Chapitre 4
Sécuriser les traitements

1. Introduction

L'évolution des technologies de l'information (Cloud computing, Big Data, médias sociaux, etc.), la prolifération et la puissance des outils technologiques, le succès d'Internet et la multiplication des acteurs du secteur ont pour conséquence un foisonnement exponentiel des collectes et des traitements de données à caractère personnel. En parallèle, les menaces pesant sur les systèmes et réseaux d'Information sont de plus en plus nombreuses (fraude informatique, captation frauduleuse, perte de données, atteinte à la confidentialité, à la vie privée, etc.) et diverses (internes, externes). Le système d'information est dès lors utilisé comme vecteur de ces menaces qui consistent à viser le fonctionnement de ce dernier et/ou les données qu'il contient.

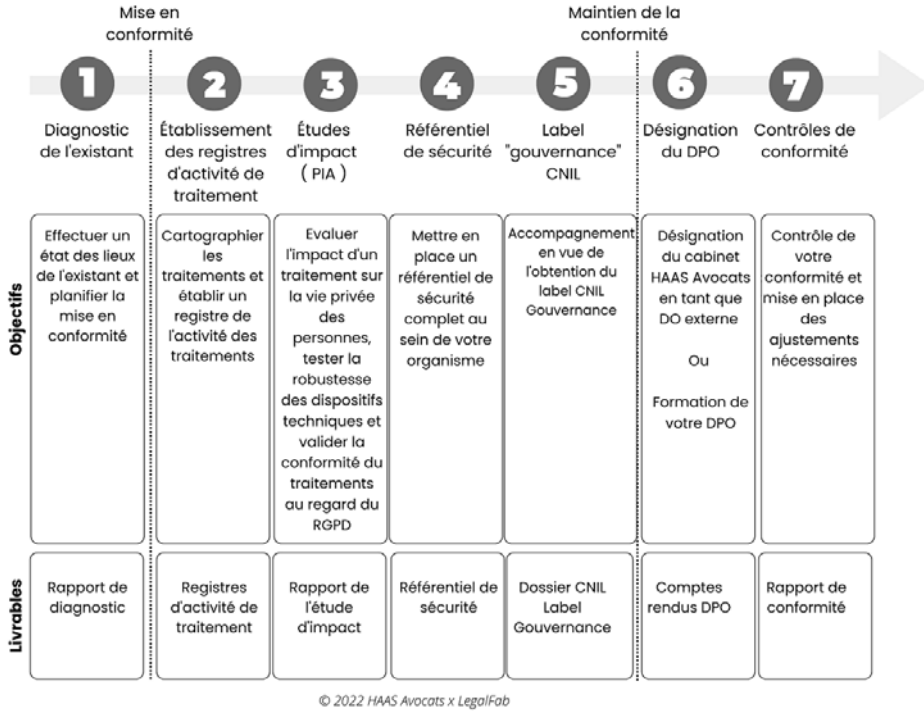
Soulignons qu'il n'existe pas de définition légale de la sécurité. Toutefois, l'agence nationale de la sécurité des systèmes d'information (ANSSI) définit la sécurité des systèmes d'information comme « *l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre et qui rend accessible* » (Défense et sécurité des systèmes d'information-Stratégie de la France, ANSSI 2011, p. 21 & 22).

La CNIL a d'ailleurs récemment rappelé que la cybersécurité du Web français était une thématique prioritaire (et a contrôlé en ce sens vingt-et-un organismes en 2021 pour, au final, en mettre quinze en demeure pour des défauts de chiffrement des données ou de gestion et de sécurisation de comptes d'utilisateurs (CNIL – Cybersécurité : 15 mises en demeure à l'encontre de sites web insuffisamment sécurisés – 08/07/22)).

