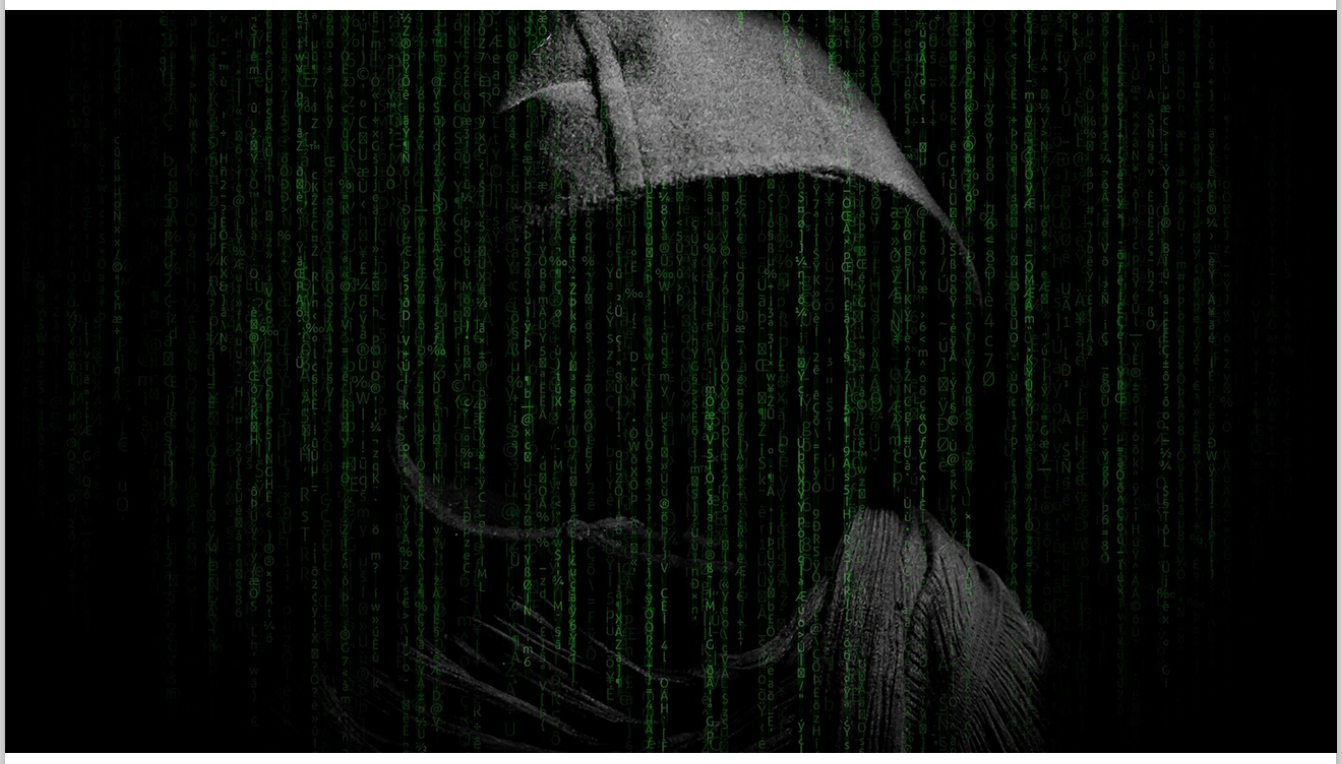
LIMITEZ VOTRE RISQUE CYBER EN MISANT SUR LE RGPD

30 mai 2022



Crédits photo : Madartzgraphics, Pixabay

La dématérialisation des échanges, le développement du télétravail, ou encore l'adoption massive de l'e-commerce, ont amplifié l'enjeu de la protection des données. Dans ce contexte, le risque Cyber a littéralement explosé, avec une augmentation de **plus de 250% des cyberattaques entre 2019 et 2021**. Ciblant les ressources vulnérables de l'entreprise pour disposer d'un point d'entrée (serveurs, équipements périphériques, réseaux, humains), les pirates prennent le

contrôle du système d'information dans lequel ils s'introduisent pour mener ensuite des actions visant à porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité des données de l'entreprise.

Tentatives d'intrusion aux multiples visages, les attaques par phishing, usurpation d'identité, par rançongiciels ou déni de services (Ddos) deviennent le quotidien des DSI.

