LAZARÈGUE AVOCATS

rapport · novembre 2026

cybersécurité · données personnelles

APRÈS LA CYBERATTAQUE, LA SANCTION

> Étude comparée de 139 décisions rendues dans 20 pays européens contre des organismes dont les données ont fui

étude de jurisprudence administrative · 20 pays · 2018-2026

18 rue de tilsitt, 75017 paris · lazaregue-avocats.fr

sommaire

Ce rapport en une page
La démarche
Repères : pourquoi une victime peut être sanctionnée
1. Le cadre juridique
2. Les décisions étudiées
3. Comment les attaques se déroulent
4. Ce que les autorités reprochent, et pourquoi cela manquait
5. Des mesures connues : confrontation aux référentiels
6. Les sanctions, d'un pays à l'autre
7. Enseignements pour les organismes
8. Auditer autrement : la preuve plutôt que la déclaration
9. Ce que le droit actuel laisse sans réponse
Lexique
Méthode, limites et sources
Annexe : liste des décisions

139

décisions de sanction rendues après une cyberattaque, dans 20 pays européens

116 MILLIONS

de personnes au moins dont les données ont été atteintes, d'après les seules 59 décisions qui donnent un chiffre

635 M€

d'amendes cumulées, dont 516 M€ pour trois décisions visant Meta

105 500 €

amende médiane sur les 134 décisions dont le montant est connu

14 CENTIMES

amende rapportée à chaque personne touchée dans l'affaire France Travail : 5 M€ pour 36,8 millions de personnes

1 À 7 ANS

entre l'attaque et la sanction selon l'autorité : douze mois en Norvège, sept ans et demi en Irlande

l'essentiel

Ce rapport en une page

Quand une entreprise se fait voler les données de ses clients, est-elle seulement victime ? Les autorités européennes répondent que non, et elles disent pourquoi.

Dans chaque pays d'Europe, une autorité publique veille à la protection des données personnelles. En France, c'est la CNIL. Après un piratage, cette autorité enquête sur l'organisme piraté et peut lui infliger une amende. Ce rapport a rassemblé 139 de ces décisions, rendues dans 20 pays entre 2018 et novembre 2026, et les a comparées : que reprochent les autorités, et sanctionnent-elles de la même façon ?

On n'est pas puni pour avoir été piraté. On l'est pour avoir laissé une porte ouverte : une précaution élémentaire manquait, qui aurait empêché l'intrusion ou limité les dégâts.

Ce sont toujours les mêmes portes. Un accès à distance protégé par un simple mot de passe. Une mise à jour jamais installée. Personne pour remarquer qu'un compte copie des millions de fiches. Un prestataire que nul ne contrôle. Une dizaine de défauts suffit à décrire presque toutes les affaires.

Ces précautions étaient connues. Elles figurent dans des guides publics et gratuits. Souvent, l'organisme avait lui-même écrit qu'il fallait agir, et ne l'avait pas fait.

D'un pays à l'autre, la sanction n'a rien de comparable. Le même règlement européen s'applique partout. Pourtant l'amende médiane va de 5 000 € en Roumanie à 1,5 M€ en France, et la sanction tombe un an après l'attaque en Norvège, plus de sept ans après en Irlande.

Les personnes dont les données ont fui ne reçoivent rien. L'amende va à l'État. Rapportée au nombre de personnes touchées, elle se compte en centimes.

Une conclusion se dégage de ces constats. Dans les affaires étudiées, l'attaque n'a pas réussi parce que les pirates étaient d'une habileté hors du commun. Elle a réussi parce qu'une précaution connue n'avait pas été prise. Respecter réellement les règles de protection des données apparaît ainsi comme la première défense contre le piratage, et non comme une formalité.

Les décisions ont été lues sur leur texte, et les chiffres sont ceux qu'elles donnent. Lues une à une, ces décisions sont des cas d'espèce. Comparées, elles font apparaître ce qu'aucune ne montre seule : les mêmes défauts sanctionnés partout, et des sanctions très inégales d'une autorité à l'autre.

la démarche

Pourquoi ce rapport, et comment il a été fait

Chaque annonce de fuite repose la même question. Ce rapport y répond par les décisions que les autorités ont déjà rendues.

La question

En novembre 2026, trois organismes français ont annoncé en dix jours qu'un tiers avait accédé aux données qu'ils détenaient.

annonce	organisme	ce qui est public
14 novembre	Maileva, filiale du groupe La Poste	Attaque à la mi-septembre. Nom, prénom et adresse postale de 22 millions de destinataires de courriers.
23 novembre	Institut national du cancer	Incident détecté le 18 novembre. Deux sites d'information indisponibles, violation de données confirmée, nature et nombre non précisés.
24 novembre	Direction générale de l'aviation civile	Accès non autorisé au site de paiement des redevances du 5 au 9 novembre. Identités, coordonnées, commandes et informations partielles de cartes bancaires.

Aucune de ces affaires n'a été examinée par une autorité, et ce rapport ne dit rien de ce qui s'y est passé. Elles posent toutes la même question : l'organisme attaqué peut-il être sanctionné, et pour quelle raison ? La réponse ne se trouve pas dans les communiqués. Elle se trouve dans les décisions rendues depuis 2018 dans des affaires comparables.

Ce qui a été fait

Rechercher. Les décisions ont été recherchées sur les sites des autorités nationales de protection des données et dans la base publique GDPR Enforcement Tracker, depuis l'entrée en application du règlement européen, en mai 2018.

Trier. Une décision n'a été retenue que si trois éléments étaient réunis : un attaquant extérieur, une enquête ouverte à la suite de cette attaque, une sanction. 139 décisions rendues dans 20 pays remplissent ces conditions.

Lire. 132 décisions ont été vérifiées sur le texte officiel, le communiqué de l'autorité ou son rapport d'activité, dans leur langue d'origine. Sept ne sont connues que par des sources secondaires. Elles sont signalées comme telles.

Relever. Les mêmes éléments ont été notés pour chaque affaire : la façon dont l'attaquant est entré, les données atteintes, le nombre de personnes, ce que l'autorité reproche, le texte qu'elle applique, le montant, le temps écoulé entre l'attaque et la sanction.

Comparer. Les décisions ont été comparées entre elles, puis aux guides publics de la CNIL et de l'ANSSI, puis d'un pays à l'autre.

Ce que le rapport ne fait pas

Il ne recense pas toutes les sanctions : plusieurs autorités ne publient pas leurs décisions, ou les anonymisent. Il ne classe pas les autorités de la plus sévère à la plus clémente, parce qu'elles ne jugent pas les mêmes organismes. Il ne se prononce sur aucune affaire en cours.

Le relevé est arrêté au 25 novembre 2026. Trois séries de décisions publiées en novembre ont été examinées et laissées de côté, faute d'attaque établie ou d'éléments suffisants : la sanction de 5 M€ prononcée par la CNIL le 12 novembre pour des mots de passe conservés en clair, les dix sanctions simplifiées annoncées par la CNIL le 9 novembre contre des collectivités, qui ne sont pas nominatives, et deux décisions italiennes du 7 octobre visant un centre de radiologie et son prestataire. Le détail figure dans la partie consacrée à la méthode.

repères

Pourquoi une victime peut être sanctionnée

Une entreprise piratée est victime d'un délit. Elle n'en reste pas moins responsable de ce qu'on lui avait confié.

La situation ressemble à celle d'un garde-meuble cambriolé. Le cambrioleur est le coupable, et la police le recherche. Mais les clients demanderont au garde-meuble si la porte était fermée, si l'alarme fonctionnait, et depuis quand la serrure était cassée. Pour les données personnelles, ces questions sont posées par une autorité publique, et de mauvaises réponses coûtent une amende.

Les deux procédures avancent côte à côte. La justice pénale recherche l'auteur de l'attaque. L'autorité de protection des données examine, elle, la façon dont l'organisme protégeait les données de ses clients, de ses salariés ou de ses usagers.

Ce qui se passe après une attaque

1. **L'attaque.** Un tiers accède aux données, les copie, parfois les bloque pour exiger une rançon.
2. **La notification.** L'organisme doit prévenir l'autorité de protection des données au plus vite, en principe dans les 72 heures, et les personnes concernées si le risque est élevé pour elles.
3. **Le contrôle.** L'autorité enquête : elle demande des documents, interroge les équipes, examine le système tel qu'il était le jour de l'attaque.
4. **La décision.** Si une mesure de protection attendue faisait défaut, l'autorité prononce une amende, souvent rendue publique, et peut ordonner des corrections.
5. **Les suites.** Les personnes dont les données ont fui peuvent demander réparation devant un tribunal.

Deux rôles à distinguer

Le RGPD distingue deux rôles, que l'on retrouvera tout au long du rapport. Le **responsable de traitement** est l'organisme qui décide d'utiliser des données pour son activité : la banque qui écrit à ses clients. Le **sous-traitant** est le prestataire qui manipule ces données pour son compte : la société qui imprime et envoie le courrier. Les deux ont des obligations de sécurité, et les deux peuvent être sanctionnés.

Qui sanctionne

Chaque pays européen dispose d'une autorité indépendante chargée de faire respecter le règlement général sur la protection des données (RGPD), texte européen applicable depuis le 25 mai 2018. En France, il s'agit de la Commission nationale de l'informatique et des libertés (CNIL). Les sigles des principales autorités citées dans ce rapport sont les suivants.

sigle	autorité	pays
CNIL	Commission nationale de l'informatique et des libertés	France
AEPD	Autorité de protection des données	Espagne
Garante	Garante per la protezione dei dati personali	Italie
DPC	Autorité de protection des données	Irlande
UODO	Autorité de protection des données	Pologne
ANSPDCP	Autorité de protection des données	Roumanie
HDPA	Autorité de protection des données	Grèce

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), également citée, n'est pas une autorité de sanction. C'est l'agence française chargée de la cybersécurité, dont les guides font référence.

Ce que la loi exige

La loi n'exige pas d'être invulnérable. Elle exige d'avoir pris les précautions raisonnables au regard de ce que l'on protège, comme on attend d'un commerçant qu'il ferme sa porte à clé et non qu'il rende tout cambriolage impossible. Après une attaque, c'est à l'organisme de montrer qu'il avait pris ces précautions.

partie 1

Le cadre juridique

1.1 Les obligations

texte	ce que dit le texte	portée pratique
RGPD, art. 5-1-f	Principe d'intégrité et de confidentialité : garantir une sécurité appropriée des données	Celui qui détient des données doit empêcher qu'elles soient vues, modifiées ou perdues par quelqu'un qui n'y a pas droit.
RGPD, art. 5-2 et 24	Responsabilité : être en mesure de démontrer la conformité	Il ne suffit pas de respecter la règle, il faut pouvoir le prouver, documents à l'appui.
RGPD, art. 25	Protection des données dès la conception et par défaut	La sécurité se prévoit au moment où l'on conçoit un service, et non après coup.
RGPD, art. 28	Recours uniquement à des sous-traitants présentant des garanties suffisantes ; traitement régi par un contrat ou un autre acte juridique	On ne confie des données qu'à un prestataire qui offre des garanties, et la relation est encadrée par contrat.
RGPD, art. 32	Mesures techniques et organisationnelles appropriées au risque, compte tenu de l'état des connaissances et des coûts	Plus les données sont nombreuses ou sensibles, plus les protections doivent être fortes. Le niveau attendu est celui que les professionnels connaissent à la date des faits.
RGPD, art. 33	Notification de la violation à l'autorité « dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance » ; le sous-traitant notifie au responsable « dans les meilleurs délais »	En cas de fuite, l'organisme prévient l'autorité au plus vite, en principe dans les trois jours. Le prestataire prévient son client sans attendre.
RGPD, art. 34	Communication aux personnes concernées en cas de risque élevé	Lorsque la fuite expose les personnes à un danger sérieux, elles doivent être prévenues et informées des précautions à prendre.
RGPD, art. 82	Droit à réparation du dommage matériel ou moral ; exonération si l'organisme prouve que le fait qui a provoqué le dommage ne lui est nullement imputable	Toute personne lésée peut demander une indemnisation devant un tribunal. L'organisme n'y échappe qu'en prouvant qu'il n'y est pour rien.
RGPD, art. 83	Amendes : jusqu'à 10 M€ ou 2 % du chiffre d'affaires mondial pour les articles 25 à 39 ; jusqu'à 20 M€ ou 4 % pour les principes de l'article 5	Deux niveaux d'amende maximale. Le plafond retenu est le plus élevé des deux montants, ce qui pèse surtout sur les grands groupes.
Directive NIS 2 (UE) 2022/2555, art. 21	Mesures de gestion des risques, dont la sécurité de la chaîne d'approvisionnement et l'authentification à plusieurs facteurs	Texte distinct du RGPD, qui impose une liste de précautions de cybersécurité aux organismes de secteurs jugés essentiels.

1.2 La règle du jeu : être piraté n'est pas une faute, mais il faut prouver qu'on s'était protégé

Deux règles commandent tout ce qui suit. Elles ne sont pas écrites telles quelles dans le RGPD : c'est la Cour de justice de l'Union européenne qui les a dégagées. Cette Cour, qui siège à Luxembourg, fixe le sens des textes européens, et ses arrêts s'imposent aux autorités et aux juges de tous les États membres.

La loi ne demande pas l'impossible. Aucune protection n'est infaillible, et la loi le sait. Elle n'exige pas qu'aucune fuite ne se produise. Elle exige que l'organisme ait pris les précautions raisonnables, compte tenu de ce qu'il avait à protéger. Les juristes parlent d'une obligation de moyens : le médecin doit soigner correctement, il ne promet pas la guérison.

Mais c'est à l'organisme de prouver qu'il s'était protégé. D'ordinaire, celui qui reproche une faute doit la prouver. Ici, la règle est inversée. Après une fuite, ce n'est ni à l'autorité ni à la victime de démontrer la négligence. C'est à l'organisme de montrer, documents à l'appui, ce qu'il avait mis en place. Celui qui ne peut rien montrer perd.

La Cour a posé ces règles le 14 décembre 2023, dans une affaire venue de Bulgarie. En 2019, l'administration fiscale bulgare avait été piratée et les données de millions de personnes publiées. L'une d'elles a demandé réparation, et le juge bulgare a interrogé la Cour (CJUE, 14 décembre 2023, C-340/21, **Natsionalna agentsia za prihodite**). Le tableau qui suit reprend ses réponses.

ce que la cour a jugé	ce que cela signifie concrètement
La divulgation ou l'accès non autorisé ne suffit pas à établir que les mesures étaient inappropriées.	Avoir été piraté ne prouve pas, à soi seul, que l'on était mal protégé.
Le juge apprécie concrètement le caractère approprié des mesures.	On examine ce qui était réellement en place, au regard de ce qu'il y avait à protéger.
La charge de prouver que les mesures étaient appropriées pèse sur le responsable du traitement.	C'est à l'organisme de démontrer qu'il avait fait le nécessaire, et non à la victime de démontrer le contraire.
L'attaque d'un tiers n'exonère le responsable que s'il prouve que le dommage ne lui est nullement imputable.	Dire « ce sont des pirates » ne suffit pas à échapper à sa responsabilité.
La crainte d'un usage abusif des données peut constituer, à elle seule, un dommage moral.	La personne dont les données ont fui peut être indemnisée pour l'inquiétude subie, même sans fraude avérée.

La Cour a précisé depuis que le responsable est tenu d'atténuer les risques de violation et non d'empêcher toute violation (CJUE, 25 janvier 2024, C-687/21). Les autorités nationales reprennent ces formules. La CNIL énonce ainsi qu'elle ne sanctionne pas la violation elle-même, mais le fait qu'elle ait été rendue possible ou facilitée par l'absence ou l'insuffisance des mesures, compte tenu de l'état de l'art (délib. SAN-2026-009, 21 juillet 2026).

Une commentatrice en résume la conséquence pratique : dès qu'une fuite survient, un soupçon pèse sur les protections qui existaient auparavant, et c'est à l'organisme de le dissiper, pièce par pièce (L. Maisnier-Boché, Comm. com. électr. 2026, comm. 101).

Les arrêts de la Cour cités dans ce rapport

Le tableau dit, pour chaque arrêt cité dans les pages qui suivent, d'où venait l'affaire et ce qu'il faut en retenir.

arrêt	ce qui s'était passé	ce qu'il faut en retenir
14 décembre 2023, C-340/21	En 2019, l'administration fiscale bulgare est piratée et les données de millions de contribuables sont publiées. Une personne concernée demande réparation.	La fuite ne prouve pas la faute, mais l'organisme doit prouver qu'il était correctement protégé. La crainte d'un mauvais usage des données est indemnisable.
25 janvier 2024, C-687/21	Affaire citée par la CNIL dans sa décision du 21 juillet 2026.	L'organisme doit réduire le risque de fuite ; il n'est pas tenu de rendre toute fuite impossible.
5 décembre 2023, C-807/21	Une société immobilière allemande conteste une amende de plus de 14 millions d'euros, infligée pour avoir conservé trop longtemps les données de locataires.	Une amende suppose une faute, commise délibérément ou par négligence. Lorsque la société appartient à un groupe, le plafond se calcule sur le chiffre d'affaires de l'ensemble.
13 février 2025, C-383/23	Une chaîne danoise de magasins de meubles est poursuivie pour avoir conservé les données d'au moins 350 000 anciens clients. Le juge danois demande s'il faut retenir son chiffre d'affaires ou celui de son groupe.	Le plafond de l'amende se calcule sur le chiffre d'affaires de l'entreprise au sens économique, donc du groupe, qui sert aussi à apprécier sa capacité à payer.

1.3 Comment sait-on quelles précautions sont exigées ? Les guides publics

Le RGPD ne donne aucune liste de précautions. Son article 32 demande des mesures « appropriées », compte tenu de « l'état des connaissances ». Autrement dit : ce qu'un professionnel sérieux sait devoir faire à la date des faits. Reste à savoir où cela est écrit.