En effet, la CNIL avait annoncé que l'un de ses objectifs était de contrôler le niveau de sécurité des « sites web français les plus utilisés dans différents secteurs ». Pour ce faire, la CNIL se concentrera sur :

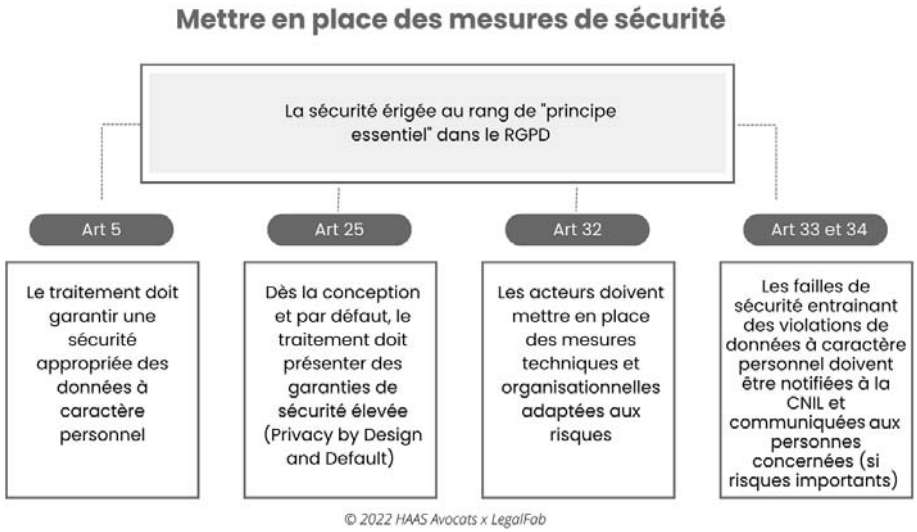
– les formulaires de recueils de données personnelles ;
– l'utilisation du protocole https ;
– la conformité des acteurs à la recommandation de la CNIL sur les mots de passe ;
– les stratégies mises en place pour se prémunir contre les rançongiciels.

(CNIL – Cybersécurité, données de santé, cookies : les thématiques prioritaires de contrôle en 2021 – 02/03/2021)



2. Qui est concerné par l'obligation de sécurité ?

Le RGPD, en introduisant une obligation générale de sécurité qui se traduit par la mise en œuvre des **mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque, érige la sécurité en pilier de la *Compliance*. L'objectif est ici de responsabiliser les différents acteurs des traitements de données en uniformisant les obligations pesant sur les entreprises (publiques ou privées). Ces nouvelles exigences sont valables pour les traitements futurs comme pour ceux déjà mis en place.



Tous les acteurs du traitement sont concernés par l'obligation générale de sécurité introduite par le RGPD, du responsable de traitement au sous-traitant qui doit désormais présenter « *des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* » (RGPD, art. 28).

Ces mesures visent à empêcher notamment toute diffusion ou accès non autorisé, la destruction accidentelle ou illicite, la perte accidentelle ou l'altération, ainsi que toute autre forme de traitement illicite.

Le devoir de sécurité comprend trois obligations distinctes : l'obligation de sécurisation, l'obligation de notification et l'obligation de communication, étant précisé que la deuxième et la troisième sont le prolongement de la première :

– L'obligation de sécurisation consiste à empêcher toute violation de données à caractère personnel, et d'une manière générale à limiter l'accessibilité aux données ;
– L'obligation de notification consiste à notifier à l'autorité de contrôle toute violation de données à caractère personnel ;

– L'obligation de communication consiste à communiquer toute violation de données à la personne concernée, si cela engendre un risque élevé pour les droits et libertés.

Le règlement indique différentes mesures techniques et organisationnelles à mettre en œuvre, selon les risques, en particulier la pseudonymisation et le chiffrement des données, la capacité d'assurer, de manière permanente, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services du traitement (RGPD, art. 32,33 et 34).

