Sanctions RGPD :
Quels enseignements pratiques pour un DPO, pour un RSSI?

Maître Garance Mathias

Avocat associé – Fondateur, Mathias Avocats

Membre de l'AFCDP

Quelles sanctions sous le RGPD ?

Les autorités de contrôle peuvent choisir parmi un panel de mesures correctrices.

L'amende administrative (sanction pécuniaire) n'est pas la seule mesure prévue par le RGPD.

Les autorités doivent choisir la mesure la plus efficace et adaptée.

Les mesures correctrices (RGPD, article 58, 2., Loi I&L, articles 20 et suivants)

Avertissement (lorsque les opérations de traitement envisagées sont susceptibles de violer le RGPD)

Rappel à l'ordre (lorsque les opérations ont entrainé une violation du RGPD)

Mise en demeure de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits

Mise en demeure de mettre les opérations en conformité

Mise en demeure de communiquer à la personne concernée une violation de données

(sauf pour les traitements qui intéressent la sûreté de l'Etat ou la défense)

Imposer une limitation temporaire ou définitive, y compris une interdiction du traitement

(sauf pour les traitements qui intéressent la sûreté de l'Etat ou la défense)

Mise en demeure de rectifier, d'effacer ou de limiter le traitement et de notifier les destinataires de ces mesures

Retirer une certification

Imposer une amende administrative

Ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale

Injonction de mise en conformité sous astreinte dont le montant ne peut excéder 100 000 euros par jour de retard

Suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale

Focus : la mise en demeure

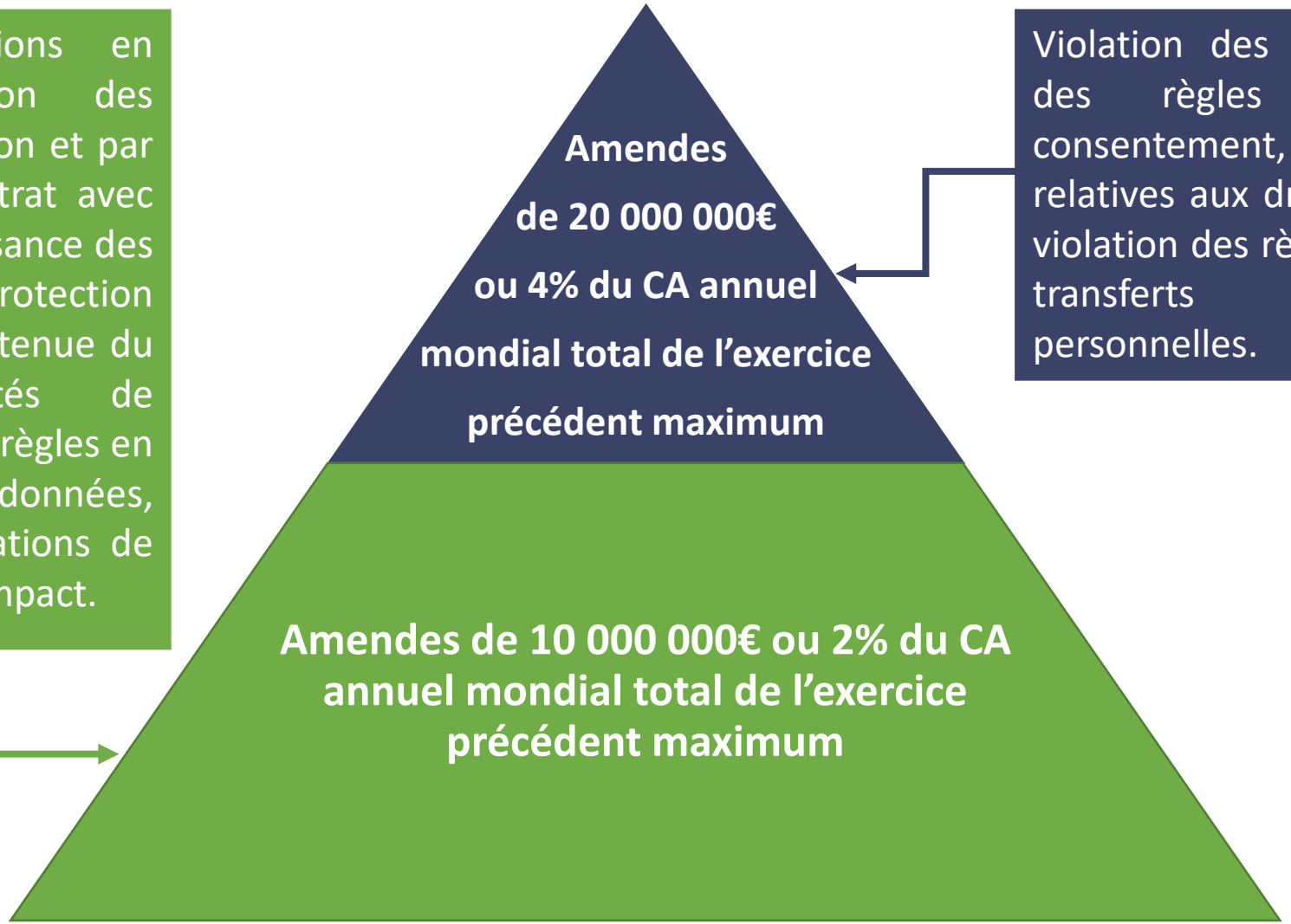
Depuis l'entrée en application de la loi pour une République Numérique**, la Cnil n'est pas contrainte de prononcer une mise en demeure préalablement à une sanction**.