La réponse se trouve dans des guides que des organismes publics rédigent et tiennent à jour. On les appelle des **référentiels**, parce qu'ils servent de référence commune. Les principaux sont les suivants.

guide	qui le publie	ce qu'on y trouve
Guide de la sécurité des données personnelles (version 2024)	La CNIL	Des fiches pratiques : mots de passe, accès, mises à jour, sauvegardes, prestataires
Guide d'hygiène informatique	L'ANSSI, agence française chargée de la cybersécurité	42 mesures de base pour protéger un système informatique
Recommandations sur les mots de passe (2022), sur l'enregistrement des accès (2021) et sur la seconde preuve d'identité (2025)	La CNIL	Des seuils précis, par exemple le nombre d'essais de mot de passe à tolérer
Lignes directrices	Le Comité européen de la protection des données, qui réunit les autorités des États membres	La façon de réagir à une fuite et de calculer une amende

Ces guides ne sont pas des lois. Nul n'est sanctionné pour ne pas les avoir suivis à la lettre. Mais lorsqu'une précaution y est recommandée depuis des années et qu'elle manquait le jour de l'attaque, l'autorité en déduit que l'organisme ne pouvait pas l'ignorer. La CNIL le dit de sa recommandation sur les mots de passe : elle « n'a certes pas de caractère impératif », mais elle fournit « un éclairage pertinent » sur les mesures attendues (délib. SAN-2026-003, France Travail). Un commentateur relève que ces recommandations occupent une place centrale dans les décisions Free (A. Latil, Comm. com. électr. 2026, comm. 38).

La partie 5 rapproche, ligne par ligne, chaque défaut sanctionné de la page du guide qui recommandait la précaution.

1.4 Ce qui avait déjà été étudié

Une étude voisine existe, mais elle ne répond pas à la même question. En novembre 2023, le Comité européen de la protection des données a publié un recueil de 90 décisions relatives à la sécurité des données, adoptées entre janvier 2019 et juin 2023 (E. Kosta). Ce recueil ne porte que sur les affaires que plusieurs autorités ont traitées ensemble, parce qu'elles concernaient plusieurs pays. Il laisse de côté les décisions purement nationales, ne s'intéresse pas au montant des amendes, et s'arrête avant l'arrêt de la Cour de justice.

Le présent rapport complète ce travail sur trois points. Il ne retient que les affaires nées d'une attaque. Il inclut les décisions nationales. Il va jusqu'en novembre 2026.

partie 2

Les décisions étudiées

Ce rapport repose sur 139 décisions. Toutes racontent la même histoire en trois temps : un tiers attaque, l'autorité enquête, l'organisme attaqué est sanctionné.

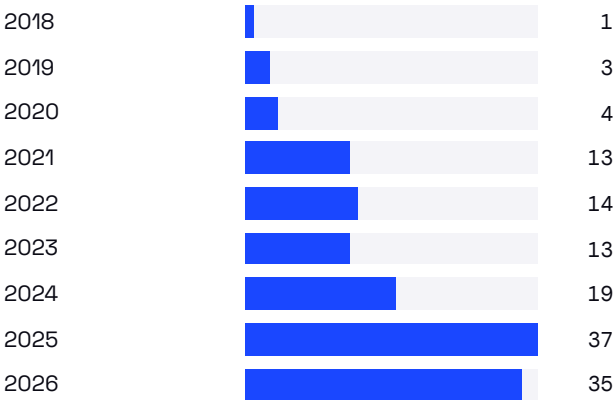
Une décision n'a été retenue que si ces trois éléments étaient réunis. Il fallait un attaquant extérieur : les fuites dues à une simple erreur interne, comme un courrier envoyé au mauvais destinataire, ont été écartées. Il fallait une enquête ouverte à la suite de cette attaque. Il fallait enfin une sanction, fondée soit sur un défaut de protection, soit sur la façon dont l'organisme a réagi à la fuite.

L'ensemble de ces décisions est appelé « le corpus » dans la suite du rapport. La liste complète figure en annexe.

2.1 Répartition par pays

pays	décisions
Espagne	41
Roumanie	24
Italie	14
Irlande	13
Pologne	10
France	7
Croatie	5
Bulgarie	3
Danemark	3
Grèce	3
Allemagne	2
Chypre	2
Finlande	2
Lituanie	2
Norvège	2
Suède	2
Belgique	1
Estonie	1
Hongrie	1
Pays-Bas	1

2.2 Répartition par année



2026 : décisions recensées jusqu'au 25 novembre.

La progression du nombre de décisions est nette depuis 2024. Elle doit être lue avec prudence : elle reflète aussi la politique de publication des autorités, très inégale. L'autorité espagnole publie l'intégralité de ses décisions et l'autorité roumaine communique sur chacune de ses amendes, quand

d'autres ne publient presque rien. Ces chiffres mesurent donc les décisions que l'on peut lire, et non l'activité réelle de chaque autorité. Un pays peu représenté n'est pas forcément un pays où l'on sanctionne peu.

partie 3

Comment les attaques se déroulent

Avant de regarder ce que les autorités reprochent, il faut voir ce qui s'est passé. Les décisions le racontent, et le récit est presque toujours le même.

Le pirate entre, le plus souvent avec un mot de passe valable. Il reste dans le système sans que personne s'en aperçoive, parfois des semaines. Il emporte beaucoup plus que ce qu'un seul accès aurait dû permettre. Rien de cela ne suppose une prouesse technique : dans la plupart des affaires, une porte était restée ouverte. Cette partie suit ces trois temps, puis mesure l'ampleur des fuites et dit ce que les fraudeurs font des données.

> repère
>
> Un **rançongiciel** est un programme qui bloque les fichiers de la victime et dont l'auteur exige une rançon, après avoir souvent copié les données. L'**hameçonnage** consiste à tromper une personne, par un faux courriel ou un faux appel, pour obtenir son mot de passe. Le **bourrage d'identifiants** consiste à essayer en masse des couples identifiant et mot de passe volés ailleurs, en comptant sur le fait que beaucoup de personnes réutilisent le même mot de passe. Une **vulnérabilité** est un défaut d'un logiciel qui permet d'y entrer sans autorisation.

voie d'attaque	de quoi s'agit-il	décisions (au moins)	exemples
Passage par un prestataire	Le pirate n'attaque pas l'organisme lui-même mais une société qui travaille pour lui et détient ses données ou un accès à son réseau.	36	Vodafone España, Iberia, Regione Lazio, caisses rurales espagnoles
Défaut d'un logiciel	Un programme utilisé par l'organisme comporte une erreur qui permet d'y entrer sans autorisation, souvent faute de mise à jour.	30	Postel, Iberia, Bayard Revistas, UniCredit
Rançongiciel	Un programme malveillant bloque les fichiers ; les pirates réclament une rançon et menacent de publier les données qu'ils ont copiées.	31	The Phone House, ELTA, LAZIOcrea, Sprinter, Østre Toten
Tromperie d'un salarié	Un faux courriel ou un faux appel conduit une personne à livrer son mot de passe ou à ouvrir un fichier piégé.	10	France Travail, University of Limerick, Kræftens Bekæmpelse
Mots de passe volés ou devinés	Le pirate utilise des mots de passe issus d'autres fuites, ou en essaie un très grand nombre de façon automatique.	6	Carrefour, 23andMe, Generali, Cosmote, Transavia

Comptage par recherche de termes dans les faits et manquements relevés ; une décision peut relever de plusieurs lignes ; les nombres sont des minimums.

3.1 L'attaquant entre avec des identifiants valides

Dans les dossiers les plus lourds, aucune barrière technique n'a été forcée. Chez Cosmote, le pirate a utilisé le mot de passe d'un salarié issu d'une ancienne fuite de LinkedIn. Chez France Travail, des comptes de conseillers ont été usurpés par ingénierie sociale. À l'Hôpital privé de la Loire, l'attaquant

disposait des identifiants d'un médecin libéral rattaché à l'établissement. Chez Servicios Financieros Carrefour, 19 identifiants compromis provenaient d'une source extérieure. Chez Wind Tre, il a suffi d'un appel téléphonique à des vendeurs, qui ont laissé prendre la main sur leur poste.

3.2 Il demeure dans le système sans être détecté

organisme	combien de temps	comment l'intrusion a été découverte	ce que cela révèle
France Travail	Du 6 février au 5 mars 2024	Alerte interne le 4 mars sur une consommation anormale de ressources ; déclaration à la CNIL le 8 mars	Un mois de consultations anormales sans alerte
Free et Free Mobile	Du 28 septembre au 22 octobre 2024	L'attaquant a lui-même prévenu l'opérateur le 21 octobre	Aucun dispositif interne n'a rien vu
Hôpital privé de la Loire	Du 26 juin au 1er juillet 2025	Signalement d'un médecin qui ne parvenait plus à se connecter	Des outils existaient mais personne n'analysait leurs relevés
The Phone House Spain	Début estimé au 31 mars 2021, découverte le 11 avril	Deux déclarations successives à l'autorité espagnole	Près de deux semaines de présence avant le blocage
Generali España	Attaque du 5 octobre 2022, fuite connue le 11 novembre	Découverte tardive	Aucun enregistrement des opérations sur l'application visée
LAZIOcrea (Italie)	Porte dérobée implantée le 25 mars 2021, attaque lancée le 31 juillet	Systèmes hors service au matin du 1er août	Quatre mois de présence latente sur le poste d'un agent en télétravail
City of Dublin ETB (Irlande)	Logiciel malveillant introduit en janvier 2018	Détecté en octobre 2018	Neuf mois sur un serveur conservant des demandes de bourses
Air Europa	Premier accès le 12 mai 2018	Alerte des émetteurs de cartes bancaires en octobre 2018, après des fraudes	Cinq mois, et une découverte venue de l'extérieur
ECG Médica (Espagne)	Premiers mouvements le 25 juin 2024	Courriels de chantage reçus du 23 au 25 juillet	Un mois sans alerte, jusqu'à ce que l'attaquant écrive

3.3 Il accède à beaucoup plus que nécessaire

Un seul compte ouvrait l'ensemble de la base. Chez France Travail, les conseillers pouvaient consulter les données de personnes qu'ils n'accompagnaient pas, ce qui a porté à 36,8 millions le nombre de personnes exposées. Chez Transavia, deux comptes du service informatique protégés par des mots de passe courants donnaient accès à presque tout le domaine, soit les données de 25 millions de personnes. À l'Hôpital privé de la Loire, 524 867 fiches de patients ont été extraites à partir d'un compte unique.

3.4 L'ampleur : combien de personnes, quelles données

Toutes les décisions ne disent pas combien de personnes ont été touchées. En additionnant les seules 59 décisions qui donnent un chiffre, on atteint 116 millions de personnes, sans compter l'affaire Meta de 2022, qui portait à elle seule sur environ 533 millions de comptes dans le monde. Ce total est un

minimum. Il comporte aussi des doublons : une même personne peut figurer dans plusieurs fuites, ce qui est précisément le problème.

organisme	personnes ou contrats touchés
France Travail	36 800 000
Free Mobile (contrats mobiles)	19 460 891
The Phone House Spain	13 000 000
Sprinter Megacentros del Deporte	6 381 913
Agence nationale des recettes (Bulgarie)	6 000 000
Free (contrats fixes)	5 172 577
Cosmote (Grèce)	4 792 869
Meta jetons d'accès (Union européenne)	3 000 000
Morele.net	2 200 000
Miljödata	2 200 000
Sportadmin	2 126 075
Iberdrola (clients de deux filiales)	1 607 550
47 autres décisions chiffrées	13 370 560
Total	**116 112 435**

Free et Free Mobile : nombre de contrats donné par les délibérations de la CNIL. Transavia : 83 000 personnes dont les données ont été copiées, sur plus de 25 millions accessibles. Hôpital privé de la Loire : patients seuls, sans les 202 246 personnes de confiance. Meta : personnes concernées dans l'Union. Agence bulgare des recettes et DSK Bank : chiffres de sources secondaires.

Les données touchées

type de données	de quoi s'agit-il	exemples dans le corpus
Identité et coordonnées	Nom, adresse, téléphone, courriel. Présentes dans presque toutes les fuites.	Free, France Travail, Sprinter, Morele.net, Sportadmin
Données bancaires	Numéros de compte (IBAN), moyens de paiement	Free et Free Mobile, Air Europa, Wind Tre, UniCredit
Numéros officiels et pièces d'identité	Numéro de sécurité sociale, copies de cartes d'identité	France Travail, Hôpital privé de la Loire
Données de santé	Dossiers de patients, analyses, suivi psychologique	Dedalus Biologie, Vastaamo, ASL Napoli 3 Sud, Centric Health, hôpitaux polonais et irlandais
Données génétiques	Résultats de tests ADN, origines	23andMe
Mots de passe	Les clés d'accès aux comptes	Knuddels, UniCredit, Telefónica
Données de communication	Relevés d'appels, messageries	Cosmote, Maynooth University

3.5 Pourquoi ces données intéressent : ce qu'un fraudeur en fait

> repère
>
> Un nom, une adresse ou un numéro de compte ne valent presque rien pris isolément. Leur valeur vient de ce qu'ils rendent un mensonge crédible. Celui qui connaît votre nom, votre adresse, votre banque et votre opérateur peut vous écrire ou vous appeler en se faisant passer pour eux, et vous n'avez aucune raison de vous méfier.

donnée volée	ce qu'un fraudeur peut en faire	ce que montrent les décisions et les sources publiques
Nom, adresse, téléphone, courriel	Envoyer de faux messages ou de faux courriers au nom d'un organisme que la victime connaît, pour lui soutirer un paiement ou un mot de passe (hameçonnage)	Après l'attaque de Servicios Financieros Carrefour, des clients ont reçu de faux courriels au nom de l'établissement, qui reprenaient leur nom, leur adresse et leur numéro de carte de fidélité. Chez Morele.net (Pologne), des clients ont reçu des SMS frauduleux. Après la fuite de Gestores Administrativos Reunidos, deux clients ont signalé à l'autorité espagnole une escroquerie par téléphone.
Coordonnées bancaires (IBAN)	Mettre en place des prélèvements sur le compte de la victime, ou se faire passer pour son conseiller bancaire	La CNIL relève, dans la décision Free Mobile, qu'un IBAN usurpé permet de souscrire un prélèvement sur des sites qui valident le mandat par une simple case à cocher.
Numéro de sécurité sociale, copie de pièce d'identité	Usurper l'identité de la victime pour ouvrir un compte, souscrire un crédit ou accomplir des démarches à sa place	À l'Hôpital privé de la Loire, la CNIL évoque des usurpations d'identité et des démarches administratives au nom de patients mineurs, protégés ou décédés.
Données de santé, données génétiques	Faire chanter la personne, ou la cibler en fonction de sa fragilité	Chez Vastaamo (Finlande), le vol de la base de patients a été suivi d'une demande de rançon.
Mots de passe	Entrer dans les autres comptes de la victime, qui réutilise souvent le même mot de passe	Chez Cosmote, le mot de passe d'un salarié provenait d'une ancienne fuite de LinkedIn. Chez Carrefour et 23andMe, les comptes ont été ouverts avec des mots de passe volés ailleurs.
Messagerie d'un salarié	Écrire au nom de l'organisme à ses clients ou fournisseurs pour détourner des paiements	À l'université de Maynooth, des messageries de salariés ont été utilisées à des fins de fraude.
Adresse du domicile associée à une activité ou à un patrimoine	Repérer des cibles pour des vols ou des violences	Le rapport d'activité 2025 de Cybermalveillance.gouv.fr rapporte des cambriolages et des visites de faux policiers chez des licenciés de la Fédération française de tir, et des violences contre des détenteurs de crypto-actifs, à la suite de fuites de données.

Chaque fuite alimente la suivante. Les données volées sont revendues, croisées avec celles d'autres fuites et réutilisées, y compris pour pénétrer d'autres organismes. La CNIL chiffre ce coût collectif : son étude de juin 2025 évalue entre 585 millions et 1,4 milliard d'euros par an, à l'échelle de l'Union, les pertes liées à l'usurpation d'identité que la seule information des victimes permet d'éviter.

3.6 Qui attaque : pas besoin d'être une organisation

Les décisions des autorités ne s'intéressent pas à l'auteur de l'attaque, qui relève du juge pénal. Les informations judiciaires rendues publiques en France complètent le tableau, et elles vont toutes dans le même sens.

affaire	ce qui a été rendu public sur les suspects
France Travail (2024)	Trois personnes âgées de 21 à 23 ans interpellées le 17 mars 2024, selon le parquet de Paris
Free (2024)	Un mineur de 16 ou 17 ans selon les sources, déjà connu pour des faits similaires, mis en examen en janvier 2025
Agence nationale des titres sécurisés (2026)	Un adolescent de 15 ans interpellé en avril 2026
Administration fiscale (2026)	Deux suspects de 16 et 18 ans mis en examen
Ensemble des vols de données, septembre 2023 à janvier 2026	31 personnes mises en cause en France : des hommes de 13 à 23 ans, majoritairement mineurs, âgés de 17 ans en moyenne, souvent isolés, selon une note du ministère de l'Intérieur révélée par la presse

Les personnes citées sont présumées innocentes. Sources : communiqués du parquet de Paris repris par l'AFP ; Le Monde, 22 mai 2026 ; Public Sénat.

Ce constat éclaire tout le rapport. Si un adolescent parvient à copier les données de dix-neuf millions de clients d'un opérateur, ce n'est pas parce qu'il dispose de moyens exceptionnels. C'est parce que la porte n'était fermée que par un mot de passe et que personne ne surveillait. Les défauts sanctionnés sont ceux qui mettent ces attaques à la portée du premier venu.

Deux nuances s'imposent. Certaines attaques restent le fait de groupes criminels organisés, en particulier les rançongiciels : celle de Postel est attribuée au groupe Medusa. Par ailleurs, toutes les fuites revendiquées ne sont pas réelles : l'ANSSI indique que 60 % des vols de données dont elle a été saisie en 2025 n'étaient pas avérés.

partie 4

Ce que les autorités reprochent, et pourquoi cela manquait

D'un pays à l'autre, les autorités reprochent les mêmes défauts. Dix reviennent sans cesse.

Chacun est présenté de la même façon : un encadré explique de quoi il s'agit, puis un tableau donne, pour les décisions les plus parlantes, ce qui s'est passé et ce que l'autorité a reproché. Deux questions viennent ensuite, que tout lecteur se pose : pourquoi ces précautions, pourtant connues, n'étaient-elles pas en place (4.11) ? Et où faut-il regarder, dans une organisation, pour s'assurer qu'elles le sont (4.12) ?