Au sein de son « *Panorama de la menace informatique* » publié en 2022, l'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) met en évidence le constat selon lequel l'ensemble des acteurs (entreprises, administrations, etc…) sont susceptibles d'être attaqués. Les cyberattaques ne visent pas que les grandes entreprises mais également, les TPE, PME et ETI représentant, selon l'ANSSI, **34% des victimes en 2021**.

Face à ces cybermenaces, **le Règlement Général sur la Protection des Données** (le « RGPD ») impose à tout acteur du marché de revoir sa gouvernance et d'améliorer ses pratiques afin de protéger la vie privée de ses salariés, usagers et clients. En effet, responsables des traitements qu'elles mettent en place, les entreprises et administrations doivent démontrer le respect de leurs obligations sous peine de sanctions (principe d'**Accountability**).

A ce titre, le RGPD impose la mise en place de mesures qui permettent, in fine, de prévenir et lutter contre les risques cyber. L'objectif du RGPD rejoint celui de la sécurité informatique et permet ainsi aux entreprises **d'accroître leur protection des données à caractère personnel et leur sensibilisation à la cybersécurité**.

L'enjeu est donc important pour les responsables de traitement car la **CNIL**, l'autorité de contrôle française, a le pouvoir d'imposer des amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

A titre d'illustration, la CNIL a pu sanctionner tant un médecin généraliste à hauteur de 3 000 euros, qu'un groupe de télécommunication à hauteur de 300 000 euros ou un fournisseur de logiciel à hauteur de 1 500 000 euros pour manquement à l'obligation d'assurer la sécurité des données. Il s'agit d'ailleurs de l'un des motifs les plus récurrents de sanction en France.

Or, respecter leurs obligations au titre du RGPD permet aux entreprises de limiter le risque cyber *a priori* mais également de leur assurer une meilleure réactivité *a posteriori*.

Prenons l'exemple du début de l'année 2021 qui a été marque par des attaques cyber de plusieurs hôpitaux. Les cyber-attaquants ont principalement eu recours à des « rançongiciels », un programme malveillant chiffrant les données de la victime et dont le but est d'obtenir de cette dernière paiement d'une rançon en échange de la clef de déchiffrement.

Afin de mieux prévenir ce risque d'attaques, le respect des principes du RGPD et la mise en place de plusieurs mesures techniques et organisationnelles ne doivent pas être négligés. Régulièrement, les cyberattaques mettent en lumière le manque de protections entourant les systèmes d'information des entreprises victimes. Une fois ces lacunes révélées, les cyberattaques peuvent aboutir à des contrôles de la CNIL et le prononcé consécutif de sanctions administratives à l'égard de l'entreprise qui n'avait pas respecté son obligation de sécurité des données personnelles. Double peine pour ces entreprises, qui subissent coup sur coup cyberattaque, contrôle, sanction et potentiellement, un impact réputationnel important.

Dès lors, **le respect du RGPD doit être regardé comme une opportunité pour les entreprises**, qui peuvent adapter leurs procédures et mesures de sécurité internes à leurs besoins spécifiques, le RGPD leur laissant la latitude nécessaire pour se responsabiliser d'elles-mêmes.

Mais certains principes sont impératifs. Par exemple, le RGPD impose aux responsables de traitement **de ne traiter qu'un minimum de données à caractère personnel**, celles strictement nécessaires à la réalisation de l'objectif poursuivi par leur traitement. Ainsi, moins les données d'une personne sont collectées, moins le risque d'atteinte à sa vie privée sera important, notamment en cas de cyberattaque.

De plus, **les entreprises doivent respecter la vie privée des personnes par défaut et dès le début du processus de conception d'un nouveau projet**, produit ou service. Dès lors, l'adoption préalable de mesures protectrices des données personnelles permet aux entreprises d'anticiper et de limiter les risques d'atteinte à la vie privée des personnes concernées.

Certaines mesures techniques et organisationnelles sont préconisées directement au sein du texte, ce dernier incitant par exemple les responsables de traitement à **pseudonymiser** leurs données. Cette technique consiste à remplacer les données directement identifiantes (nom, prénoms, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Ainsi, en cas d'attaque visant à divulguer des données sensibles telles que l'état de santé d'une personne, pseudonymiser les données pourra limiter l'impact de l'attaque.