La mise en demeure est désormais une **simple faculté** de la présidente de la Cnil, « ***si le manquement constaté est susceptible de faire l'objet d'une mise en conformité*** » (article 45 II de la loi 78-17).

Même dans le cadre d'une mise en demeure, **la présidente de la Cnil peut saisir la formation restreinte en vue du prononcé d'une amende administrative** (article 45 III, 7 de la loi 78-17).

Les sanctions pécuniaires

Violation des obligations en matière de protection des données dès la conception et par défaut, absence de contrat avec les sous-traitants, insuffisance des clauses relatives à la protection des données, défaut de tenue du registre des activités de traitement, violation des règles en matière de sécurité des données, de notification des violations de données et d'analyse d'impact.

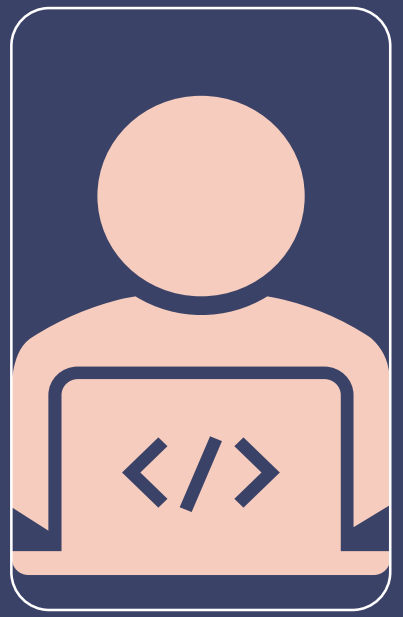


Violation des principes, violation des règles applicables au consentement, violation des règles relatives aux droits des personnes, violation des règles applicables aux transferts de données personnelles.

Quels critères ?

Les amendes doivent être « ***effectives, proportionnées et dissuasives*** ». Il doit être tenu compte des éléments suivants (article 83) :

- la **nature**, la **gravité** et la **durée de la violation**, compte tenu de la **nature**, de la **portée** ou de la **finalité du traitement** concerné, ainsi que du **nombre de personnes concernées affectées** et le **niveau de dommage** qu'elles ont subi
- le fait que la violation a été **commise délibérément** ou par **négligence**
- toute mesure prise par le responsable du traitement ou le sous-traitant pour **atténuer le dommage subi** par les personnes concernées ;
- le **degré de responsabilité du responsable du traitement ou du sous-traitant**, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre
- toute **violation pertinente commise précédemment** par le responsable du traitement ou le sous-traitant ;
- le **degré de coopération établi avec l'autorité de contrôle** en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs
- les **catégories de données** à caractère personnel concernées par la violation
- la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a **notifié la violation**
- Lorsque des mesures correctrices ont déjà été ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, **le respect de ces mesures**
- l'application de **codes de conduite** approuvés ou de **mécanismes de certification** approuvés
- toute autre **circonstance aggravante ou atténuante** applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation



La sécurité des données au cœur des sanctions

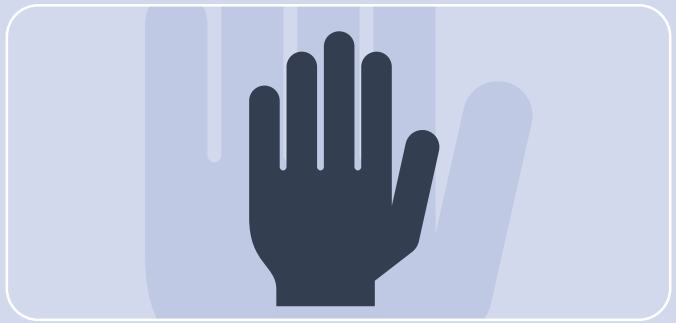
Un prérequis : la sécurité

L'article 32 du RGPD impose aux responsables de traitements et aux sous-traitants de « *mettre en œuvre les **mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque* ».

Cette obligation de sécurité, qui préexiste au RGPD, est d'autant plus **primordiale** aujourd'hui.

Attention notamment aux **violations de données** dues à une sécurisation insuffisante !

Des échelles de sanctions variables



L'article 83 du RGPD liste les **critères devant être pris en compte** par les autorités de contrôle dans la détermination du montant des amendes administratives prononcées afin qu'elles soient « ***effectives, proportionnées et dissuasives*** ».

Le considérant 11 du RGPD précise qu'un niveau équivalent de protection dans l'ensemble de l'UE exige que les autorités de contrôles prononcent des « ***sanctions équivalentes*** *pour les violations* ».

Le but est de permettre une **plus grande cohérence** que sous l'empire du droit antérieur.

Des échelles de sanctions variables

Le G29 avait publié le 3 octobre 2017 des lignes directrices sur l'application et la fixation des amendes administratives. Toutefois, celles-ci portent principalement sur l'interprétation des critères retenus et non sur les montants des sanctions.

Pour les traitements transfrontaliers, le mécanisme de coopération et d'autorité chef de file devrait permettre une harmonisation des sanctions. Mais **quid des sanctions prononcées par chaque autorité nationale** ?

Déclaration de Marie-Laure Denis, présidente de la Cnil, au Monde du 15 avril 2019 : « *il n'y a aucun tabou à utiliser avec discernement toute la palette de sanctions dont dispose la CNIL* ».

L'autorité de contrôle des Pays-Bas a publié le 14 mars 2019 une échelle des catégories de sanctions pécuniaires, qu'elle était susceptible de prononcer, en précisant qu'elle n'est pas liée par les montants indiqués. **Cette échelle va jusqu'à 1 million d'euros**.

L’échelle de sanction de l’autorité néerlandaise

Niveau	Echelle	Montant par défaut	Exemples
Catégorie I	0 € à 200.000 €	100.000€	Non publication des coordonnées du DPO, absence d’accord écrit entre les responsables conjoints, etc.
Catégorie II	120.000 € à 500.000 €	310.000€	Manquements au privacy by design ou by default, absence de contrat encadrant la sous-traitance, absence de registre des activités de traitement, etc.
Catégorie III	300.000 € à 750.000 €	525.000€	Absence de représentants dans l’UE, non notification de violation de données à l’autorité de contrôle, manquements aux principes de limitation des finalités, de minimisation des données, d’exactitude, de limitation de la conservation ou d’intégrité et de confidentialité des données, etc.
Catégorie IV	450.000 € à 1.000.000 €	725.000€	Manquements aux règles spécifiques aux prises de décisions entièrement automatisées, traitement illicite de données particulières, traitement illicite du NIR néerlandais, non-respect d’une injonction de l’autorité de contrôle, etc.