4.1 Des accès distants sans authentification multifacteur

> repère
>
> L'**authentification multifacteur** consiste à exiger, en plus du mot de passe, une seconde preuve d'identité : un code reçu sur le téléphone, une clé physique, une application. Chacun la connaît pour sa banque en ligne. Sans elle, un mot de passe volé suffit à entrer. Un **VPN** est le tunnel sécurisé par lequel un salarié ou un prestataire se connecte au réseau de l'entreprise depuis l'extérieur : c'est la porte d'entrée à distance, et donc celle qu'il faut le mieux garder.

C'est le grief le plus constant des décisions récentes. L'accès par réseau privé virtuel, par portail externe ou par compte de prestataire n'exigeait qu'un identifiant et un mot de passe.

décision	amende	ce qui s'est passé	ce qui a été reproché
CNIL, 8 janv. 2026, SAN-2026-001, Free Mobile	27 M€	À l'automne 2024, un pirate entre par l'accès à distance réservé aux salariés et consulte pendant près d'un mois les données de 19,46 millions de contrats mobiles, dont des coordonnées bancaires.	L'accès à distance n'exigeait pas de seconde preuve d'identité et ne vérifiait pas l'ordinateur utilisé. Rien n'a signalé l'activité anormale.
CNIL, 8 janv. 2026, SAN-2026-002, Free	15 M€	Même intrusion ; 5,17 millions de contrats fixes concernés.	Mêmes défauts sur l'accès à distance et la détection.
CNIL, 22 janv. 2026, SAN-2026-003, France Travail	5 M€	En février 2024, des pirates se font passer pour des conseillers et prennent le contrôle de leurs comptes. Ils accèdent un mois durant aux données de 36,8 millions de personnes.	Mots de passe trop faibles, pas de seconde preuve d'identité alors qu'elle était prévue depuis 2023, accès des conseillers trop étendus.
CNIL, 21 juill. 2026, SAN-2026-009, Hôpital privé de la Loire	500 000 €	En juin 2025, un pirate muni des identifiants d'un médecin libéral copie 524 867 fiches de patients en cinq jours.	Le logiciel proposait la seconde preuve d'identité ; elle n'était pas activée pour les utilisateurs extérieurs.
AEPD, 10 déc. 2024, PS-00453-2023, Generali España	4 M€	En octobre 2022, un pirate utilise les identifiants d'un courtier et interroge en masse un formulaire de consultation. Plus d'un million de personnes sont informées.	Aucune seconde preuve d'identité pour les courtiers ; aucun enregistrement des opérations sur l'application.

décision	amende	ce qui s'est passé	ce qui a été reproché
AEPD, 14 mars 2025, PS-00128-2024, Centros Comerciales Carrefour	3,2 M€	Des comptes clients sont ouverts par des tiers à cinq reprises, avec des mots de passe volés ailleurs.	La seconde preuve d'identité n'a été mise en place qu'après les premières attaques.
AKI (Estonie), 5 sept. 2025, Allium UPI (Apotheka)	3 M€	La base du programme de fidélité d'une chaîne de pharmacies est volée ; 750 000 personnes sont concernées.	Pas de seconde preuve d'identité ; un même compte d'administrateur utilisé par plusieurs personnes.
AEPD, 16 juill. 2026, PS-00140-2025, 23andMe	2,4 M€	Des comptes d'un service de tests génétiques sont ouverts avec des mots de passe volés ailleurs ; des données génétiques et d'origine sont mises en vente.	La seconde preuve d'identité était seulement proposée, et non imposée, pour des données aussi sensibles.
AEPD, 26 sept. 2024, PS-00291-2023, Telefónica de España	1,3 M€	En septembre 2022, des tiers utilisent l'identifiant d'un salarié sur une application interne ouverte sur internet ; 1,4 million de clients sont concernés.	Accès par simple identifiant et mot de passe ; données non chiffrées.
AEPD, 10 mars 2021, PS-00179-2020, Air Europa	600 000 €	Des tiers accèdent aux coordonnées et aux données bancaires d'environ 489 000 personnes.	Systèmes reliés à internet sans seconde preuve d'identité ; autorité prévenue tardivement.

4.2 Des mots de passe faibles, partagés ou mal conservés

> repère
>
> Un mot de passe court ou courant se devine en quelques essais automatisés. Un compte partagé par plusieurs personnes empêche de savoir qui a fait quoi. Un mot de passe conservé « en clair », c'est-à-dire lisible tel quel dans la base, est immédiatement utilisable par celui qui vole la base. La règle de l'art est de n'en conserver qu'une empreinte irréversible, obtenue par une opération appelée **hachage**.

décision	ce qui s'est passé	ce qui a été reproché
Garante, 8 févr. 2024, n° 9991020, UniCredit, 2,8 M€	Une attaque vise le portail de banque sur mobile ; l'identité de clients est accessible sans code, et des codes sont découverts.	Rien ne limitait le nombre d'essais ; des codes trop simples étaient acceptés.
AEPD, 5 févr. 2024, PS-00145-2023, I-DE Redes Eléctricas Inteligentes, 3,5 M€	En mars 2022, une application en ligne du distributeur d'électricité est attaquée ; 1 350 000 clients sont concernés.	Défaut de l'application et règles de mots de passe trop faibles.
AEPD, 18 août 2023, PS-00565-2023, Holaluz-Clidom, 675 000 €	En octobre 2022, un tiers se connecte avec les identifiants d'un prestataire commercial et télécharge massivement des données de clients.	Un seul compte était partagé par 120 personnes chez le prestataire : impossible de savoir qui faisait quoi.
AP (Pays-Bas), 23 sept. 2021, Transavia, 400 000 €	En 2019, un pirate devine les mots de passe de deux comptes du service informatique. Il peut atteindre les données de 25 millions de personnes et en copie 83 000.	Mots de passe courants ; réseau sans séparation interne.
LfDI Bade-Wurtemberg, 21 nov. 2018, Knuddels, 20 000 €	En juillet 2018, les mots de passe et adresses électroniques d'environ 330 000 utilisateurs sont révélés.	Les mots de passe étaient conservés lisibles dans la base. C'est la décision la plus ancienne du corpus.

4.3 Des correctifs non installés et des systèmes obsolètes

repère

Lorsqu'un éditeur de logiciel découvre un défaut de sécurité, il publie un **correctif**, c'est-à-dire une mise à jour qui le répare. La publication du correctif révèle aussi l'existence du défaut : les attaquants cherchent alors les organismes qui ne l'ont pas installé. Tarder à mettre à jour revient à laisser ouverte une porte dont l'emplacement vient d'être rendu public.

décision	ce qui s'est passé	ce qui a été reproché
Garante, 4 juill. 2024, n° 10063782, Postel, 900 000 €	En août 2023, des pirates bloquent les serveurs et copient des données pour exiger une rançon.	La réparation du défaut exploité était disponible et signalée ; elle n'avait pas été installée.
AEPD, 11 mars 2026, PS-00437-2024, Iberia, 650 000 €	En janvier 2023, des données de la compagnie sont copiées depuis le système d'un prestataire.	Deux défauts connus depuis 2017 et 2019, réparés par l'éditeur, ne l'étaient pas chez le prestataire ; la compagnie ne vérifiait rien.
Garante, 21 mars 2024, n° 10002324, LAZIOcrea, 271 000 €	Dans la nuit du 31 juillet au 1er août 2021, un rançongiciel paralyse les services de santé de la région de Rome. La porte dérobée avait été posée quatre mois plus tôt sur l'ordinateur d'un agent en télétravail.	Accès à distance par simple mot de passe ; réseau non cloisonné ; un serveur dont le système n'était plus mis à jour ; alertes mal traitées.
UODO, 30 juin 2025, DKN.5131.48.2022, hôpital pédiatrique de Białystok, 66 500 zlotys (environ 15 800 €)	Un rançongiciel bloque les systèmes de l'hôpital.	Logiciels non à jour ; aucune vérification régulière.
NAIH (Hongrie), 22 juin 2023, Digi, 80 millions de forints (environ 216 500 €)	Un pirate accède par le site de l'opérateur aux données d'environ 322 000 personnes, restées dans une base d'essai.	Défaut du logiciel du site connu depuis plus de neuf ans, jamais réparé ; base d'essai jamais supprimée.
APD (Belgique), 17 déc. 2024, n° 166/2024, hôpital, 200 000 €	Un rançongiciel paralyse l'hôpital en 2021 ; jusqu'à 300 000 personnes concernées.	C'était le second rançongiciel en deux ans et demi ; les leçons du premier n'avaient pas été tirées.

4.4 L'absence de journalisation exploitée et de détection

repère

La **journalisation** est l'enregistrement automatique de ce qui se passe dans un système : qui s'est connecté, quand, pour consulter quoi. C'est l'équivalent d'une caméra de surveillance. Elle ne sert à rien si personne ne regarde les images : la **détection** consiste à repérer les comportements anormaux, comme un compte qui consulte en une nuit des centaines de milliers de dossiers, et à déclencher une alerte.

Les autorités n'exigent pas un outil déterminé. Elles exigent que l'activité anormale soit détectée en temps réel ou à bref délai, et que les traces soient analysées. À l'Hôpital privé de la Loire, l'établissement disposait d'un logiciel de détection, d'un centre opérationnel de sécurité et de journaux applicatifs ; aucune alerte significative n'est remontée, et la CNIL a jugé le dispositif insuffisant faute d'analyse automatisée ou de contrôle régulier des traces. Chez Generali España, l'absence de journaux sur

l'application visée a empêché de mesurer l'attaque pendant plus d'un mois. À Østre Toten (Datatilsynet, Norvège, 7 janv. 2022, 21/00480-14, 4 millions de couronnes), les relevés du réseau ne couvraient que trois jours, ce qui a empêché de retracer la sortie des données.

4.5 Des habilitations trop larges et un réseau non cloisonné

> repère
> Les **habilitations** déterminent ce que chaque utilisateur a le droit de voir. Le principe est que chacun n'accède qu'aux données dont il a besoin pour son travail. Le **cloisonnement** applique la même logique au réseau, à la manière des portes coupe-feu d'un immeuble : l'incendie qui se déclare dans une pièce ne doit pas pouvoir gagner tout le bâtiment.

Ce manquement n'ouvre pas la porte à l'attaquant, mais il détermine l'ampleur de la fuite. France Travail, l'Hôpital privé de la Loire et Transavia en sont les illustrations principales. L'autorité espagnole a de même reproché à 23andMe l'absence de toute limite d'accès ou de téléchargement par adresse IP.

4.6 Des données non chiffrées

> repère
> Le **chiffrement** rend les données illisibles pour quiconque ne possède pas la clé. Des données chiffrées qui sont volées restent en principe inexploitables. La **pseudonymisation** consiste à séparer les données de l'identité des personnes, de sorte qu'un fichier volé ne permette pas de savoir à qui elles se rapportent.

The Phone House Spain (AEPD, 27 déc. 2023, PS-00084-2023, 6,5 M€) n'avait ni chiffré ni pseudonymisé les données d'environ 13 millions de personnes, alors que ses propres analyses d'impact prévoyaient ces mesures depuis plus de deux ans. Les données ont été publiées en clair. L'amende se décompose en 4 M€ au titre de l'article 5-1-f et 2,5 M€ au titre de l'article 32.

4.7 L'absence de tests et d'évaluation régulière

> repère
> Une mesure de sécurité peut exister sur le papier et ne pas fonctionner. L'article 32 du RGPD impose pour cette raison « une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures ».

décision	ce qui s'est passé	ce qui a été reproché
Finlande, 8 sept. 2025, TSV/3606/2024, S-Bank, 1,8 M€	En avril 2022, une modification du service de connexion de la banque introduit un défaut. Des clients signalent des anomalies pendant trois mois.	Nouvelle fonction insuffisamment essayée avant sa mise en service ; réclamations des clients non examinées.
Garante, 14 mai 2026, n° 10263796, Wind Tre, 1 715 600 €	En février 2025, un tiers interroge en série les systèmes de l'opérateur et obtient les données de 365 048 clients, dont des moyens de paiement.	Les points d'accès ouverts sur internet n'avaient jamais été soumis à une attaque simulée.
UODO, 19 janv. 2022, DKN.5130.2215.2020, Fortum et PIKA	Lors d'une intervention technique, un prestataire crée une copie de la base clients, que des tiers récupèrent.	Intervention menée sans examen préalable des risques ; prestataire non vérifié.

4.8 Le prestataire non contrôlé

> repère
> Confier des données à un prestataire ne décharge pas de la responsabilité de les protéger. L'organisme doit choisir un prestataire qui présente des garanties, l'encadrer par contrat et vérifier dans la durée que ces garanties sont réelles. La sécurité d'une chaîne est celle de son maillon le plus faible, et les attaquants visent de plus en plus le prestataire, qui détient les données de nombreux clients.

Cette catégorie est celle qui progresse le plus. La CNIL relève que 10 % des violations qui lui ont été notifiées en 2025 se rattachent à des incidents survenus chez huit sous-traitants seulement. Trois configurations se rencontrent.

Le donneur d'ordre sanctionné pour défaut de contrôle. Vodafone España a fait l'objet de quatre décisions entre août et septembre 2026 (PS-00240-2025, PS-00248-2025, PS-00253-2025, PS-00194-2025), pour un total de 2,05 M€, à la suite d'attaques survenues chez quatre sous-traitants différents. L'autorité y relève des comptes génériques sans second facteur chez les prestataires et l'absence d'audit périodique par l'opérateur. Iberia a été sanctionnée parce qu'elle ne disposait d'aucun mécanisme pour vérifier la sécurité de son prestataire. Quatorze caisses rurales espagnoles ont été sanctionnées en janvier 2025 après l'exploitation, en novembre 2022, d'une vulnérabilité chez leur sous-traitant informatique commun, découverte un mois plus tard.

Le client et le prestataire sanctionnés ensemble. Après le rançongiciel de l'été 2021 contre les systèmes de santé du Latium, le Garante a sanctionné le même jour le prestataire LAZIOcrea (271 000 €) et la Région (120 000 €), celle-ci pour défaut de surveillance.

Le sous-traitant sanctionné en propre. La CNIL a infligé 1,5 M€ à Dedalus Biologie, éditeur de logiciels pour laboratoires, après la diffusion des données de 491 840 patients (SAN-2022-009, 15 avril 2022, articles 28, 29 et 32). L'autorité espagnole a sanctionné Konecta BTO, prestataire de relation client, pour des vulnérabilités déjà relevées en audit (PS-00613-2025, 22 avril 2026, 300 000 €). Elle a aussi sanctionné Iberdrola, en qualité de sous-traitant de deux sociétés de son groupe dont elle gérait la base de données, après l'attaque qui a touché I-DE Redes (PS-00221-2023, 7 févr. 2024, 3 M€). L'autorité polonaise a sanctionné dans la même décision le fournisseur d'énergie Fortum et son prestataire PIKA, et, dans une autre, un centre social et le maire de la commune, qui hébergeait ses données.

> **Une illustration récente : Maileva.** Maileva, filiale de Docaposte (groupe La Poste), envoie des documents pour le compte d'entreprises et d'institutions. Selon le communiqué du groupe du 15 novembre 2026, une cyberattaque survenue à la mi-septembre a permis de dérober les nom, prénom et adresse postale de 22 millions de destinataires. Les personnes touchées n'ont jamais contracté avec Maileva : elles ont reçu un courrier de leur banque, de leur assureur ou d'une administration. Une seule attaque atteint ainsi les fichiers de nombreux organismes à la fois.
>
> Le mode opératoire n'est pas public. Rien ne permet de dire qu'une précaution a fait défaut, et ce rapport ne formule aucune appréciation sur ce point. Trois opérateurs postaux européens ont en revanche déjà été sanctionnés après une attaque.

organisme	décision	amende	ce qui s'est passé	ce qui a été reproché
Postel (Italie), société du groupe Poste Italiane spécialisée dans la gestion de documents et de communications pour le compte d'entreprises et d'administrations	Autorité italienne, 4 juillet 2024, n° 10063782	900 000 €	En août 2023, un groupe de pirates a bloqué les serveurs et copié les données d'environ 25 000 personnes pour exiger une rançon.	Le logiciel de messagerie présentait un défaut connu. L'éditeur avait publié la réparation et l'agence italienne de cybersécurité avait alerté. La mise à jour n'avait pas été faite pendant près d'un an, selon l'autorité italienne.
ELTA, poste grecque	Autorité grecque, 28 février 2024, n° 10/2024	2 995 140 €	Le 20 mars 2022, des pirates ont pris la main à distance sur des postes de travail, obtenu les mots de passe des administrateurs du réseau, bloqué les fichiers puis publié des données.	Les règles de sécurité que l'entreprise s'était fixées n'étaient pas appliquées.
Postes bulgares	Autorité bulgare, 4 mai 2022	500 000 €	Attaque informatique contre l'opérateur postal.	Texte officiel non consulté ; décision connue par des sources secondaires.

4.9 Le risque identifié et non traité

> repère
>
> L'**analyse d'impact** est le document par lequel un organisme évalue, avant de traiter des données sensibles ou nombreuses, les risques encourus par les personnes et les mesures pour les réduire. Elle est obligatoire dans certains cas. Lorsqu'elle signale un risque et que rien n'est fait, elle prouve que l'organisme savait.

