyse préalable des risques à la fois techniques (A) et stratégiques (B) auxquels sont confrontées les entreprises.

A. RISQUES TECHNIQUES

Les risques techniques, dont il est admis par le RGPD que « *le degré de probabilité et de gravité varie* », portent notamment sur la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel, ou encore sur l'accès non autorisé à de telles données, de manière accidentelle ou illicite (art. 32.2 RGPD).

Les causes de ces risques peuvent être multiples : humaines (salariés), parfois délibérées (concurrents) voire malveillantes (fraudeurs organisés) ; ou purement matérielles telles que des pannes (hardware ou software), des accidents (incendies, dégâts des eaux...) et autres sinistres (perte, casse...)

B. RISQUES STRATÉGIQUES

Il existe trois principaux risques d'attaque qui peuvent avoir des répercussions désastreuses sur la réputation et l'économie des entreprises : l'atteinte à l'image (action de déstabilisation consistant notamment à rendre un site internet indisponible ou à en modifier le contenu), la cyber-criminalité (attaque visant à soustraire des données pour les

Julie GRINGORE

utiliser frauduleusement ou rançonner leur propriétaire) et l'espionnage (accès discret à un système afin de capter les données souhaitées le plus longtemps possible).

Parallèlement à ces potentielles attaques extérieures, dans le cadre de leur stratégie de mise en conformité, les entreprises doivent également tenir compte des condamnations financières pouvant, à défaut, être prononcées par la CNIL ; ainsi, sur les 17 sanctions pécuniaires publiées par cette dernière en 2018 et 2019, 13 visent des défaillances en matière de sécurité – étant rappelé que les amendes administratives peuvent s'élever jusqu'à 20 000 000 € ou 4 % du chiffre d'affaires annuel.

*

C'est donc l'ensemble de ces risques qu'il convient d'anticiper lors de l'évaluation du niveau de sécurité à mettre en œuvre, afin de déterminer les mesures adaptées.

2. MESURES ADAPTÉES AUX CYBER-RISQUES

Parmi les « *obligations générales* » du responsable de traitement (Chap. IV – Section 1 RGPD), figure notamment celle consistant à prendre des mesures techniques (A) et organisationnelles (B) adaptées aux risques susvisés (art. 25.1 RGPD).

A. MESURES TECHNIQUES

Le Règlement donne lui-même quelques exemples de mesures pouvant être adoptées par les entreprises pour disposer d'un niveau de sécurité approprié, à savoir notamment la pseudonymisation et le chiffrement des données, et tous autres moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement, ainsi que de rétablir la disponibilité des données en cas d'incident (art. 32.1 RGPD).

Plusieurs guides pratiques traduisent pour les entreprises ces préconisations générales en mesures concrètes, tel le « *Guide d' hygiène informatique* » édité par l'ANSSI, tenant compte des évolutions récentes (télétravail notamment, en outre croissant avec la gestion de la crise Covid-19) et partant du constat selon lequel la sécurité n'est plus une option.

B. MESURES ORGANISATIONNELLES

La CNIL recense plusieurs précautions élémentaires à intégrer dans l'organisation des entreprises afin d'assurer la protection des données personnelles, consistant notamment à sensibiliser les salariés aux risques liés aux libertés et à la vie privée, et documenter les procédures de traitement de données ; rédiger une charte informatique en lui donnant une force contraignante, rappelant des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.

Il est également conseillé de disposer d'un plan de continuité d'activité pour anticiper la gestion d'évènements potentiellement bloquants (panne généralisée, attaque informatique...) ; et en cas de violation de données susceptible d'engendrer un risque pour les droits des personnes physiques, l'entreprise doit alors le notifier dans les 72 heures à la CNIL, voire à la personne concernée en cas de risque grave (art. 33 et 34 RGPD).

*

La cyber-sécurité permet ainsi de mettre en œuvre les mesures techniques et juridiques adaptées à des risques préalablement identifiés ; elle offre ce faisant l'avantage de préserver la valeur que représentent ces données, en renforçant au surplus le capital confiance de l'entreprise auprès de sa clientèle.

***

Julie GRINGORE
DERBY Avocats

www.village-justice.com

n°78
[Septembre - Octobre 2020]

Le Journal du Management
juridique et réglementaire

La revue pour les services juridiques d'entreprises et collectivités