Panorama de sanctions (non exhaustif) : une aide à la conformité pour les acteurs de la sécurité (DPO, DSI ou RSSI).

Portugal

Sanction prononcée le 11 octobre 2018 par la CNDP à l'encontre d'un hôpital :

- Manquement à l'obligation d'assurer l'intégrité et la confidentialité des données : **des personnels non autorisés ont pu accéder à des données de patients, ce qui est constitutif d'une violation de données** ;
- Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles adéquates pour assurer la sécurité des données : le personnel disposant d'un accès à la base de données de l'hôpital avait accès aux données de tous les patients (**pas de niveaux d'habilitations distincts**) et pouvait accéder aux données de patients d'autres hôpitaux, sans justification. De plus, l'hôpital n'était pas en mesure d'assurer en continue la surveillance de son système d'information pour s'assurer de l'intégrité et de la confidentialité des données.
- Montant : **400.000 euros**

Allemagne

Sanction prononcée le 21 novembre 2018 par la LfDI à l'encontre d'un réseau social :

- Le site avait subi une cyberattaque en septembre 2018. Les mots de passe des utilisateurs étaient conservés **en clair** dans la base de données copiée par les attaquants
- Pour la LfDI, cela était constitutif **d'un manquement à l'obligation de définir des mesures de sécurité adéquates.**
- La LfDI a toutefois déclaré avoir pris en compte la « *coopération exemplaire* » dont a fait preuve la société lors de la procédure. Celle-ci a notifié sans délai l'autorité et les personnes concernées et a rapidement mis en œuvre d'importants moyens pour se mettre en conformité.
- Montant : **20.000 euros**

Italie

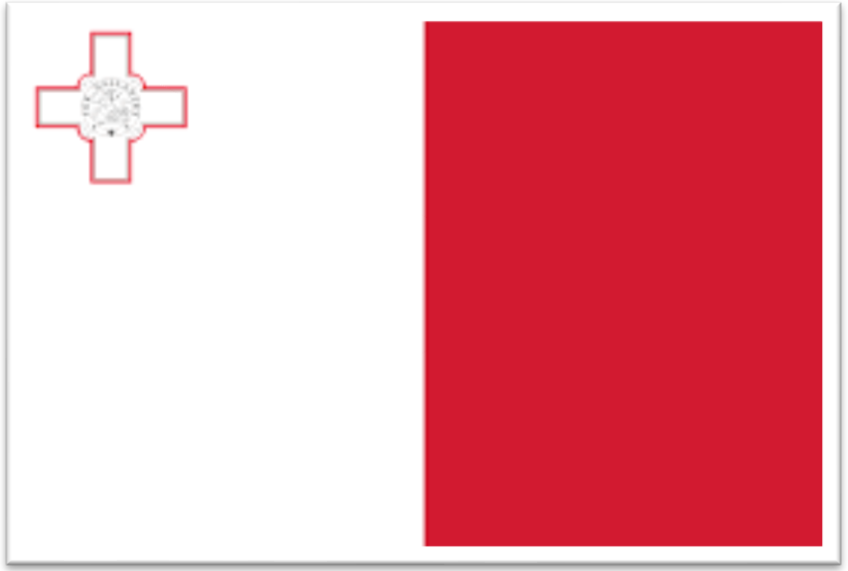
Sanction prononcée le 4 avril 2019 par l'autorité de contrôle italienne à l'encontre d'une association (mouvement politique) :

- Les sites de l'association avaiet fait l'objet d'un premier contrôle à l'été 2017, qui avait révélé de nombreux défauts de sécurité. Depuis ce contrôle, ils faisaient l'objet d'un suivi pour s'assurer de l'implémentation de mesures de sécurité adéquates. L'autorité de contrôle note que des progrès ont été fait et des mesures mises en places, mais qu'il subsiste des manquements à l'obligation de sécurité.
- Notamment, l'autorité souligne **l'absence de traçabilité complète des accès à la base de données, du partage d'identifiants entre plusieurs personnes en charge de l'une des plateformes contrôlées, de l'absence de définition de profils d'habilitation pour restreindre l'accès aux données.**
- Montant : **50.000 euros**