Ce constat traverse les catégories précédentes et pèse sur le montant de l'amende, parce qu'il établit la négligence.

organisme	ce que l'organisme savait	ce qui est arrivé ensuite
France Travail	Seconde preuve d'identité prévue par ses propres études de risques dès 2023, puis repoussée	Données de 36,8 millions de personnes exposées en 2024
Hôpital privé de la Loire	Absence de cloisonnement des dossiers désignée par sa propre analyse d'impact de 2021 comme la principale menace	524 867 fiches de patients copiées en 2025
The Phone House Spain	Protection des données par chiffrement prévue par ses études depuis plus de deux ans	Données d'environ 13 millions de personnes publiées lisibles en 2021
Postel	Alertes de l'éditeur du logiciel et de l'agence nationale de cybersécurité	Serveurs bloqués et données copiées en août 2023
Flexicar (AEPD, 28 juill. 2026, PS-00540-2025, 680 000 €)	Précaution recommandée par un contrôle de sécurité de 2022, jamais mise en place	Attaque déclarée le 3 juin 2024

organisme	ce que l'organisme savait	ce qui est arrivé ensuite
Konecta BTO (AEPD, 22 avr. 2026, PS-00613-2025, 300 000 €)	Absence de seconde preuve d'identité relevée par un audit de son client en novembre 2022	Données de 808 800 personnes atteintes en mai 2024
Kræftens Bekæmpelse (Danemark, 29 sept. 2021, amende de 800 000 couronnes proposée au juge)	Seconde preuve d'identité jugée nécessaire par l'association elle-même après une attaque de 2018	Deux nouvelles tromperies par faux courriel
Hoy Voy a Conducir (AEPD, 31 juill. 2026, PS-00035-2026, 30 000 €)	Installation informatique que l'entreprise savait dépassée depuis avril 2021	Base de plus de 200 000 élèves et salariés mise en vente en 2024
Hôpital belge (APD, 17 déc. 2024, 200 000 €)	Premier rançongiciel subi en 2019	Second rançongiciel en 2021

4.10 La gestion de la violation

> repère
>
> Dans le vocabulaire du RGPD, une **violation de données** désigne tout incident qui compromet des données personnelles : fuite, perte, destruction, accès par un tiers. La loi impose alors deux démarches. L'organisme prévient l'autorité au plus vite, en principe dans les 72 heures. Il prévient aussi les personnes lorsque le risque est élevé pour elles, afin qu'elles puissent se protéger, par exemple en surveillant leurs comptes ou en se méfiant de faux messages.

L'attaque ouvre une seconde série d'obligations, dont la méconnaissance est sanctionnée de façon autonome. Free et Free Mobile sont les premiers organismes sanctionnés par la CNIL pour une information incomplète des personnes. L'Hôpital privé de la Loire l'a été pour avoir omis d'informer plus de 200 000 personnes de confiance désignées par les patients. Postel et Air Europa l'ont été pour une notification insuffisante ou tardive à l'autorité (quarante et un jours pour la compagnie aérienne), de même que 23andMe, le Teaching Council et l'université de Maynooth en Irlande. Vastaamo (Finlande, 7 déc. 2021, 608 000 €) n'a prévenu l'autorité et ses patients qu'à l'automne 2020, d'une intrusion de mars 2019. En Espagne, l'autorité a dû ordonner à Gestores Administrativos Reunidos de prévenir les personnes. En Irlande, le même refus a valu 50 000 € à l'organisme public City of Dublin ETB.

4.11 Pourquoi ces précautions manquaient : ce que les organismes ont répondu

Si ces précautions sont connues, pourquoi ne sont-elles pas prises ? Les décisions permettent de répondre, parce qu'elles rapportent les explications que les organismes ont données pour leur défense. Ces explications ne sont pas absurdes. Elles décrivent des difficultés réelles, que toute organisation reconnaîtra.

l'explication donnée	l'exemple	la réponse de l'autorité
La précaution dépendait d'un partenaire.	France Travail ouvrait son système aux conseillers de Cap emploi, structures indépendantes. Exiger un code en plus du mot de passe supposait que ces structures équipent leurs salariés d'un téléphone. Elles ne l'ont pas fait, puis ont refusé la solution de remplacement.	Celui qui ouvre son système en reste responsable. D'autres solutions existaient, comme la distribution de petits boîtiers générateurs de codes.

l'explication donnée	l'exemple	la réponse de l'autorité
Le service ne pouvait pas s'arrêter.	France Travail explique que suspendre l'accès des Cap emploi aurait interrompu l'accompagnement de demandeurs d'emploi. À l'Hôpital privé de la Loire, une fois l'attaque découverte, un même mot de passe provisoire a été donné dans l'urgence à tous les médecins extérieurs, pour ne pas interrompre les soins.	La continuité du service compte, mais le risque devait peser davantage dans la balance, d'autant que des solutions intermédiaires existaient.
Un projet plus vaste était en cours.	En 2024, le logiciel de l'Hôpital privé de la Loire aurait permis d'exiger une seconde preuve d'identité. L'hôpital a préféré attendre la solution retenue par son groupe, déployée en septembre 2025, après l'attaque. The Phone House prévoyait de chiffrer ses données depuis plus de deux ans.	Seul compte ce qui était en place le jour de l'attaque. Un projet n'est pas une protection.
Le logiciel ne le permettait pas.	Le logiciel de dossiers médicaux de l'hôpital ne savait pas réserver chaque dossier à l'équipe qui soigne le patient, et en changer était lourd. Chez LAZIOcrea, un serveur gardait un système dépassé pour faire fonctionner une ancienne application. Chez Dedalus, l'outil ne savait exporter que le fichier entier.	La limite d'un outil ne dispense pas de protéger les données. Elle impose de compenser par d'autres moyens, ou de changer d'outil.
Le risque paraissait théorique.	France Travail jugeait le risque « seulement théorique » au vu de ses autres protections. Generali avait estimé que son fichier présentait un risque faible et ne méritait pas d'étude approfondie. Un opticien en ligne faisait valoir que des banques acceptent des mots de passe de cinq caractères.	Le risque s'apprécie d'après le nombre de personnes et la nature des données, et non d'après ce que font les autres.
Les outils de surveillance existaient.	L'Hôpital privé de la Loire disposait d'un logiciel de détection et d'une équipe de surveillance. Ils étaient réglés pour repérer une surcharge du réseau. La copie de 73 fiches par minute n'en provoquait aucune.	Il manquait l'essentiel : un examen automatique de ce que chaque compte fait dans le logiciel qui contient les données.
Le prestataire avait dit que tout était en ordre.	Konecta avait déclaré, lors des contrôles de son client, respecter les exigences du contrat. Vodafone imposait des obligations par contrat mais n'a pu justifier d'aucun contrôle. Iberia objectait qu'on ne peut pas contrôler les outils de centaines de fournisseurs.	L'autorité espagnole ne demande pas de tout vérifier. Elle rappelle que l'organisme répond du résultat, et qu'il lui faut donc un moyen de s'assurer de ce que font ses prestataires.

Un trait commun se dégage. Dans aucune de ces affaires, l'organisme n'ignorait la précaution. Il l'avait remise à plus tard, pour une raison qui paraissait bonne sur le moment : un partenaire qui ne suit pas, un logiciel ancien, un budget, un service qui ne peut pas s'interrompre. Les autorités ne nient pas ces difficultés. Elles répondent qu'une difficulté appelle une solution de remplacement et une décision assumée par la direction, et non l'attente.

L'explication est aussi économique. Selon une étude publiée par la CNIL en juin 2025, une partie du coût d'une fuite est supportée par d'autres que l'organisme, au premier rang desquels les personnes concernées, ce qui l'incite à investir moins qu'il ne faudrait (voir partie 5).

4.12 Où porter l'attention : les personnes, les contrats, les réglages

Dire qu'il faut « une seconde preuve d'identité » ou « des mises à jour » ne suffit pas. Ces précautions sont fastidieuses à mettre en place, et c'est aux endroits où elles sont le plus pénibles qu'elles manquent. Les décisions montrent où regarder.

précaution	où elle manque le plus souvent	ce qui la rend difficile	le contrat ou le document à vérifier
Seconde preuve d'identité	Chez ceux qui se connectent sans être salariés : médecins libéraux et leurs secrétariats (environ 450 utilisateurs extérieurs à l'Hôpital privé de la Loire), partenaires (France Travail), courtiers (Generali), points de vente (Wind Tre), prestataires (Vodafone)	Il faut équiper des personnes que l'on n'emploie pas, et quelqu'un doit payer le téléphone ou le boîtier	La convention de partenariat, le contrat d'exercice, le contrat de distribution ou de sous-traitance : qui fournit le second moyen d'identification, et à quelle date
Mots de passe	Comptes de clients sur les sites en ligne ; comptes techniques ; comptes partagés par toute une équipe chez un prestataire (120 personnes chez celui d'Holaluz) ; mots de passe d'origine jamais changés (Casa di cura Borghi)	Les anciens logiciels acceptent des mots de passe faibles ; les comptes partagés sont commodes	Le cahier des charges du site ou du logiciel ; les règles imposées au prestataire
Mises à jour	Tout ce qui est relié à internet : messagerie (Postel), site marchand (Digi, boutique en ligne de Basse-Saxe), équipements du prestataire (Iberia)	Il faut savoir ce que l'on possède ; une vieille application peut cesser de fonctionner après la mise à jour	Le contrat de maintenance : dans quel délai une réparation de sécurité est installée, et qui le vérifie
Enregistrement et alerte	Dans le logiciel qui contient les données (dossier patient, gestion des abonnés, formulaire de consultation), et pas seulement sur le réseau	Il faut définir ce qu'est un comportement anormal, par exemple le nombre de fiches qu'un compte consulte en une heure, et désigner quelqu'un pour traiter l'alerte	Le contrat avec l'éditeur du logiciel et avec l'équipe de surveillance : quelles traces sont conservées, combien de temps, qui les examine
Accès limités	Comptes des partenaires (France Travail), comptes du service informatique (Transavia), logiciel conçu sans cloisonnement (Hôpital privé de la Loire)	Restreindre les accès complique le travail quotidien, et certains logiciels ne le permettent pas	Le tableau qui dit qui a droit à quoi, comparé à ce que les comptes peuvent réellement faire
Sauvegardes	Sauvegardes atteintes en même temps que le reste, parce qu'elles étaient sur le même réseau (ASL Matera, Østre Toten, NIER) ; sauvegarde trop ancienne (Dentalcuadros) ; serveur de sauvegarde en panne (commune polonaise)	Il faut une copie hors d'atteinte du réseau, et l'essayer réellement	Le compte rendu du dernier essai de restauration
Prestataires	Sous-traitant du sous-traitant, dont personne ne connaît l'existence (UniCredit, Vodafone) ; accès permanent laissé à l'éditeur d'un logiciel pour la maintenance (Hôpital privé de la Loire) ; base commune à tout un groupe (Iberdrola)	Le prestataire détient les données de nombreux clients et se contrôle mal de l'extérieur	Le contrat prévu par l'article 28 du RGPD : droit de contrôle réellement exercé, autorisation préalable de tout nouveau sous-traitant, délai d'alerte en cas d'incident

précaution	où elle manque le plus souvent	ce qui la rend difficile	le contrat ou le document à vérifier
Moments de changement	Migration de données (Dedalus, CityBee), intervention technique (Fortum, ID Finance), projet mené dans l'urgence (Fastway), nouvelle fonction mise en service (S-Bank, Sportadmin), base d'essai contenant de vraies données (Digi, MyConnector)	Les projets vont vite, et les copies de travail sont oubliées une fois le projet fini	La procédure de mise en service : essais préalables, suppression des copies, données fictives pour les essais

Les autorités vont parfois jusqu'à fixer le réglage attendu. Ces exigences donnent une idée concrète de ce que recouvre « l'état de l'art ».

ce que l'autorité a exigé ou rappelé	décision
Bloquer un compte après dix essais de mot de passe au plus	CNIL, France Travail, rappelant sa recommandation de 2022
Déclencher des alertes selon des seuils d'erreurs et de sollicitations, et vérifier par des attaques simulées que la détection fonctionne	CNIL, France Travail
Exiger une seconde preuve d'identité pour tout compte qui se connecte à distance, et imposer des mots de passe complexes	Roumanie, PGS Sofa
N'autoriser l'accès aux équipements que depuis le réseau interne ou, à défaut, par un accès à distance sécurisé assorti d'une seconde preuve d'identité	Roumanie, Auchan et Agricola International
Conserver l'enregistrement des accès au moins trente jours, et en garder une copie	Roumanie, Gerocossen et Primonet
Fixer un délai moyen pour détecter les défauts de sécurité et un délai moyen pour les réparer	Italie, Postel
Utiliser des données fictives, et non de vraies données, pour les essais d'une application	Roumanie, MyConnector

partie 5

Des mesures connues

Aucune des mesures dont l'absence est sanctionnée n'est nouvelle. Toutes figurent dans deux documents publics et gratuits.

défaut sanctionné	la précaution attendue	guide cnil (version 2024)	guide anssi
Pas de seconde preuve d'identité	Demander un code ou une clé en plus du mot de passe pour toute connexion depuis l'extérieur	Fiches 4 et 8	Mesures 13 et 32
Mots de passe faibles ou lisibles	Imposer des mots de passe solides, bloquer les essais répétés, ne jamais les conserver lisibles	Fiches 4 et 21 ; délibération n° 2022-100	Mesures 10 et 11
Mises à jour non faites	Installer sans délai les réparations de sécurité publiées par les éditeurs	Fiche 9	Mesures 34 et 35
Ni enregistrement ni alerte	Enregistrer qui fait quoi, et surveiller ces relevés pour repérer une activité anormale	Fiche 16 ; délibération n° 2021-122	Mesure 36
Accès trop larges	Ne donner à chacun que l'accès dont il a besoin ; séparer le réseau en zones	Fiches 5 et 8	Mesure 19
Données non chiffrées	Rendre les données illisibles sans clé, pour qu'un vol reste sans conséquence	Fiches 13 et 21	Mesures 18 et 31
Sauvegardes défaillantes	Conserver des copies à l'abri et vérifier qu'elles permettent de tout rétablir	Fiche 17	Mesure 37
Aucune vérification	Faire éprouver régulièrement ses défenses	Fiches 1 et 11	Mesure 38
Prestataire non contrôlé	Exiger des garanties par contrat et aller vérifier	Fiche 14	Mesure 3
Risque connu non traité	Suivre l'exécution des décisions prises après chaque étude de risques	Fiche 20	Mesure 41

La CNIL a renforcé ces préconisations pour les grandes bases de données : ses consignes du 30 avril 2025 présentent l'authentification multifacteur sur les accès externes comme une mesure en principe requise, et recommandent la journalisation, l'analyse des flux et la limitation des volumes exportables. Son bilan du 28 janvier 2025 décrit le même enchaînement que le corpus : identifiants compromis, système accessible depuis internet, habilitations trop larges, extraction massive non détectée.

L'écart entre la règle connue et la pratique a une explication économique. Une étude publiée par la CNIL en juin 2025 estime, sur la base d'un modèle théorique, que les entreprises sous-investissent en cybersécurité dans une proportion comprise entre 20 % et 66 %, parce qu'une partie du coût d'une fuite est supportée par des tiers, au premier rang desquels les personnes concernées.

partie 6

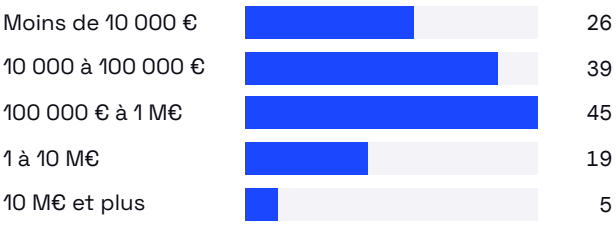
Les sanctions, d'un pays à l'autre

Le même règlement s'applique dans tous les pays de l'Union. Les sanctions, elles, diffèrent par leur montant, par le temps qu'elles mettent à venir et par le texte sur lequel elles reposent.

6.1 La distribution des montants

repère

L'amende **médiane** est celle qui partage les décisions en deux moitiés égales : la moitié des amendes lui est inférieure, l'autre supérieure. Elle décrit mieux la sanction ordinaire que la moyenne, tirée vers le haut par quelques amendes exceptionnelles.



134 décisions dont le montant est connu. Espagne : montant dû après réduction légale. Hors zone euro : contre-valeur (voir Méthode).

L'amende médiane s'établit à 105 500 €. Le total de 635 M€ est concentré sur un petit nombre de décisions : trois décisions irlandaises visant Meta en représentent 516 M€, et les décisions Free et Free Mobile 42 M€. Hors Meta, le cumul atteint 119 M€.

La majorité des sanctions frappe donc des organismes de taille moyenne ou modeste, pour des montants de quelques milliers à quelques centaines de milliers d'euros.