3. Pourquoi mettre en place des mesures de sécurité ?

Comme nous venons de le souligner, la sécurité constitue un élément de conformité incontournable et la plupart des acteurs du traitement devront accroître leur dispositif existant pour se mettre en conformité. Mais outre le volet légal, la sécurité doit aussi être abordée sous le volet économique, avec l'explosion du cyber-risque dont le montant du préjudice est de plus en plus élevé chaque jour. Nous vivons en effet dans une société du tout numérique, du tout connecté, du tout partagé. Mais derrière l'accroissement de la facilité d'accès aux données se cache l'accroissement des failles de sécurité possibles. Imaginez un voleur face à une première maison comprenant une porte d'entrée blindée, et une seule fenêtre protégée par des barreaux de fer, et une seconde maison avec trois portes d'entrée, deux baies vitrées, et une flopée de fenêtres ouvertes. À votre avis, où va-t-il aller ? Le problème est exactement le même en matière de sécurité informatique, et la recette du butin peut être très juteuse. D'après l'IBM Security Cost of a Data Breach Report 2021, les coûts des violations de données sont passés de 3,86 millions USD à 4,24 millions USD, soit le coût total moyen le plus élevé de l'histoire du rapport. Les coûts ont été :

– largement inférieurs pour plusieurs organismes ayant une stratégie de sécurité plus aboutie ;
– et plus élevés pour les organismes ayant pris du retard dans des domaines tels que la sécurité (IA), l'automatisation et la sécurité du cloud.

Il est intéressant de noter que le coût moyen des violations de données est supérieur de 1.07 million USD dans le cas où le télétravail était impliqué dans lesdites violations.

Ce même rapport estime que les données à caractère personnel des clients sont également les plus coûteuses, à 180 USD par fichier perdu ou volé. Le coût moyen global par donnée dans l'étude de 2021 était de 161 USD, une augmentation par rapport aux 146 USD par fichier perdu ou volé évoqué dans le rapport de 2020.

À l'échelon français, dans son « Panorama de la menace informatique » 2021, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) observe une amélioration constante des capacités des acteurs malveillants. Ainsi, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37 % entre 2020 et 2021 (786 en 2020 contre 1082 en 2021, soit désormais près de 3 intrusions avérées par jour).

La CNIL elle-même précise que 5037 notifications de violation de données ont été reçues en 2021 soit une augmentation de 79 % par rapport à 2020. Le fort impact des rançongiciels dans les crises de cybersécurité se confirment dans la mesure où 43 % de ces notifications concernent une attaque par rançongiciel (CNIL – Cybersécurité : 15 mises en demeure à l'encontre de sites web insuffisamment sécurisés – 08/07/22). Cette tendance ne semble pas près de stagner et des mesures de sécurité fortes doivent nécessairement être mises en place pour protéger le patrimoine informationnel de l'entreprise. De plus, les préjudices pour les entreprises sont multiples : atteinte à la réputation et à l'image, perte de confiance des utilisateurs, perte d'un savoir-faire, perte d'un avantage concurrentiel à la suite de diffusion de données stratégiques…

Il est dès lors primordial pour une entreprise de prévenir les risques qui pèsent sur ses systèmes d'information et de prendre des mesures correctives et préventives afin d'endiguer ces derniers. À ce titre, elle doit veiller à la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information et dans certains cas également de l'authenticité, de l'imputabilité, la non-répudiation et la fiabilité de cette dernière.

Un risque est caractérisé par trois composantes :

– la menace ;
– les vulnérabilités ;
– les impacts.

Atteintes aux données

La sécurité informatique ne se mesure que par sa résistance à une menace ou à une faille dans son système de traitement. L'attaquant (cracker ou hacker) cherchant avant tout à porter atteinte à l'état du système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

L'**atteinte à la disponibilité** réside dans le fait que les données (annuaire des fournisseurs, dossier patient, inventaire de pharmacie…) ou les traitements (application, web service, composant logiciel…) soient inaccessibles au moment prévu pour leurs usages autorisés.

L'**atteinte à la confidentialité** se caractérise par la mise à disposition non-autorisée de données qui deviennent accessibles à des utilisateurs non-habilités à les consulter.