Le RGPD incite également les entreprises à **chiffrer leurs données** afin de protéger leurs documents en les rendant illisibles par toute personne n'ayant pas accès à la clef de déchiffrement. De cette façon, un attaquant qui souhaiterait accéder aux données pour potentiellement les divulguer ou les revendre ne pourrait pas accéder aux données en clair, le chiffrement faisant potentiellement office de dissuasion.

En outre, **disposer de plusieurs sauvegardes** afin d'éviter de paralyser son activité lors d'une cyberattaque est une mesure qui peut être mise en place par les responsables de traitement. Elle leur permettra, d'une part, d'assurer leur conformité au RGPD et, d'autre part, de se protéger. A ce titre, la règle du « 3-2-1 » veut que toutes les données soient copiées 3 fois, dans 2 types de supports différents (cloud et disques durs par exemple) dont 1 hors site (pour prévenir les risques d'incendie, de vol ou d'inondation notamment).

Ces mesures techniques doivent être complétées par **des mesures physiques**, dès lors que l'entreprise dispose de locaux. Afin de prévenir les accès non autorisés dans les locaux, des alarmes de sécurité, la journalisation des accès ou le recours à des systèmes de vidéosurveillance peuvent ainsi être nécessaires pour protéger les données sous format numérique et papier.

La formation et **la sensibilisation** du personnel sont indispensables, le risque humain étant un facteur non négligeable en matière de cybersécurité. A ce sujet, la CNIL a constaté que les attaques par rançongiciel résultaient très régulièrement du téléchargement d'un fichier malveillant reçu par hameçonnage, adressé sur une messagerie autre que celle de l'établissement, mais dont le message aurait été ouvert depuis un poste de travail en interne.

Prévoir un plan de continuité de l'activité (« **PCA** ») et un plan de reprise de l'activité (« **PRA** ») permettra aux entreprises de prévoir en amont la stratégie à adopter pour assurer la poursuite de son activité pendant l'attaque et sa stratégie de sortie de crise.

Dans une logique de conformité, l'entreprise doit organiser une gouvernance robuste destinée à contrôler régulièrement l'environnement dans lequel ses données sont traitées, en organisant **des audits internes de ses systèmes** (tests d'intrusion). Elle ne devra pas non plus négliger de **contrôler l'infrastructure technique de ses sous-traitants**, au moment de la conclusion du contrat mais également au cours de son exécution. En outre, sa gouvernance permettra d'assurer le suivi de la mise en place de nouveaux traitements susceptibles d'accroître le risque de cyber-attaques selon la sensibilité des données et/ou du dispositif technique retenu (lors de l'externalisation de données vers un cloud par exemple). **Le suivi des failles de sécurité** ou **des fuites d'information** ne doit pas non plus être oublié au regard de l'obligation de notifier les violations de données personnelles à laquelle est tenu le responsable de traitement.

Ces mesures, qui ne sont que des exemples, ont un double intérêt pour les entreprises : assurer leur conformité à des obligations règlementaires issues du RGPD ; limiter les risques et l'impact des cyberattaques et prendre en compte, dès la conception des projets, les enjeux liés à la cybersécurité.

La CNIL, dans son rapport annuel 2021, a d'ailleurs fixé comme deuxième axe stratégique la promotion du RGPD comme **atout pour la confiance**, **l'image** et **la compétitivité des entreprises**. Selon l'autorité, la conformité RGPD est « *la meilleure prévention contre les risques cyber* ».

Or, aujourd'hui, l'immense majorité des entreprises et des organismes fonctionnent grâce à des outils et services numériques. Le risque d'une cyberattaque pèse théoriquement sur tous les organismes. Protéger leurs actif immatériels, leurs bases de données et leurs systèmes d'information est une priorité pour ces acteurs, que le respect du RGPD aidera à parachever.

Article rédigé par :

Antoine Gravereaux

Avocat Associé

DS AVOCATS

Valentine Chauveau

Avocate

DS AVOCATS

Disposant d'une équipe de spécialistes en droit du numérique, DS Avocats vous accompagne dans la conformité de vos traitements de données personnelles et dans la gestion du risque cyber.