6.2 Les amendes les plus élevées

organisme et décision	amende	ce qui s'est passé
Meta - scraping Irlande, 25/11/2022	265 000 000 €	Fichier de données d'environ 533 millions d'utilisateurs Facebook mis en ligne sur une plateforme de pirates ; enquête ouverte en 2021 après la presse.
Meta (jetons d'accès) Irlande, 12/12/2024, IN-18-11-1	240 000 000 €	Du 14 au 28 septembre 2018, exploitation d'une faille de la fonction « Voir en tant que », présente depuis juillet 2017, permettant de voler des jetons d'accès à des comptes ; près de 3 millions de personnes dans l'Union.
Free Mobile France, 08/01/2026, SAN-2026-001	27 000 000 €	Du 28 septembre au 22 octobre 2024, intrusion par l'accès à distance de l'entreprise ; l'attaquant prévient lui-même l'opérateur le 21 octobre ; 19 460 891 contrats mobiles concernés, dont des IBAN ; 2 614 plaintes.
Free France, 08/01/2026, SAN-2026-002	15 000 000 €	Même intrusion ; 5 172 577 contrats fixes concernés.

organisme et décision	amende	ce qui s'est passé
Meta (jetons d'accès) Irlande, 12/12/2024, IN-18-10-1	11 000 000 €	Du 14 au 28 septembre 2018, exploitation d'une faille de la fonction « Voir en tant que », présente depuis juillet 2017, permettant de voler des jetons d'accès à des comptes ; près de 3 millions de personnes dans l'Union.
Cosmote et OTE Grèce, 27/01/2022, 4-2022	9 250 000 €	Pirate entré avec le mot de passe d'un salarié, issu d'une ancienne fuite de LinkedIn ; requêtes sur le système de données massives de l'opérateur ; données de trafic de 4 792 869 abonnés extraites.
The Phone House Spain Espagne, 27/12/2023, PS-00084-2023	6 500 000 €	Rançongiciel : début estimé au 31 mars 2021, détecté le 11 avril ; données d'environ 13 millions de clients, salariés et fournisseurs exfiltrées et publiées en clair ; deux notifications à l'AEPD.
France Travail France, 22/01/2026, SAN-2026-003	5 000 000 €	Ingénierie sociale visant des comptes de conseillers Cap emploi, du 6 février au 5 mars 2024 ; données de plus de 36,8 millions de personnes ; alerte interne le 4 mars, notification à la CNIL le 8 mars 2024.
Generali España Espagne, 10/12/2024, PS-00453-2023	4 000 000 €	Attaque par force brute détectée le 5 octobre 2022 sur le formulaire de consultation des clients, avec les identifiants d'un courtier ; fuite connue le 11 novembre 2022 ; plus d'un million de personnes informées.
I-DE Redes Eléctricas Inteligentes Espagne, 05/02/2024, PS-00145-2023	3 500 000 €	Du 7 au 15 mars 2022, extraction d'environ 4,5 millions d'enregistrements par l'application en ligne des raccordements ; 1 350 000 clients de la société ; notification le 18 mars 2022.
Centros Comerciales Carrefour Espagne, 14/03/2025, PS-00128-2024	3 200 000 €	Cinq violations notifiées : accès illégitimes à des comptes clients, très probablement par bourrage d'identifiants issus d'autres fuites.
Iberdrola Espagne, 07/02/2024, PS-00221-2023	3 000 000 €	Même attaque de mars 2022 : la base, gérée par Iberdrola pour les sociétés du groupe, contenait aussi les données de 1 515 000 clients d'Iberdrola Clientes et de 92 550 clients de Curenergía.
Allium UPI (Apotheka) Estonie, 05/09/2025	3 000 000 €	Vol de la base du programme de fidélité ; 750 000 personnes.
ELTA (poste grecque) Grèce, 28/02/2024, 10/2024	2 995 140 €	Rançongiciel du 20 mars 2022 : accès distant non autorisé aux postes de travail, mots de passe des comptes d'administration du domaine obtenus, fichiers chiffrés puis publiés sur le dark web le 4 mai 2022.
UniCredit Italie, 08/02/2024, 9991020	2 800 000 €	Du 11 au 21 octobre 2018, attaque sur le portail de banque mobile ; l'identité de clients s'affichait même en cas d'échec de connexion ; 731 519 codes clients touchés, le mot de passe étant découvert pour 6 859 d'entre eux.
Agence nationale des recettes NAP Bulgarie, 28/08/2019	2 600 000 €	Piratage de l'administration fiscale ; données d'environ 6 millions de personnes rendues accessibles.

organisme et décision	amende	ce qui s'est passé
23andMe Espagne, 16/07/2026, PS-00140-2025	2 400 000 €	Bourrage d'identifiants ; 2 642 résidents espagnols ; données génétiques et d'origine ethnique ; échantillon publié sur un forum et fichier mis en vente ; annonce repérée le 1er octobre 2023, notification le 17 octobre.
S-Bank Finlande, 08/09/2025, TSV/3606/2024	1 800 000 €	Faille introduite en avril 2022 dans le service d'identification de la banque ; paiements non autorisés au préjudice de clients ; violation notifiée le 5 août 2022.
Wind Tre Italie, 14/05/2026, 10263796	1 715 600 €	En février 2025, des tiers obtiennent par téléphone la prise en main du poste de vendeurs de deux points de vente, puis interrogent en série la base clients (environ 2 millions de requêtes) ; données de 365 048 clients, dont moyens de paiement pour 41 359.
Sprinter Megacentros del Deporte Espagne, 28/11/2025, PS-00373-2025	1 560 000 €	Premier accès illégitime le 24 octobre 2023 ; copie des données du 24 au 27 octobre puis chiffrement par rançongiciel ; 6 381 913 personnes, dont 6 351 300 clients (4 671 960 en Espagne).

Les deux décisions Meta de 2022 (265 M€) et de 2024 (240 M€) sont fondées sur l'article 25 et non sur l'article 32 ; la décision de 11 M€ sanctionne la seule notification. Leur rattachement au périmètre est discuté (voir Méthode).

6.3 Les critères retenus

- **Le nombre de personnes et la nature des données.** Données bancaires chez Free, numéro de sécurité sociale chez France Travail, données de santé et copies de pièces d'identité à l'Hôpital privé de la Loire, données génétiques chez 23andMe.
- **La négligence.** Le risque identifié et non traité est systématiquement relevé (voir 4.9).
- **Le caractère élémentaire de la mesure omise.** Les autorités soulignent que les mesures manquantes sont rappelées depuis des années par les agences de sécurité.
- **La capacité financière du groupe.** La CNIL détermine le plafond au regard du chiffre d'affaires de la société mère, conformément à la notion d'entreprise retenue par la Cour de justice (CJUE, 5 déc. 2023, C-807/21 ; 13 févr. 2025, C-383/23). Elle l'a fait pour Free (groupe Iliad) et pour l'Hôpital privé de la Loire (groupe Ramsay Santé).

6.4 Le choix du fondement détermine le plafond

> repère
>
> Le RGPD prévoit deux niveaux d'amende maximale. Un même défaut de sécurité peut être rattaché à l'article 32, qui relève du niveau bas, ou au principe général de l'article 5, qui relève du niveau haut. Selon le texte que l'autorité choisit de viser, le maximum encouru varie du simple au double.

Le manquement à l'article 32 relève du palier bas de l'article 83 (10 M€ ou 2 %). La CNIL s'y est tenue pour France Travail, établissement public sans chiffre d'affaires, sanctionné de 5 M€ sous un plafond de 10 M€. L'autorité espagnole retient fréquemment, pour les mêmes faits, le principe d'intégrité et de confidentialité de l'article 5-1-f, qui relève du palier haut (20 M€ ou 4 %), et cumule les deux amendes : 4 M€ et 2,5 M€ pour The Phone House, dont 2,5 M€ au titre de l'article 5-1-f pour I-DE Redes. Des faits identiques exposent ainsi à un plafond qui varie du simple au double selon l'autorité.

6.5 La sanction n'épuise pas le risque

L'amende administrative n'indemnise personne. Les personnes concernées peuvent agir en réparation sur le fondement de l'article 82. La difficulté tient à la preuve du lien de causalité entre une fraude déterminée et une fuite déterminée, lorsque les mêmes données ont été compromises à plusieurs reprises. Le tribunal judiciaire de Paris a rejeté pour ce motif, le 12 juin 2025, la demande qu'un abonné de Free fondait sur la fuite (RG 25/00731). La question est développée en partie 9.

6.6 Toutes les autorités sanctionnent-elles de la même façon ?

Non, et l'écart se mesure. Il ne permet pourtant pas de classer les autorités de la plus sévère à la plus clémente, pour une raison simple : elles ne jugent pas les mêmes organismes. Une amende de 5 000 € infligée à un cabinet comptable roumain et une amende de 27 M€ infligée à un opérateur français ne disent rien, à elles seules, de la sévérité de chacune. Trois éléments se laissent en revanche comparer.

Le niveau des amendes.

pays	décisions	amende médiane	amende la plus forte
France	7	1 500 000 €	27 000 000 €
Espagne	41	190 000 €	6 500 000 €
Pologne	10	132 900 €	1 135 000 €
Irlande	13	125 000 €	265 000 000 €
Italie	14	30 000 €	2 800 000 €
Roumanie	24	5 000 €	125 000 €

Pays comptant au moins sept décisions dans le corpus. La médiane française est élevée parce que la CNIL publie peu de décisions et qu'elles visent de grands organismes. L'autorité roumaine communique au contraire sur chacune de ses amendes, y compris les plus modestes.

Le temps écoulé entre l'attaque et la sanction. C'est l'écart le plus net, et il ne dépend pas de la taille des organismes.

autorité	affaire	attaque	décision	délai
France	Hôpital privé de la Loire	juin 2025	juillet 2026	13 mois
France	Free et Free Mobile	octobre 2024	janvier 2026	15 mois
Norvège	Østre Toten	janvier 2021	janvier 2022	12 mois
Suède	Miljödata	août 2025	septembre 2026	13 mois
Espagne	The Phone House	avril 2021	décembre 2023	2 ans et 8 mois
Italie	LAZIOcrea	août 2021	mars 2024	2 ans et 7 mois
Italie	UniCredit	octobre 2018	février 2024	5 ans et 3 mois
Pologne	Hôpital de Białystok	janvier 2020	juin 2025	5 ans et 5 mois
Irlande	Meta, jetons d'accès	septembre 2018	décembre 2024	6 ans et 2 mois
Irlande	Hôpital de Tullamore	novembre 2018	juin 2026	7 ans et 6 mois

Une sanction qui arrive sept ans après les faits ne joue plus le même rôle : l'organisme a changé, ses dirigeants aussi, et les personnes touchées ont cessé d'attendre.

L'amende rapportée à chaque personne touchée. Lorsque la décision donne le nombre de personnes, la division est possible. Elle va de quelques centimes à quelques euros, sans que la nature des données l'explique toujours.

affaire	autorité	personnes touchées	amende par personne
ASL Napoli 3 Sud, hôpital public	Italie	842 118	0,04 €
Miljödata	Suède	2 200 000	0,07 €
France Travail	France	36 800 000	0,14 €
The Phone House	Espagne	13 000 000	0,50 €
Free Mobile	France	19 460 891	1,39 €
Cosmote et OTE	Grèce	4 792 869	1,93 €
UniCredit	Italie	731 519	3,83 €
Allium UPI (Apotheka)	Estonie	750 000	4,00 €
Centric Health	Irlande	70 000	6,57 €

Dans ces exemples, les organismes publics sont nettement moins sanctionnés que les entreprises : quatre centimes par patient pour un hôpital public italien, quatorze centimes par personne pour France Travail. D'autres différences tiennent à la procédure. L'autorité espagnole réduit l'amende de 20 % à 40 % lorsque l'organisme paie sans contester, ce qu'ont fait 26 des 41 organismes espagnols du corpus. Au Danemark, l'autorité ne fixe pas l'amende : elle la propose au juge.

Le Comité européen de la protection des données travaille à rapprocher ces pratiques. Il a adopté le 17 septembre 2026 un projet de lignes directrices 04/2026 sur le recours à l'amende par rapport aux autres mesures correctrices, soumis à consultation publique jusqu'au 13 novembre 2026. Ce texte complète les lignes directrices 04/2022 sur le calcul du montant. Il n'est pas encore définitif.

partie 7

Enseignements pour les organismes

Les décisions désignent les vérifications que toute direction générale est en mesure d'exiger, parce que chacune appelle une réponse précise et une preuve.

question à poser	pourquoi
Tous les accès distants, y compris ceux des prestataires et des utilisateurs externes, exigent-ils un second facteur ?	Une seule exception suffit à l'attaquant (Free, Hôpital privé de la Loire, Vodafone).
Quel délai s'écoule entre la publication d'un correctif critique et son installation ?	Postel et Iberia ont été sanctionnées pour des failles dont le correctif existait.
Une extraction massive déclencherait-elle une alerte, et quelqu'un la traiterait-il ?	Disposer de journaux ne suffit pas s'ils ne sont pas analysés.
Que peut atteindre un seul compte compromis ?	La réponse mesure l'ampleur de la fuite à venir (France Travail, Transavia).
Quelles preuves de sécurité les prestataires ont-ils fournies, et quand ont-ils été contrôlés ?	La clause contractuelle ne protège pas le donneur d'ordre.
Les risques déjà écrits dans une analyse d'impact ou un audit ont-ils été traités ?	Le document qui signale un risque non traité devient une pièce à charge.
L'information des personnes serait-elle complète et exhaustive ?	Free et l'Hôpital privé de la Loire ont été sanctionnés sur ce seul terrain, en plus du défaut de sécurité.

Des défenses qui ne prospèrent pas

- **La qualité de victime.** Le dépôt de plainte et le statut de victime d'une infraction n'empêchent pas la sanction administrative. Les deux procédures avancent en parallèle.
- **La feuille de route.** Seules comptent les mesures en place au jour de l'attaque. La CNIL l'a rappelé à l'Hôpital privé de la Loire, qui invoquait une trajectoire de sécurisation en cours de déploiement.
- **La faute du prestataire.** Le responsable de traitement répond du choix et du suivi de son sous-traitant.
- **L'existence d'outils.** La présence d'un centre opérationnel de sécurité ou d'un logiciel de détection n'exonère pas si l'attaque n'a pas été détectée.

La taille ne protège pas davantage. Le corpus comprend des opérateurs de télécommunications et des banques, mais aussi des communes, des hôpitaux, des universités, une association de lutte contre le cancer, un parti politique, un cabinet d'avocats et des commerces en ligne. Le montant s'ajuste aux capacités de l'organisme ; le reproche reste le même.

partie 8

Auditer autrement : la preuve plutôt que la déclaration

Les autorités sanctionnent un état de fait, et non un état documentaire. La question est de savoir si les méthodes d'audit habituelles permettent de voir l'écart entre les deux.

repère

Un **audit de conformité** vérifie qu'un organisme respecte ses obligations. Il prend souvent la forme d'un questionnaire et d'un examen de documents : registre des traitements, politique de sécurité, contrats. Cette méthode établit ce que l'organisme déclare faire. Elle n'établit pas ce que son système fait réellement, et c'est sur ce second point que portent les sanctions.

Ce que les décisions établissent

Les décisions ne disent pas comment chaque organisme avait été audité avant l'attaque, et aucune ne met en cause une méthode d'audit. Elles établissent autre chose. Dans sept dossiers au moins, un document interne décrivait le risque ou la mesure à prendre, et la mesure n'était pas en place le jour de l'attaque : les études de risques de France Travail, de l'Hôpital privé de la Loire et de The Phone House, l'audit de cybersécurité de Flexicar, l'évaluation de Konecta, les alertes reçues par Postel, le constat de l'association danoise Kræftens Bekæmpelse (voir 4.9).

Deux de ces dossiers méritent attention. Chez Flexicar et chez Konecta, un audit avait vu juste. Le diagnostic était bon ; c'est la suite qui a manqué. L'écart ne se situe donc pas toujours dans le contrôle lui-même. Il se situe entre ce qui est écrit et ce qui est fait.

Ce que l'on peut en déduire

L'observation qui suit relève de l'expérience du cabinet, que les décisions rendent plausible sans la démontrer. Un audit fondé sur des déclarations et des documents établit ce que l'organisme dit faire. Il ne permet pas de constater qu'une fonction de sécurité existe sans être activée, qu'un outil de surveillance n'alerte personne ou qu'une décision prise n'a pas été exécutée. Or ce sont exactement les situations que les autorités ont sanctionnées.

La méthode gagne donc à changer de nature : que chaque point de contrôle se close par une preuve datée tirée du système, et non par une déclaration, et que le suivi des écarts fasse partie de l'audit.

point vérifié	question habituelle	preuve à demander	pourquoi
Connexion à distance	« Avez-vous une double authentification ? »	La liste des comptes qui en sont dispensés, prestataires compris	Le pirate passe par l'exception
Mises à jour	« Avez-vous une politique de mises à jour ? »	Un relevé récent des défauts non réparés sur les équipements reliés à internet	La règle écrite ne dit pas ce qui est réellement installé

point vérifié	question habituelle	preuve à demander	pourquoi
Surveillance	« Avez-vous une supervision ? »	Le résultat d'un essai : une copie massive de données déclenche-t-elle une alerte ?	Un outil qui n'alerte pas ne protège pas
Accès	« Les accès sont-ils limités ? »	Ce qu'un compte pris au hasard peut réellement consulter	C'est la mesure de l'ampleur d'une fuite
Mots de passe	« Sont-ils protégés ? »	La façon dont ils sont conservés dans la base	Un mot de passe lisible est utilisable par le voleur
Prestataires	« Le contrat contient-il la clause prévue ? »	Les preuves de sécurité reçues et la date du dernier contrôle	Le contrat ne remplace pas la vérification
Sauvegardes	« Sont-elles réalisées ? »	Le compte rendu du dernier essai de restauration	Une sauvegarde jamais essayée peut être inutilisable
Études de risques	« Ont-elles été réalisées ? »	La concordance entre les risques signalés et les précautions en place	Un risque écrit et non traité se retourne contre l'organisme

Le livrable change également. Au tableau de conformité se substitue un registre des écarts, où chaque écart reçoit un responsable, une échéance et une date de contre-vérification. Tout risque identifié et non traité fait l'objet d'un arbitrage signé par la direction, de sorte que la décision de ne pas agir soit prise et assumée au niveau approprié.

Une méthode en cinq temps

Ces constats conduisent à une façon de procéder que l'on peut appeler l'audit par la preuve. Elle ne remplace pas les méthodes existantes. Elle en change le point d'arrivée : on ne note plus ce que l'organisme déclare, on constate ce que son système fait.

1. **Partir des sanctions.** La liste des points à contrôler n'est pas théorique. Elle reprend les défauts que les autorités ont effectivement sanctionnés (partie 4), dans l'ordre de leur fréquence.

2. **Commencer par les portes.** On recense tout ce qui est joignable depuis l'extérieur et tous ceux qui s'y connectent, prestataires et partenaires compris. C'est par là que les attaquants sont entrés.

3. **Constater dans le système.** Chaque point se clôt par une preuve datée : la copie d'un réglage, la liste des comptes dispensés de seconde preuve d'identité, le résultat d'un essai. Une réponse orale ou un document de principe ne suffit pas.

4. **Faire trancher par écrit.** Pour chaque écart, la direction choisit : corriger, compenser par une autre mesure, ou accepter le risque. La décision est signée et datée. C'est ce qui a manqué à France Travail, à l'Hôpital privé de la Loire et à The Phone House.

5. **Revenir vérifier.** L'audit n'est clos qu'après une seconde visite, à la date fixée, qui constate que la correction est en place. Chez Flexicar et chez Konecta, le diagnostic était juste ; personne n'est revenu.

Les références existantes

Cette méthode s'appuie sur des outils publics, que l'on peut combiner. Aucun ne suffit seul, parce qu'aucun ne part des sanctions.

référence	ce qu'elle apporte	sa limite pour notre objet
CNIL, Guide de la sécurité des données personnelles (2024)	La liste des précautions attendues, fiche par fiche	Dit ce qu'il faut faire, non comment vérifier que c'est fait
ANSSI, Guide d'hygiène informatique	42 mesures techniques de base	S'adresse aux informaticiens, sans lien avec le RGPD
ANSSI, méthode EBIOS Risk Manager	Une démarche pour identifier les risques et les scénarios d'attaque	Produit une étude de risques ; ne vérifie pas que les mesures décidées sont en place
Norme ISO/IEC 27001	Un cadre d'organisation de la sécurité, qui peut être certifié	Certifie une organisation et ses procédures, sur un périmètre que l'organisme choisit
ANSSI, référentiel des prestataires d'audit de sécurité (PASSI)	La liste des prestataires qualifiés pour mener des tests techniques	Concerne la technique ; l'auditeur ne dit pas ce que l'autorité reprochera
Comité européen de la protection des données, lignes directrices 9/2022 et 01/2021 sur les violations de données	La conduite à tenir après une fuite, avec des cas pratiques	Porte sur la réaction, non sur la prévention

Lorsqu'un logiciel de suivi de la conformité est utilisé, la grille de contrôle peut y être reprise, à condition que chaque question soit assortie d'une pièce justificative datée et d'une échéance de contre-vérification. Un questionnaire que l'on remplit par oui ou par non reconduit le défaut que cette partie décrit.