Malte

Sanction prononcée le 18 février 2019 par l'IDPC à l'encontre de l'Autorité foncière de Malte :

- Un article paru dans le journal Times of Malta, le 23 novembre 2018 révélait que près de 10 Go de données à caractère personnel collectées par l'Autorité étant librement accessibles sur Internet.
- **Cette fuite de données était due à un défaut de sécurisation du formulaire de collecte présent sur le site internet, par lequel des administrés pouvaient effectuer des demandes diverses.**
- L'Autorité foncière a suspendu rapidement l'accès à son site jusqu'à la résolution du défaut de sécurité.
- Montant : **5000 euros**



Chypre

Sanction prononcée le 7 novembre 2018 à l'encontre d'un hôpital :

- Manquement à l'obligation de mettre en œuvre des mesures propres à assurer, notamment, l'intégrité des données à caractère personnel.
- En effet, un patient avait demandé à l'hôpital d'accéder à son dossier, **au format papier.** Toutefois, celui-ci n'a pas pu le retrouver. Le dossier aurait été perdu à la suite du départ d'un médecin.
- Pour l'autorité, **l'hôpital n'a pas mis en place de mesures suffisantes visant à prévenir la perte accidentelle de données.**
- Montant : **5000 euros**

Danemark

Sanction recommandée par l'autorité danoise en mars 2019 à l'encontre d'une société de taxis :

- L'autorité danoise ne peut pas directement prononcer d'amende administrative. Le prononcé revient aux tribunaux.
- **Manquement au principe de minimisation des données et de limitation de leur conservation**. En effet, la société déclarait « anonymiser » les données qu'elle collectait sur ses clients au bout de deux ans, mais se contentait de supprimer leurs noms et prénoms. Elle conservait de nombreuses données telles que leurs données de géolocalisation, ou leur numéro de téléphone. Ces derniers étaient conservés pendant trois ans à compter de « l'anonymisation ».
- De plus, **la société n'était pas en mesure de démonter adéquatement qu'elle supprimait les données dans les intervalles convenus, faute notamment d'une traçabilité complète et de mécanismes de purge automatique**.
- Montant : **environ 161.000 euros**

Pologne

Sanction prononcée en mars 2019 par l'UODO à l'encontre d'une société :

- La société traitait des données tirées de l'équivalent polonais du RCS (le CEiDG). Toutefois, elle n'informait du traitement que les personnes concernées pour lesquelles elle disposait d'une adresse de courrier électronique. Elle justifiait cette absence d'information par un coût important généré par le fait d'informer les autres personnes concernées.
- Manquement à l'obligation d'information : l'autorité polonaise estime que **les coûts n'étaient pas suffisamment élevés pour justifier de ne pas informer les personnes pour lesquelles la société disposait d'une adresse postale et/ou du numéro de téléphone**.
- Pour fixer le montant de l'amende, l'autorité souligne que **la société avait conscience de ses obligations et que son manquement était intentionnel**. De plus, elle n'a pris aucune mesure pour mettre fin à la violation avant la sanction et n'a pas indiqué vouloir le faire.
- Montant : **environ 220 000 euros**

Pologne

Sanction prononcée en septembre 2019 par l'UODO à l'encontre d'une société :

- Un site Internet de commerce électronique a fait l'objet d'une violation de données entrainant **la divulgation non autorisée de données de 2.2 millions de personnes concernées.**
- L'autorité a considéré que le site Internet n'avait pas pris de mesures techniques et organisationnelles suffisantes, qui auraient permis de détecter et faire cesser le trafic réseau inhabituel.
- Pour fixer le montant de l'amende, l'autorité souligne que a déclaré avoir pris en compte « *l'importance considérable* » et « *le caractère sérieux* » de la violation, « *le nombre élevé des personnes concernées* » ainsi que les risques éventuels liés à une telle violation comme **l'usurpation d'identité**
- Montant : **645 000 euros**

Lituanie

Sanction prononcée en mai 2019 par the state data protection inspectorate à l'encontre d'une société :

- Les données à caractère personnel des clients d'une société **de paiement électronique** ont été rendues publiques sur un site internet pendant au moins deux jours en juillet 2018. Le site contenait également plus de 9 000 captures d'écran présentant des informations sur les opérations de paiement des clients. L'origine de cette violation de données n'est pas connue de manière certaine.