Ces vérifications excèdent la compétence du seul juriste comme celle du seul technicien. Elles supposent que l'avocat et l'expert en sécurité conduisent l'audit ensemble : le premier sait ce que l'autorité reprochera, le second sait le constater dans le système.

partie 9

Ce que le droit actuel laisse sans réponse

Les règles actuelles permettent de sanctionner. Elles préviennent moins bien, et elles ne réparent presque rien. Les décisions font apparaître plusieurs points sur lesquels la loi, française ou européenne, pourrait évoluer.

9.1 Le coût d'une fuite ne pèse pas sur celui qui pouvait l'éviter

C'est le constat le plus net de cette étude. L'organisme qui laisse fuir des données en supporte une faible part du coût. Les personnes dont les données ont fui en supportent l'essentiel, et ne reçoivent rien.

L'amende, rapportée aux personnes touchées, se compte en centimes.

affaire	amende	personnes ou contrats touchés	amende par personne
France Travail	5 M€	36,8 millions	0,14 €
Sprinter (Espagne)	1,56 M€	6,38 millions	0,24 €
The Phone House (Espagne)	6,5 M€	13 millions	0,50 €
Hôpital privé de la Loire	500 000 €	plus de 700 000	0,70 €
Free et Free Mobile	42 M€	24,6 millions de contrats	1,70 €

Rapportée au chiffre d'affaires, elle reste inférieure à un pour cent.

affaire	amende	chiffre d'affaires de référence	proportion
Free et Free Mobile	42 M€	Groupe Iliad, 10,02 milliards d'euros en 2024	0,4 %
Hôpital privé de la Loire	500 000 €	Plus de 90 millions d'euros pour l'établissement, déficitaire	environ 0,5 %
Meta (deux décisions du 12 décembre 2024)	251 M€	164,5 milliards de dollars en 2024	moins de 0,2 %

Sources : résultats annuels 2024 d'Iliad et de Meta ; pour l'hôpital, chiffre repris de la délibération d'après L. Maisnier-Boché, préc. Le plafond légal est de 2 % ou 4 % du chiffre d'affaires mondial.

L'amende n'indemnise personne. Elle est versée au budget de l'État. L'autorité de protection des données n'a pas le pouvoir d'accorder des dommages et intérêts, ce que la CNIL rappelle elle-même.

La réparation devant le juge existe en droit et presque pas en fait. L'article 82 du RGPD ouvre un droit à réparation. La Cour de justice en a fixé la portée dans une série d'arrêts.

arrêt	ce que la cour a jugé	conséquence pour la victime d'une fuite
4 mai 2023, C-300/21	Trois conditions cumulatives : une violation du règlement, un dommage et un lien de causalité. Aucun seuil de gravité n'est exigé. Les critères d'évaluation relèvent de chaque État.	Un préjudice modeste est indemnisable, mais il faut le démontrer.

arrêt	ce que la cour a jugé	conséquence pour la victime d'une fuite
14 décembre 2023, C-340/21	La crainte d'un usage abusif des données peut constituer un dommage moral.	L'inquiétude est indemnisable sans fraude avérée.
21 décembre 2023, C-667/21	La réparation a une fonction compensatoire, et non dissuasive ou répressive. La faute de l'organisme est présumée, mais son degré est sans incidence sur le montant.	Les dommages et intérêts punitifs sont exclus.
20 juin 2024, C-182/22 et C-189/22	Un montant minime est admis si le dommage est peu grave. Le vol de données n'est pas, à lui seul, une usurpation d'identité.	L'indemnité peut être très faible.

La pratique confirme cette portée limitée. En Allemagne, la Cour fédérale de justice a jugé le 18 novembre 2024 (VI ZR 10/24) que la seule perte de contrôle sur ses données constitue un dommage, et a indiqué qu'une somme de l'ordre de 100 euros était appropriée dans l'affaire Facebook. En France, les décisions sont rares et individuelles. Le tribunal judiciaire de Nice a condamné une agence immobilière à verser 8 899,95 euros de dommages et intérêts à un locataire qui avait payé ses loyers à un fraudeur après le piratage de la messagerie de l'agence ; le tribunal y fait peser sur l'agence la charge de prouver que ses mesures de sécurité étaient appropriées (3e ch. civ., 18 novembre 2025, RG 22/03193). Le tribunal judiciaire de Paris a condamné Free à verser à un abonné 1 000 euros pour une panne de connexion de plusieurs mois, mais a rejeté la demande que celui-ci fondait sur la fuite de 2024, faute de pouvoir rattacher à cette fuite les sollicitations dont il se plaignait (12 juin 2025, RG 25/00731). Aucune indemnisation collective de victimes d'une fuite de données n'a été identifiée en France.

L'action de groupe n'a pas comblé ce vide. Trente-cinq actions de groupe seulement avaient été engagées en France, tous domaines confondus, entre 2014 et 2020, et la plupart ont échoué (Assemblée nationale, rapport d'information n° 3085, 11 juin 2020). L'action engagée contre Google en matière de données personnelles a été déclarée irrecevable (TJ Paris, 18 décembre 2024, RG 19/08151). La loi du 30 avril 2025 a unifié le régime et introduit une sanction civile en cas de faute lucrative, mais elle conserve le principe de l'adhésion volontaire de chaque victime.

La comparaison avec les États-Unis. Elle est souvent invoquée. Elle mérite d'être faite sans complaisance, car le modèle américain a ses propres limites.

affaire	ce qui s'est passé	somme mise à la charge de l'entreprise	par personne touchée
Equifax (fuite de 2017)	Données de 147 millions de personnes copiées, par un défaut logiciel non corrigé	425 millions de dollars pour les consommateurs, et 1 milliard de dollars d'investissements de sécurité imposés	environ 2,90 $
T-Mobile (fuite de 2021)	Données de 76,6 millions de personnes copiées chez un opérateur de téléphonie	350 millions de dollars, frais d'avocats et de gestion compris, et 150 millions de dollars d'investissements de sécurité	environ 4,60 $

Il s'agit de transactions conclues dans le cadre d'actions collectives et homologuées par un juge, non de condamnations. Montant par personne : fonds divisé par le nombre de personnes touchées, avant déduction des frais.

critère	états-unis	union européenne
Qui paie, et à qui	L'entreprise verse un fonds destiné aux personnes touchées	L'entreprise verse une amende à l'État
Ordre de grandeur	Plusieurs centaines de millions de dollars dans les plus grandes affaires	42 M€ pour Free, 5 M€ pour France Travail

critère	états-unis	union européenne
Ce que reçoit chaque personne	Quelques dollars en moyenne, davantage pour celles qui justifient d'une perte	Rien, sauf action individuelle
Preuve du préjudice	En Californie, la loi fixe une indemnité de 100 à 750 dollars par personne et par incident, sans preuve d'un préjudice, lorsque la fuite résulte d'un défaut de sécurité raisonnable	La victime doit prouver son dommage et le lien avec la fuite
Action collective	Dans les actions en dommages et intérêts, les personnes touchées sont incluses d'office, sauf à s'en retirer	En France, chaque victime doit adhérer
Contrôle public	Pas de loi fédérale générale équivalente au RGPD ; la protection varie d'un État à l'autre	Une règle commune et une autorité dans chaque pays, avec pouvoir d'enquête et de sanction

Le système américain n'est pas un modèle à importer. Chaque personne y reçoit peu : la somme versée par T-Mobile couvre aussi les honoraires des avocats et les frais de gestion. Les États-Unis n'ont pas de loi fédérale générale sur la protection des données, et les règles varient d'un État à l'autre. La comparaison met en revanche en évidence ce qui manque en Europe. En Californie, la fuite due à un défaut de sécurité a un prix fixé d'avance par la loi, dû aux personnes sans qu'elles aient à prouver un préjudice. En Europe, la règle de sécurité est commune et contrôlée par une autorité dans chaque pays, mais sa méconnaissance coûte peu et ne profite pas aux personnes lésées. Un mécanisme européen pourrait associer les deux : la règle commune et l'autorité de contrôle d'un côté, une indemnité forfaitaire due aux personnes de l'autre.

La conséquence est économique. Lorsqu'une précaution coûte à l'organisme et que son absence coûte surtout à des tiers, l'organisme investit moins qu'il ne faudrait. L'étude de la CNIL de juin 2025 situe ce sous-investissement entre 20 % et 66 %. Tant que le coût d'une fuite restera à la charge de ceux qui la subissent, la sanction administrative ne suffira pas à modifier ce calcul.

Les pistes en débat. Deux questions écrites ont été posées au Gouvernement à l'Assemblée nationale en 2026 (n° 14767, publiée le 28 avril ; n° 16032, publiée le 16 juin). Elles envisagent une indemnisation forfaitaire et automatique des personnes concernées, versée par l'organisme défaillant sans que la victime ait à prouver un préjudice financier. D'autres voies sont concevables, qui laissent toutes la charge à l'organisme défaillant : une présomption de lien entre la fuite et la fraude subie dans les mois qui suivent, ou l'ouverture d'une action collective sans adhésion préalable. Appliquée aux affaires du corpus, une indemnité de 100 euros par personne représenterait 3,7 milliards d'euros pour France Travail et près de 2,5 milliards pour Free. L'ordre de grandeur dit à lui seul pourquoi la question est politique.

Derrière chaque ligne d'un fichier, il y a une personne. Celle dont l'adresse, le numéro de compte ou le dossier médical circule est ensuite sollicitée, trompée, parfois menacée, pendant des années. Le droit actuel traite la fuite comme un manquement administratif. Il gagnerait à la traiter aussi comme un dommage causé à des personnes.

9.2 Le plafond de l'amende

Le défaut de sécurité relève du palier bas de l'article 83, et le résultat dépend du fondement choisi par chaque autorité (voir 6.4). La hiérarchie arrêtée en 2016 correspond-elle encore à la gravité des fuites touchant plusieurs dizaines de millions de personnes ?

9.3 Un socle minimal opposable

L'authentification multifacteur sur les accès externes aux grandes bases n'est exigée que par des recommandations. Les autorités en sanctionnent pourtant l'absence comme celle d'une obligation. L'inscription d'un socle de mesures dans un texte donnerait aux organismes une règle lisible et aux directions un argument budgétaire. La directive NIS 2 le fait pour les entités qu'elle vise ; le RGPD ne le fait pour personne.

9.4 La chaîne de sous-traitance

Un prestataire concentre les données de nombreux clients sans que les personnes concernées le connaissent. La question se pose de soumettre les sous-traitants traitant les données de plusieurs millions de personnes à des obligations renforcées de contrôle et de transparence, et d'articuler ce régime avec celui de la directive NIS 2.

9.5 Le retour d'expérience

Les décisions publiées sont expurgées de leurs éléments techniques, pour des raisons de sécurité compréhensibles. La doctrine observe qu'il devient impossible de comprendre exactement ce qui est reproché (A. Latil, préc.). Une publication périodique et anonymisée des modes opératoires constatés, sur le modèle des rapports d'enquête après accident dans le transport aérien, permettrait aux autres organismes de se corriger.

9.6 Le délai d'information du public

Le RGPD impose d'informer les personnes « dans les meilleurs délais » en cas de risque élevé, sans fixer de terme. Lorsque la fuite survient chez un sous-traitant, cette information dépend de chacun de ses clients. Environ deux mois se sont écoulés entre l'attaque de Maileva et son annonce publique.

lexique

Les termes employés

Analyse d'impact (AIPD)
Analyse, menée avant un traitement susceptible d'engendrer un risque élevé pour les personnes, de l'impact de ce traitement sur la protection de leurs données.

ANSSI
Agence nationale de la sécurité des systèmes d'information, agence française de cybersécurité.

Authentification multifacteur
Authentification qui combine au moins deux facteurs de catégories distinctes : ce que l'on sait, ce que l'on possède, ce que l'on est.

Bourrage d'identifiants
Attaque par saisie d'identifiants volés lors de fuites précédentes.

Chiffrement
Transformation cryptographique des données, qui les rend illisibles sans la clé.

Cloisonnement
Séparation du réseau en zones étanches, pour limiter la propagation d'une intrusion.

CNIL
Commission nationale de l'informatique et des libertés, autorité française de protection des données.

Correctif
Mise à jour de sécurité publiée par un éditeur ; l'ANSSI recommande de l'appliquer dans le mois qui suit sa publication.

Exfiltration
Vol ou transfert non autorisé de données depuis un terminal ou un réseau.

Habilitation
Droit d'accès accordé à un utilisateur sur des données ou des fonctions.

Hachage
Fonction cryptographique qui transforme une chaîne de caractères en une empreinte de taille fixe ; elle sert à conserver les mots de passe sans les garder lisibles.

Hameçonnage
Vol d'identités ou d'informations confidentielles, comme des codes d'accès ou des coordonnées bancaires, par subterfuge.

Journalisation
Enregistrement automatique des opérations réalisées sur un système.

NIS 2
Directive européenne de 2022 imposant des mesures de cybersécurité aux entités de secteurs essentiels.

Rançongiciel
Programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon ; l'attaque bloque l'accès aux données, les chiffre ou les copie.

Responsable de traitement
Organisme qui, seul ou avec d'autres, détermine les finalités et les moyens du traitement.

RGPD
Règlement général sur la protection des données, applicable dans l'Union européenne depuis le 25 mai 2018.

Sous-traitant
Organisme qui traite des données personnelles pour le compte du responsable du traitement.

Violation de données
Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles.

VPN
Tunnel chiffré par lequel un poste situé à l'extérieur se connecte au réseau de l'organisme.

Vulnérabilité
Défaut d'un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal ou à la confidentialité des données.

Définitions établies d'après le RGPD (articles 4 et 35), le CyberDico de l'ANSSI (édition 2024), le guide d'hygiène informatique de l'ANSSI, le guide de la sécurité des données personnelles de la CNIL (version 2024) et la fiche « rançongiciels » de Cybermalveillance.gouv.fr.

méthode

Méthode, limites et sources

Constitution du corpus

Les décisions ont été recherchées sur les sites des autorités nationales et dans la base publique GDPR Enforcement Tracker, puis retenues lorsqu'elles répondaient aux trois conditions énoncées en partie 2. Les textes officiels ont été téléchargés lorsqu'ils étaient accessibles.

Vérifications effectuées sur les textes

Les articles 4, 5, 24, 25, 28, 32 à 35, 82, 83 et 99 du RGPD ont été relus sur le texte publié par la CNIL. Les arrêts C-300/21, C-340/21 et C-807/21 ont été vérifiés sur les communiqués de la Cour, l'arrêt C-383/23 sur son texte, l'arrêt C-667/21 sur son dispositif publié au Journal officiel. Les jugements des tribunaux judiciaires de Paris et de Nice ont été lus dans leur texte intégral. Les arrêts C-687/21 et C-182/22 sont cités d'après la doctrine et, pour le premier, d'après la décision de la CNIL qui le vise.

Les décisions du corpus ont été confrontées une à une, en novembre 2026, à la pièce officielle conservée : dispositif, montant, articles visés, faits et griefs. Les plus longues ont été lues par leurs parties utiles (exposé des faits, motifs de la sanction, dispositif) et non de la première à la dernière page. Celles qui sont rédigées en espagnol, en italien, en polonais, en grec, en finnois, en hongrois, en néerlandais ou dans une langue scandinave ont été lues dans leur langue, sans traduction officielle. Cette relecture a conduit à corriger plusieurs montants et plusieurs faits, et à écarter cinq décisions.

Limites

- **Exhaustivité.** Le corpus ne prétend pas recenser toutes les décisions. Plusieurs autorités ne publient pas leurs sanctions ou les anonymisent.
- **Lecture.** Sur les 139 décisions, 132 ont été vérifiées sur le texte de la décision, sur le communiqué officiel ou sur le rapport d'activité de l'autorité. Sept ne sont connues que par des sources secondaires, la pièce officielle étant inaccessible : les trois décisions bulgares, les deux décisions chypriotes, la décision lituanienne InMedica et la décision de la CNIL du 27 janvier 2021, dont le communiqué n'est plus en ligne.
- **Comptages.** Les fréquences des parties 3 et 4 proviennent d'une recherche de termes. Elles donnent un ordre de grandeur et un minimum.
- **Montants.** Les montants sont ceux du dispositif des décisions. En Espagne, l'organisme qui paie sans contester bénéficie d'une réduction légale de 20 % à 40 % : le montant retenu est celui qui reste dû, soit par exemple 4 M€ au lieu de 5 M€ pour Generali. Hors zone euro, le montant est converti selon l'équivalence donnée par la décision elle-même, à défaut au cours légal polonais (cours moyen de la banque nationale au 28 janvier) ou au cours de référence de la Banque centrale européenne au jour de la décision. Au Danemark, l'autorité propose l'amende et le juge la fixe : les deux montants proposés (800 000 et 500 000 couronnes) ne sont pas comptés dans le total. Les montants des sept décisions connues par des sources secondaires proviennent de la base Enforcement Tracker.
- **Cas discutés.** Cinq décisions sont à la limite du périmètre et ont été maintenues : les décisions Meta fondées sur l'article 25 ou sur la seule notification, la décision ASL Roma 3 (article 33), la décision

Permanent TSB, où les fraudeurs ont trompé le centre d'appels sans intrusion informatique, et celle visant le Bureau croate des assurances, où l'auteur de la sortie des données n'est pas identifié.

- **Décisions écartées.** Cinq décisions d'abord recensées ont été écartées à la relecture. Deux ne procèdent pas d'une attaque : Sambla (Finlande), sanctionnée pour des failles constatées par l'autorité sans intrusion établie, et Continental Automotive (Roumanie), pour un fichier diffusé en interne. La décision italienne visant NTT Data a été retirée du site de l'autorité à la suite d'un jugement du tribunal de Milan du 1er juillet 2025. Une décision allemande n'a pu être consultée, et une décision espagnole figurait en double. Les décisions publiées en novembre 2026 ont été examinées jusqu'au 25 novembre, sur les publications de la CNIL, les actualités nationales relayées par le Comité européen de la protection des données et la presse spécialisée. Trois séries n'ont pas été retenues. La délibération SAN-2026-016 de la CNIL du 12 novembre 2026 (5 M€, société non nommée) sanctionne la conservation de mots de passe en clair à la suite d'un signalement, et le communiqué de l'autorité ne fait état d'aucune attaque. Les dix sanctions simplifiées annoncées par la CNIL le 9 novembre 2026 contre des collectivités et un établissement public ne sont pas nominatives ; l'autorité indique que certaines avaient subi des violations de données, sans autre précision. Les décisions du Garante italien n° 764 et n° 754 du 7 octobre 2026 (centre de radiologie de Matera et son prestataire, 28 000 € au total) portent sur une faille signalée à l'autorité, sans intrusion établie.
- **Versions publiques.** Plusieurs décisions, espagnoles et françaises notamment, sont occultées sur les points techniques.
- **Référentiels.** La confrontation utilise le guide de la CNIL dans sa version 2024 ; les faits de certaines décisions sont antérieurs.
- **Actualité.** Les faits relatifs à Maileva, à l'Institut national du cancer et à la Direction générale de l'aviation civile sont ceux rendus publics au 25 novembre 2026. Aucune autorité ne s'est prononcée sur ces affaires.

Sources

- Groupe La Poste, « Cyberattaque de Maileva, ce qu'il faut savoir », 15 novembre 2026, lapostegroupe.com
- franceinfo, « Victime d'une cyberattaque, Maileva annonce un vol de données touchant 22 millions de personnes », 14 novembre 2026
- Ouest-France, « Les données de milliers d'usagers de l'aviation civile potentiellement exposées lors d'une fuite », 24 novembre 2026 ; Institut national du cancer, annonce publique du 23 novembre 2026
- CNIL, délibération SAN-2026-016 du 12 novembre 2026 et communiqué du 18 novembre 2026 ; CNIL, annonce du 9 novembre 2026 sur dix sanctions simplifiées visant des collectivités ; Garante per la protezione dei dati personali, décisions n° 764 et n° 754 du 7 octobre 2026
- Comité européen de la protection des données, projet de lignes directrices 04/2026, consultation publique du 21 septembre au 13 novembre 2026, edpb.europa.eu
- CJUE, 4 mai 2023, C-300/21 ; 14 décembre 2023, C-340/21, communiqué de presse n° 191/23 ; 21 décembre 2023, C-667/21 ; 25 janvier 2024, C-687/21 ; 20 juin 2024, C-182/22 et C-189/22 ; 5 décembre 2023, C-807/21 ; 13 février 2025, C-383/23
- Bundesgerichtshof, 18 novembre 2024, VI ZR 10/24
- TJ Nice, 18 novembre 2025, RG 22/03193 ; TJ Paris, 12 juin 2025, RG 25/00731 ; TJ Paris, 18 décembre 2024, RG 19/08151
- Assemblée nationale, questions écrites n° 14767 (JO 28 avril 2026) et n° 16032 (JO 16 juin 2026) ; rapport d'information n° 3085 du 11 juin 2020 sur les actions de groupe
- Loi n° 2025-391 du 30 avril 2025, article 16

- États-Unis : transaction Equifax (Cohen Milstein ; EPIC, 4 juin 2021) ; transaction T-Mobile (The Record, 2022 ; CSO Online) ; California Civil Code, § 1798.150 (JD Supra ; Morgan Lewis) ; Federal Rules of Civil Procedure, Rule 23(b)(3) (Congressional Research Service, IF12763) ; Future of Privacy Forum, 2026, sur l'absence de loi fédérale générale
- Garante per la protezione dei dati personali, provvedimento n. 572 du 4 juillet 2024 (doc. web 10063782) et newsletter n° 528 du 22 octobre 2024, sur Postel
- Directive (UE) 2022/2555, article 21, paragraphe 2, points d) et j)
- CNIL, « Violations de données personnelles : dans quels cas peut-on être indemnisé ? », 2 octobre 2026
- CNIL, délibérations SAN-2021-001, SAN-2022-009, SAN-2026-001, SAN-2026-002, SAN-2026-003, SAN-2026-009
- CNIL, Guide de la sécurité des données personnelles, version 2024
- CNIL, « Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ? », 28 janvier 2025
- CNIL, « Cybersécurité. Le RGPD : la meilleure prévention contre les risques cyber », édition 2026
- CNIL, « Économie de la cybersécurité et bénéfices du RGPD », juin 2025
- ANSSI, Guide d'hygiène informatique ; Panorama de la cybermenace 2025
- Cybermalveillance.gouv.fr, rapport d'activité 2025, communiqué de mars 2026
- Le Monde, « Données personnelles, la grande fuite », 22 mai 2026 ; Public Sénat ; AFP, sur le profil des personnes mises en cause
- Comité européen de la protection des données, programme Support Pool of Experts, « One-Stop-Shop case digest on Security of Processing and Data Breach Notification », E. Kosta, novembre 2023
- G. Goldberg, N. Bekhat, O. Maurice et N. McEvoy, « Actualité Informatique et libertés », AJDA 2026, p. 458
- A. Latil, « Lourdes sanctions prononcées en matière de manquement aux obligations de sécurité issues de l'article 32 du RGPD », Comm. com. électr. 2026, comm. 38
- L. Maisnier-Boché, « La CNIL durcit le ton sur l'authentification forte et impose sa vision des habilitations d'accès », Comm. com. électr. 2026, comm. 101
- Décisions des autorités nationales citées en annexe ; GDPR Enforcement Tracker, enforcementtracker.com

annexe

Liste des décisions du corpus

Classement par pays puis par date. Pour chaque décision : ce qui s'est passé, puis ce que l'autorité a reproché, d'après le texte ou le communiqué officiel. Montants en euros.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Knuddels Allemagne, LfDI Bade-Wurtemberg, 21/11/2018 20 000 €	Piratage de juillet 2018 ; mots de passe et adresses électroniques d'environ 330 000 utilisateurs révélés.	Mots de passe des utilisateurs conservés en clair (art. 32-1-a), selon le communiqué.
Boutique en ligne obsolète Allemagne, LfD Basse-Saxe, 2020 65 000 €	Violation notifiée par l'entreprise ; l'examen technique du site révèle un logiciel de boutique en ligne obsolète ; base de données téléchargée.	Logiciel de boutique en ligne xt:Commerce dans une version que l'éditeur ne maintenait plus depuis 2014 au plus tard, avec des failles permettant l'injection SQL ; mots de passe protégés par un procédé inadapté (MD5 sans sel).
Hôpital anonymisé Belgique, APD, 17/12/2024 166-2024 200 000 €	Rançongiciel de 2021, le second subi par l'hôpital en deux ans et demi ; jusqu'à 300 000 personnes concernées.	Pas d'analyse d'impact ; aucun audit régulier de la sécurité ; mot de passe faible pour l'accès au dossier patient ; politique de sécurité inadéquate (art. 32). Amende de base de 390 000 € réduite d'environ un tiers.
Agence nationale des recettes NAP Bulgarie, CPDP, 28/08/2019 2 600 000 €	Piratage de l'administration fiscale ; données d'environ 6 millions de personnes rendues accessibles.	Non détaillé dans les sources consultées.
DSK Bank Bulgarie, CPDP, 28/08/2019 511 000 €	Accès de tiers à plus de 23 000 dossiers de crédit concernant plus de 33 000 clients.	Non détaillé dans les sources consultées.
Postes bulgares Bulgarie, CPDP, 04/05/2022 500 000 €	Piratage : les attaquants ont accédé aux bases de données de l'opérateur postal.	Non détaillé dans les sources consultées.
Hermes Airports, ministère de la Défense, DW Dynamic Works Chypre, Commissaire, 2022 6 000 €	Cyberattaques contre l'aéroport et le ministère de la Défense, passant par leur sous-traitant commun.	Non détaillé dans les sources consultées.
Open University of Cyprus Chypre, Commissaire, 22/11/2023 45 000 €	Pirates publiant sur le dark web les données d'étudiants et d'anciens étudiants.	Non détaillé dans les sources consultées.
Prestataire informatique Croatie, AZOP, 05/07/2021 montant non publié	Intrusion de pirates chez un prestataire informatique sous-traitant d'un opérateur télécom ; 28 085 personnes concernées.	Sous-traitant sanctionné : mesures insuffisantes au regard des risques prévisibles, aucun test régulier (art. 32-1-b et d, 32-2), selon le communiqué.
Opérateur télécom Croatie, AZOP, 21/07/2022 285 900 € 2 150 000 HRK, convertis au cours de la BCE du 21 juillet 2022 (7,52)	Attaquants ayant accédé aux données d'environ 100 000 clients ; systèmes sans restriction d'accès.	Mesures de sécurité insuffisantes au regard des risques prévisibles (art. 25-1, 32-1-b et d, 32-2), selon le communiqué.
Hôpital Croatie, AZOP, 24/03/2025 20 000 €	Cyberattaque contre le centre hospitalier de Zagreb, révélée par la presse ; au moins 3 Go copiés en sept jours ; entrée probable par ingénierie sociale puis VPN.	Mesures techniques insuffisantes ayant facilité l'accès de l'attaquant.
Bureau croate des assurances Croatie, AZOP, 02/07/2025 101 000 €	Signalement anonyme d'une fuite des données de plus d'un million de propriétaires de véhicules, correspondant à la base du Bureau ; les circonstances de la sortie des données font l'objet d'une enquête de police, l'auteur n'étant pas identifié.	Mesures de protection insuffisantes (art. 32-2 et 32-4) ; durées de conservation non fixées (art. 5-1-e).

organisme et décision	ce qui s'est passé	ce qui a été reproché
Société informatique Croatie, AZOP, 22/07/2025 50 000 €	Cyberattaque subie par la société ; notification puis enquête.	Mesures techniques non mises en place à temps ; une fois entré, l'attaquant a circulé librement dans tout le système.
Kræftens Bekæmpelse Danemark, Datatilsynet, 29/09/2021 amende proposée, fixée par le juge Amende de 800 000 DKK proposée (≈ 107 600 €). Au Danemark, l'autorité saisit la police et propose un montant ; l'amende est fixée par le juge. Issue judiciaire non recherchée.	Quatre violations notifiées, dont deux hameçonnages et deux vols d'ordinateurs ; données d'au moins 1 448 personnes, dont des données de santé.	Seconde preuve d'identité jugée nécessaire par l'association elle-même après une attaque d'août 2018, jamais mise en place.
Danish Agro Danemark, Datatilsynet, 26/10/2021 2021-7329-0005 réprimande, sans amende	Hameçonnage d'un salarié le 10 avril 2020 ; pirates dans le réseau du 11 au 19 avril, données chiffrées ; salariés de sept pays concernés.	Mesures techniques et organisationnelles insuffisantes de l'aveu même de l'entreprise (art. 32-1) ; réprimande, compte tenu des mesures prises depuis ; pas de manquement à l'article 34.
SIRIUS advokater Danemark, Datatilsynet, 14/07/2022 amende proposée, fixée par le juge Amende de 500 000 DKK proposée (≈ 67 200 €). Au Danemark, l'autorité saisit la police et propose un montant ; l'amende est fixée par le juge. Issue judiciaire non recherchée.	Pirates ayant accédé en mars 2020 aux serveurs du cabinet d'avocats et les ayant chiffrés ; données de clients et de parties adverses.	Accès à distance mis en place sans mesure de vérification du type seconde preuve d'identité, pour des données de clients et de parties adverses.
Air Europa Espagne, AEPD, 10/03/2021 PS-00179-2020 600 000 €	Premier accès de l'attaquant le 12 mai 2018, découvert en octobre 2018 après des fraudes sur environ 4 000 cartes bancaires ; coordonnées et données bancaires d'environ 489 000 personnes.	Systèmes reliés à internet sans seconde preuve d'identité ; autorité prévenue 41 jours après la découverte. 500 000 € (art. 32) et 100 000 € (art. 33).
Bayard Revistas Espagne, AEPD, 28/09/2022 PS-00246-2022 31 200 € 52 000 € avant réduction de 40 %	Un tiers se présentant comme chercheur en sécurité accède à la base par une vulnérabilité du site et prévient l'éditeur ; environ 465 000 utilisateurs.	Vulnérabilité du site ; données non chiffrées avant l'incident ; notification tardive (art. 5-1-f, 32 et 33).
Holaluz-Clidom Espagne, AEPD, 18/08/2023 PS-00565-2023 675 000 € 400 000 € (art. 5-1-f) et 275 000 € (art. 32)	Les 26 et 27 octobre 2022, tiers connecté avec les identifiants d'un sous-traitant commercial ; téléchargement massif de données clients.	Un seul compte partagé par 120 utilisateurs du sous-traitant commercial ; aucune politique de contrôle d'accès, donc aucune traçabilité des actions.
The Phone House Spain Espagne, AEPD, 27/12/2023 PS-00084-2023 6 500 000 € 4 000 000 € (art. 5-1-f) et 2 500 000 € (art. 32)	Rançongiciel : début estimé au 31 mars 2021, détecté le 11 avril ; données d'environ 13 millions de clients, salariés et fournisseurs exfiltrées et publiées en clair ; deux notifications à l'AEPD.	Données ni chiffrées ni pseudonymisées, alors que ses propres analyses d'impact prévoyaient ces mesures depuis plus de deux ans ; politique de mots de passe. 4 M€ (art. 5.1.f) et 2,5 M€ (art. 32).
I-DE Redes Eléctricas Inteligentes Espagne, AEPD, 05/02/2024 PS-00145-2023 3 500 000 € 2 500 000 € (art. 5-1-f) et 1 000 000 € (art. 32)	Du 7 au 15 mars 2022, extraction d'environ 4,5 millions d'enregistrements par l'application en ligne des raccordements ; 1 350 000 clients de la société ; notification le 18 mars 2022.	Vulnérabilité de l'application ; règles de mots de passe trop faibles ; accès autorisés depuis des adresses suspectes et inutiles à l'activité.
Iberdrola Espagne, AEPD, 07/02/2024 PS-00221-2023 3 000 000 € 2 000 000 € (art. 5-1-f) et 1 000 000 € (art. 32)	Même attaque de mars 2022 : la base, gérée par Iberdrola pour les sociétés du groupe, contenait aussi les données de 1 515 000 clients d'Iberdrola Clientes et de 92 550 clients de Curenergía.	Sanctionnée en qualité de sous-traitant des filiales dont elle gérait la base de données : mesures de sécurité insuffisantes.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Dentalcuadros BCN Espagne, AEPD, 08/05/2024 PS-00078-2024 12 000 € 20 000 € avant réduction de 40 %	Rançongiciel détecté le 20 avril 2023, entré par le service de bureau à distance, protégé par le seul pare-feu intégré de Windows ; données de 2 500 patients chiffrées ; dernière sauvegarde vieille d'un mois.	Bureau à distance exposé sans réseau privé ni restriction d'accès ; notification tardive (art. 32 et 33).
Institut Marquès Espagne, AEPD, 03/09/2024 EXP202204816 montant non publié 80 000 € proposés ; procédure close par paiement volontaire le 18 octobre 2023, montant payé non indiqué	Cyberattaque détectée le 21 décembre 2021 ; données de patients extraites et utilisées pour leur écrire ; environ 400 personnes selon la notification.	Mesures de sécurité inadaptées (art. 5-1-f et 32) et information tardive des personnes (art. 34).
Telefónica de España Espagne, AEPD, 26/09/2024 PS-00291-2023 1 300 000 € 500 000 € et 800 000 € (art. 5-1-f et 32)	Du 9 au 20 septembre 2022, des tiers accèdent, avec l'identifiant d'un salarié, à une application interne du portail des salariés ouverte sur internet ; 1 407 257 clients concernés.	Accès par simple identifiant et mot de passe, sans seconde preuve d'identité ; données non chiffrées, dont les mots de passe wifi des routeurs.
Generali España Espagne, AEPD, 10/12/2024 PS-00453-2023 4 000 000 € 1 M€ (art. 5-1-f), 1 M€ (art. 32), 2 M€ (art. 25) et 1 M€ (art. 35), soit 5 M€ avant réduction de 20 %	Attaque par force brute détectée le 5 octobre 2022 sur le formulaire de consultation des clients, avec les identifiants d'un courtier ; fuite connue le 11 novembre 2022 ; plus d'un million de personnes informées.	Aucun enregistrement des opérations sur l'application visée, d'où l'impossibilité de mesurer l'attaque pendant plus d'un mois ; pas de seconde preuve d'identité pour les courtiers, qui accédaient aussi aux données d'anciens clients ; ni analyse de risques ni analyse d'impact.
Caja Rural de Jaén, Barcelona y Madrid Espagne, AEPD, 16/01/2025 PS-00004-2024 400 000 € 500 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL CENTRAL, S.C.C. Espagne, AEPD, 16/01/2025 72 000 € 90 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
Caja Rural de Salamanca Espagne, AEPD, 17/01/2025 PS-00007-2024 200 000 € 250 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DEL SUR, S.C.C. Espagne, AEPD, 17/01/2025 16 000 € 20 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE EXTREMADURA S.C.C. Espagne, AEPD, 17/01/2025 88 000 € 110 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL NTRA. SRA. DEL ROSARIO Espagne, AEPD, 17/01/2025 8 000 € 10 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE ALBACETE, CIUDAD REAL Y CUENCA, S.C.T Espagne, AEPD, 17/01/2025 80 000 € 100 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).