- L'autorité de contrôle constate que la société **n'a pas notifié la violation** de données, ni à l'autorité de contrôle, ni aux personnes concernée. Par ailleurs, elle précise que la société ne disposait pas des mesures techniques et organisationnelles suffisantes pour garantir la sécurité des données (un seul salarié affecté à la sécurité du SI, des données non chiffrées, absence de mesures de contrôle d'accès).

- Montant : **61 500 euros**

Royaume-Uni

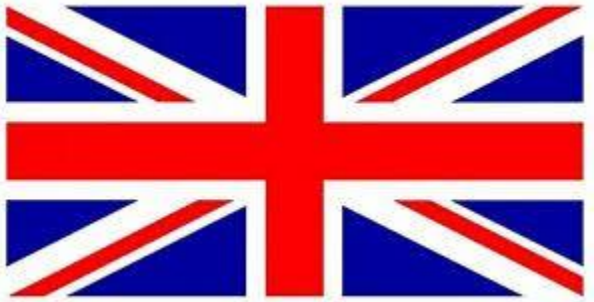
Sanction prononcée en juillet 2019 par l'ICO à l'encontre d'une société :

- Une compagnie aérienne a été victime en septembre 2018 d'un incident de sécurité ayant entrainé le détournement d'une partie du trafic destiné au site internet institutionnel de la société vers un site frauduleux. **Grâce à ce site frauduleux, les attaquants ont pu avoir accès aux données à caractère personnel d'environ 500 000 utilisateurs**.

-En tant qu'autorité chef de file, l'autorité a effectué un contrôle au cours duquel elle a relevé qu'ont été notamment compromises les données relatives à la connexion, aux cartes de paiement, aux réservations de voyage, ainsi que les noms et les adresses des utilisateurs.

-L'autorité de contrôle a précisé que la compagnie a coopéré au cours du contrôle et a amélioré ses outils de sécurité

-Montant : **environ 204 millions d'euros**



Royaume-Uni

Sanction prononcée en juillet 2019 par l'ICO à l'encontre d'une société :

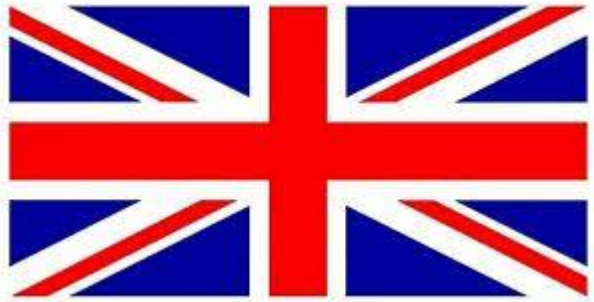
-Un groupe hôtelier a été victime d'un incident de sécurité entrainant la divulgation des données de 339 millions de clients dans le monde, dont 30 millions de résidents de l'Union européenne.

-L'autorité a annoncé que l'incident avait affecté la base de données d'une chaîne hôtelière, qui avait été acquise en 2016 par le groupe hôtelier. Toutefois, ce n'est qu'en 2018 que l'incident a été découvert par le groupe.

Lors d'un contrôle effectué en tant qu'autorité chef de file, l'ICO a constaté que le groupe **hôtelier n'avait pas effectué des vérifications lors de l'acquisition de la chaîne hôtelière et n'avait pas pris des mesures nécessaires pour sécuriser ses systèmes d'information**.

-L'autorité a souligné la coopération dont le groupe a fait preuve au cours du contrôle et l'amélioration de ses mesures de sécurité.

Montant : **environ 110 millions d'euros**



France

Sanction prononcée en mai 2019 par la Cnil, à l'encontre d'une société :

- L'autorité de contrôle a constaté que l'on pouvait accéder aux documents (comme les copies de cartes d'identité, d'avis d'imposition ou encore de relevés de compte bancaire, etc.) mis en ligne par les candidats à la location en modifiant l'URL affichée dans le navigateur. Il est reproché à la société de ne pas avoir mis en place les mesures techniques et organisationnelles nécessaires pour garantir la sécurité de données.

- L'autorité a notamment souligné **l'absence d'une procédure d'authentification des utilisateurs du site lors de l'accès aux URL litigeuses**. L'autorité a estimé que la société conservait **en base active** les documents des candidats n'ayant pas accédé à la location pour une durée non-proportionnée aux finalités du traitement.

- Montant : **400 000 euros**

France

Sanction prononcée en juin 2019 par la Cnil, à l'encontre d'une société :

- L'autorité a relevé une série de manquements. L'une des caméras filmait en continu les postes de travail de 6 salariés et les images étaient conservées pour une durée excessive. Les salariés n'étaient pas informés formellement de l'existence du dispositif. Par ailleurs, les postes de travail des collaborateurs **n'étaient pas verrouillés par mot de passe,** de même que celui du dirigeant, sur lequel un logiciel permettait de consulter les images captées. Enfin, tous avaient accès, via un mot de passe commun, à une boite de messagerie électronique pour la société. Celle-ci ne disposait **pas de mesures de traçabilité** permettant de retracer les actions effectuées par chacun.

- Le montant et la publicité sont justifiés par la Cnil par l'absence de collaboration de la société, la « particulière sensibilité » du dispositif de vidéosurveillance, la pluralité des manquements en cause ainsi que leur persistance et leur gravité. Toutefois, l'autorité indique également avoir tenu compte des mesures prises par la société au cours de l'instruction, du fait qu'il s'agisse d'une microentreprise et de sa situation financière difficile.

- Montant : **20 000 euros et astreinte de 200 euros par jour de retard**

France

Sanction prononcée en juillet 2019 par la Cnil, à l'encontre d'une société :

- Suite au signalement par un utilisateur du site web édité par une société du secteur de l'assurance permettant à ses clients de demander des devis, de souscrire des contrats et d'accéder à leur espace personnel. Le client de la société a indiqué à l'autorité qu'il pouvait accéder aux données d'autres clients à partir de son compte. La Cnil a également été avisée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) que l'accès aux données des internautes dudit site web était possible **sans procédure authentification préalable depuis un moteur de recherche**.

-L'autorité a notamment relevé que les mesures élémentaires de sécurité n'avaient pas été prises dès la conception du site web, comme la mise en place d'une procédure d'authentification et d'une gestion des droits d'accès ainsi que l'utilisation d'un fichier tel que « robots.txt » pour éviter le référencement.

- Montant : **180 000 euros**

Que retenir ?

Les sanctions et les pratiques des autorités de contrôle sont encore très variées, et il est trop tôt pour voir se dessiner des tendances.

Plus que jamais, la sécurité et en particulier la cybersécurité constitue un enjeu majeur pour les responsables de traitements de données à caractère personnel.

Quelles voies de recours en France ?

Les décisions et délibérations des autorités de contrôle sont **susceptibles de recours**.

En France, il est possible de faire appel des décisions de la Cnil devant le Conseil d'Etat, dans un **délai de deux mois à compter de la notification de la délibération** de la formation restreinte.

Il s'agit d'un recours dit de pleine juridiction.

Quelles voies de recours en France ?

Le 7 mai 2018, la formation restreinte de la Cnil a prononcé une **sanction pécuniaire de 250 000 euros** à l'encontre d'une société, pour manquement à son obligation d'assurer la sécurité des données.

En effet, à la suite d'un défaut de sécurité, des factures de clients de la société étaient librement accessibles sur Internet.

La société a fait appel de la sanction auprès du Conseil d'Etat.

Par une décision du 17 avril 2019, celui-ci a **réduit le montant de l'amende administrative à 200 000 euros**, au regard de la réactivité de la société dans la résolution du défaut de sécurité une fois que celui-ci lui avait été signalé.