organisme et décision	ce qui s'est passé	ce qui a été reproché
CAJA RURAL DE GIJÓN, S.C.A.C. Espagne, AEPD, 17/01/2025 76 000 € 95 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE ARAGÓN, S.C.C. Espagne, AEPD, 17/01/2025 PS-00019-2024 12 000 € 15 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL NTRA MADRE DEL SOL S.C.A.C. Espagne, AEPD, 17/01/2025 8 000 € 10 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE ONDA, S.C.C. Espagne, AEPD, 17/01/2025 12 000 € 15 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL GRANADA, S.C.C. Espagne, AEPD, 17/01/2025 12 000 € 15 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE BAENA NTRA. SRA. DE GUADALUPE, S.C.C.A. Espagne, AEPD, 17/01/2025 8 000 € 10 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
CAJA RURAL DE ASTURIAS, S.C.C. Espagne, AEPD, 17/01/2025 12 000 € 15 000 € avant réduction de 20 %	Violation survenue le 10 novembre 2022 chez RSI, prestataire informatique commun des caisses rurales, et détectée le 9 décembre 2022 ; accès aux données de clients par une vulnérabilité des systèmes du prestataire.	Vulnérabilité chez le sous-traitant, corrigée après l'attaque ; la caisse, responsable du traitement, répond des mesures confiées à son prestataire (art. 5-1-f, 32 et 33).
Centros Comerciales Carrefour Espagne, AEPD, 14/03/2025 PS-00128-2024 3 200 000 € 2 000 000 € (art. 5-1-f), 1 000 000 € (art. 32) et 200 000 € (art. 34)	Cinq violations notifiées : accès illégitimes à des comptes clients, très probablement par bourrage d'identifiants issus d'autres fuites.	Seconde preuve d'identité mise en place seulement après les premières attaques ; information insuffisante des personnes.
Real Sociedad de Fútbol Espagne, AEPD, 12/08/2025 PS-00286-2025 66 000 € 110 000 € avant réduction de 40 %	Rançongiciel découvert le 16 octobre 2023 ; données d'environ 60 000 personnes, dont des données biométriques ; entrée probable par l'accès à distance, sans certitude faute de journaux suffisants.	Journaux et télémétrie insuffisants pour reconstituer l'attaque (art. 5-1-f et 32).
SAREB Espagne, AEPD, 04/09/2025 PS-00313-2025 180 000 € 300 000 € avant réduction de 40 %	Rançongiciel de l'été 2023 chez son prestataire informatique ; environ 7 200 personnes touchées selon le prestataire.	Mesures de sécurité insuffisantes ; contrat de sous-traitance non conforme (art. 5-1-f et 28).
Servicios Financieros Carrefour Espagne, AEPD, 17/09/2025 PS-00288-2025 1 500 000 € 2 500 000 € avant réduction de 40 %	Du 17 au 19 décembre 2023, un attaquant interroge en masse un service en ligne avec 19 identifiants de clients compromis, provenant d'une source extérieure ; des clients reçoivent ensuite des courriels d'hameçonnage reprenant leurs données.	Service configuré de façon vulnérable depuis sa mise en place en 2017 et jamais revu depuis (art. 5-1-f).

organisme et décision	ce qui s'est passé	ce qui a été reproché
Sprinter Megacentros del Deporte Espagne, AEPD, 28/11/2025 PS-00373-2025 1 560 000 € 2 600 000 € avant réduction de 40 %	Premier accès illégitime le 24 octobre 2023 ; copie des données du 24 au 27 octobre puis chiffrement par rançongiciel ; 6 381 913 personnes, dont 6 351 300 clients (4 671 960 en Espagne).	Mesures de sécurité insuffisantes, le vecteur d'entrée étant occulté dans la version publiée ; information insuffisante des personnes.
Iberia Espagne, AEPD, 11/03/2026 PS-00437-2024 650 000 € Amende prononcée au titre de l'article 5-1-f ; griefs tirés des articles 32 et 34 classés	En janvier 2023, des données de la compagnie sont copiées depuis le système d'un prestataire, par deux vulnérabilités connues depuis 2017 et 2019.	Vulnérabilités corrigées de longue date par l'éditeur, non corrigées chez le prestataire ; aucun mécanisme pour vérifier la sécurité de celui-ci.
Alía Gestión Integral de Servicios Espagne, AEPD, 20/03/2026 PS-00511-2025 150 000 € 250 000 € avant réduction de 40 %	Rançongiciel détecté le 24 avril 2024 ; hypothèse principale : identifiants d'accès à distance et certificat numérique d'un utilisateur compromis ; au moins 77 027 personnes.	Mesures de sécurité insuffisantes (art. 5-1-f), la version publiée en occultant le détail.
Konecta BTO Espagne, AEPD, 22/04/2026 PS-00613-2025 300 000 € 500 000 € avant réduction de 40 %	Du 5 au 7 mai 2024, attaque chez ce prestataire de relation client de deux sociétés ; 808 800 personnes touchées.	Pas de seconde preuve d'identité pour accéder à l'environnement du client, carence relevée par un audit du client en novembre 2022 et non corrigée (art. 5-1-f).
ECG Médica Espagne, AEPD, 15/07/2026 PS-00009-2026 18 000 € 30 000 € avant réduction de 40 %	Du 23 au 25 juillet 2024, un inconnu menace par courriel de publier des données de patients ; 1 352 patients concernés, certaines données ayant été publiées.	Aucun dispositif d'alerte précoce : les premiers mouvements de l'attaquant remontent au 25 juin 2024, un mois avant la découverte (art. 32).
23andMe Espagne, AEPD, 16/07/2026 PS-00140-2025 2 400 000 € 2 000 000 € (art. 5-1-f) et 400 000 € (art. 33)	Bourrage d'identifiants ; 2 642 résidents espagnols ; données génétiques et d'origine ethnique ; échantillon publié sur un forum et fichier mis en vente ; annonce repérée le 1er octobre 2023, notification le 17 octobre.	Seconde preuve d'identité seulement facultative ; aucune exigence de robustesse du mot de passe ; aucune limite d'accès ou de téléchargement par adresse IP ; autorité prévenue tardivement.
Flexicar Internacional Espagne, AEPD, 28/07/2026 PS-00540-2025 680 000 € 400 000 € (art. 5-1-f), 250 000 € (art. 32) et 30 000 € (art. 13)	Cyberattaque notifiée le 3 juin 2024 ; mesures recommandées en 2022 non mises en place.	Mesure recommandée par un examen de cybersécurité de 2022, jamais mise en place ; négligence grave retenue ; information insuffisante des clients.
Hoy Voy a Conducir Espagne, AEPD, 31/07/2026 PS-00035-2026 30 000 € 50 000 € avant réduction de 40 %	Base de plus de 200 000 enregistrements d'élèves et de salariés mise en vente : annonce du 5 mai 2024, repérée par la police le 12 août, connue de l'entreprise le 2 octobre.	Infrastructure obsolète, composants sans support de l'éditeur ; obsolescence connue de l'entreprise depuis avril 2021 (art. 32).
Gestores Administrativos Reunidos (GARSA) Espagne, AEPD, 04/08/2026 PS-00008-2026 75 000 € 125 000 € avant réduction de 40 %	Identifiants de domaine compromis ; accès par les services distants, élévation de privilèges, puis rançongiciel ; environ 85 Go de documents publiés sur le dark web le 28 juin 2024.	Mesures de sécurité insuffisantes et notification tardive (art. 5-1-f et 33) ; l'autorité a dû ordonner l'information des personnes.
Vodafone España (Super Wifi) Espagne, AEPD, 18/08/2026 PS-00240-2025 750 000 € 500 000 € (art. 5-1-f), 150 000 € et 100 000 € (art. 32 et 28)	Attaque à partir du 11 novembre 2023 visant le service Super Wifi, exploité par un prestataire ; notification le 23 novembre.	Carences de sécurité chez le prestataire et défaut de contrôle par l'opérateur ; aucun contrat de sous-traitance valable.
Vodafone España (plateforme clients) Espagne, AEPD, 11/09/2026 PS-00248-2025 500 000 €	Rançongiciel à partir du 1er novembre 2023 chez le prestataire gérant une plateforme de clients ; données chiffrées et indisponibles.	Compte générique sans seconde preuve d'identité chez le prestataire ; aucun audit du prestataire par l'opérateur (art. 32).

organisme et décision	ce qui s'est passé	ce qui a été reproché
Vodafone España (télévente) Espagne, AEPD, 11/09/2026 PS-00253-2025 400 000 € 100 000 € (art. 28) et 300 000 € (art. 32)	Attaque du 5 novembre 2023 chez un sous-traitant de télévente : entrée par le VPN avec un compte sans privilèges, élévation de privilèges, antivirus neutralisé ; 98 509 personnes.	Sous-traitant sans double authentification sur l'ensemble de ses accès VPN ; défaut de contrôle du sous-traitant.
Vodafone España (sous-traitant) Espagne, AEPD, 17/09/2026 PS-00194-2025 400 000 €	Attaque à partir du 27 mai 2023 chez le prestataire gérant les incidents clients ; numéros de téléphone de 486 768 clients particuliers et de 14 571 clients professionnels, non chiffrés.	Aucun audit ni contrôle périodique du sous-traitant, dont les systèmes n'étaient pas à jour.
Allium UPI (Apotheka) Estonie, AKI, 05/09/2025 3 000 000 €	Vol de la base du programme de fidélité ; 750 000 personnes.	Pas d'authentification à plusieurs facteurs ; un même compte administrateur partagé par plusieurs personnes ; suivi des journaux insuffisant ; sauvegardes de la base conservées sans sécurité.
Vastaamo Finlande, Tietosuojavaltuutettu, 07/12/2021 20211183 608 000 €	Base de patients d'un centre de psychothérapie très probablement téléchargée par un port ouvert sur internet entre novembre 2017 et mars 2019 ; connexions établies le 20 décembre 2018 et le 15 mars 2019 ; demande de rançon ; notification en septembre 2020.	Base de patients accessible depuis internet sans protection suffisante ; violation de mars 2019 ni notifiée à l'autorité ni annoncée aux patients avant l'automne 2020.
S-Bank Finlande, Tietosuojavaltuutettu, 08/09/2025 TSV/3606/2024 1 800 000 €	Faille introduite en avril 2022 dans le service d'identification de la banque ; paiements non autorisés au préjudice de clients ; violation notifiée le 5 août 2022.	Fonctionnalité insuffisamment testée avant mise en service ; réclamations de clients non instruites (art. 5-1-f, 25 et 32).
Opticien anonymisé France, CNIL, 06/01/2021 SAN-2021-001 250 000 €	Intrusions sur le site de vente en ligne par un module de dépôt de fichiers vulnérable ; données de 210 692 clients compromises ; notification puis contrôle.	Politique de mots de passe insuffisante sur les comptes clients ; exercice des droits non facilité (art. 12).
Bourrage d identifiants (responsable et sous-traitant anonymisés) France, CNIL, 27/01/2021 150 000 €	Vagues de bourrage d'identifiants sur un site marchand entre juin 2018 et janvier 2020 ; notifications répétées puis contrôle.	Décision non publiée ; le communiqué de la CNIL n'est plus en ligne.
Dedalus Biologie France, CNIL, 15/04/2022 SAN-2022-009 1 500 000 €	Fichier de données médico-administratives de 491 840 patients de laboratoires diffusé sur internet ; révélé par la presse ; contrôle en ligne et sur place.	Extraction de données au-delà des instructions des laboratoires (art. 29) ; contrats sans les mentions obligatoires (art. 28) ; données non chiffrées sur un serveur dont une partie était accessible sans authentification, comptes partagés, aucune supervision (art. 32).
Free Mobile France, CNIL, 08/01/2026 SAN-2026-001 27 000 000 €	Du 28 septembre au 22 octobre 2024, intrusion par l'accès à distance de l'entreprise ; l'attaquant prévient lui-même l'opérateur le 21 octobre ; 19 460 891 contrats mobiles concernés, dont des IBAN ; 2 614 plaintes.	VPN sans authentification multifacteur ni authentification des postes ; détection des comportements anormaux inefficace ; information incomplète des personnes (art. 34) ; conservation excessive de données d'anciens abonnés (art. 5-1-e).
Free France, CNIL, 08/01/2026 SAN-2026-002 15 000 000 €	Même intrusion ; 5 172 577 contrats fixes concernés.	VPN sans authentification multifacteur ; détection des comportements anormaux inefficace ; information incomplète des personnes (art. 34).
France Travail France, CNIL, 22/01/2026 SAN-2026-003 5 000 000 €	Ingénierie sociale visant des comptes de conseillers Cap emploi, du 6 février au 5 mars 2024 ; données de plus de 36,8 millions de personnes ; alerte interne le 4 mars, notification à la CNIL le 8 mars 2024.	Mots de passe des conseillers insuffisamment robustes ; pas de seconde preuve d'identité, pourtant prévue par ses propres analyses dès 2023 ; extractions massives non détectées ; conseillers habilités à consulter des personnes qu'ils n'accompagnaient pas.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Hôpital privé de la Loire France, CNIL, 21/07/2026 SAN-2026-009 500 000 €	Attaquant muni des identifiants d'un médecin libéral ; extraction de 524 867 fiches de patients du 26 juin au 1er juillet 2025, révélée par le signalement d'un praticien.	Pas d'authentification multifacteur pour les utilisateurs externes du dossier patient, alors que le logiciel la proposait ; requêtes massives non détectées pendant près d'une semaine ; personnes de confiance non informées (art. 34).
Cosmote et OTE Grèce, HDPA, 27/01/2022 4-2022 9 250 000 € Cosmote : 6 000 000 € ; OTE : 3 250 000 € (art. 32)	Pirate entré avec le mot de passe d'un salarié, issu d'une ancienne fuite de LinkedIn ; requêtes sur le système de données massives de l'opérateur ; données de trafic de 4 792 869 abonnés extraites.	Cosmote : conservation et traitement illicites de données de trafic, analyse d'impact insuffisante, information incomplète des abonnés, anonymisation mal appliquée, sécurité défaillante, rôles mal répartis avec OTE. OTE : mesures de sécurité insuffisantes (art. 32).
ELTA (poste grecque) Grèce, HDPA, 28/02/2024 10/2024 2 995 140 €	Rançongiciel du 20 mars 2022 : accès distant non autorisé aux postes de travail, mots de passe des comptes d'administration du domaine obtenus, fichiers chiffrés puis publiés sur le dark web le 4 mai 2022.	Politique de sécurité non appliquée (art. 5-1-f et 32).
EETAA et ministère de la Cohésion sociale Grèce, HDPA, 28/07/2026 15-2026 350 000 € Ministère : 150 000 € et 50 000 € ; société EETAA : 100 000 € et 50 000 €	Rançongiciel en deux temps du 1er au 5 mars 2025 sur le système du programme de bons de garde d'enfants ; base chiffrée.	Système d'information obsolète maintenu en service malgré une vulnérabilité connue (art. 5-1-f et 32) ; absence de contrat de sous-traitance conforme entre le ministère et la société (art. 28).
Digi Hongrie, NAIH, 22/06/2023 216 500 € 80 000 000 HUF, convertis au cours de la BCE du 22 juin 2023 (369,43). Décision reprise après l'annulation par le juge de la décision de 2020, qui infligeait 100 millions de forints	Pirate ayant exploité, par le site de l'opérateur, une vulnérabilité connue depuis plus de neuf ans ; données d'environ 322 000 personnes, conservées dans une base de test qui n'avait pas été supprimée ; violation connue le 23 septembre 2019.	Vulnérabilité ancienne, détectable et corrigible, jamais corrigée ; base de test conservée sans nécessité ; données non chiffrées.
University College Dublin Irlande, DPC, 17/12/2020 70 000 €	Sept violations : accès de tiers à des messageries de l'université, identifiants publiés en ligne.	Messagerie insuffisamment sécurisée (art. 5-1-f et 32-1) ; conservation excessive de données dans une boîte ; une violation notifiée avec 13 jours de retard (résumé officiel).
Teaching Council Irlande, DPC, 02/12/2021 IN-20-04-01 60 000 € 40 000 € (art. 5 et 32) et 20 000 € (art. 33)	Hameçonnage de deux agents ; redirection automatique de 323 courriels vers une adresse malveillante (17 février au 6 mars 2020) ; 9 735 personnes.	Fichiers de données ni chiffrés ni protégés par mot de passe ; messagerie permettant le transfert automatique vers l'extérieur ; aucune évaluation régulière des mesures ; notification tardive.
Meta - scraping Irlande, DPC, 25/11/2022 265 000 000 €	Fichier de données d'environ 533 millions d'utilisateurs Facebook mis en ligne sur une plateforme de pirates ; enquête ouverte en 2021 après la presse.	Protection des données dès la conception et par défaut insuffisante sur les outils de recherche et d'import de contacts (art. 25-1 et 25-2) ; pas de grief au titre de l'article 32.
VIEC Irlande, DPC, 12/12/2022 IN-21-2-5 100 000 €	Hameçonnage d'un cadre d'un exploitant de maisons de retraite : identifiants saisis sur un faux site ; courriels contenant des mots liés aux paiements transférés automatiquement à un tiers pendant plus de trois mois.	Messagerie sans mesures de sécurité adaptées ; aucune preuve de formation du personnel à l'hameçonnage (art. 5-1-f et 32-1).
Fastway Couriers Irlande, DPC, 30/12/2022 IN-21-6-2 15 000 €	Serveur mal configuré par un prestataire lors d'un projet informatique et exposé sur internet ; un tiers y copie des données de clients ; 446 143 personnes selon la notification.	Aucune analyse de risque avant la modification du système d'information.
Centric Health Irlande, DPC, 23/01/2023 IN-21-2-4 460 000 €	Rançongiciel (famille Phobos) sur le système de gestion des patients ; environ 70 000 patients touchés, 2 500 dossiers perdus ; notification en décembre 2019.	Protections par mots de passe insuffisantes ; aucun test régulier des mesures ; aucune trace documentée des correctifs appliqués (art. 5-1-f, 5-2 et 32-1). Total 460 000 €.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Maynooth University Irlande, DPC, 22/11/2024 IN-19-9-3 40 000 € 25 000 € (art. 5-1-f et 32) et 15 000 € (art. 33)	Accès d'un tiers aux messageries de plusieurs salariés, utilisées pour détourner un versement de pension ; fraude détectée le 10 octobre 2018.	Pas de seconde preuve d'identité ; mots de passe sans expiration ; filtrage des courriels insuffisant ; postes sans correctifs de sécurité ; notification tardive.
Meta (jetons d'accès) Irlande, DPC, 12/12/2024 IN-18-10-1 11 000 000 € 8 M€ (art. 33-3) et 3 M€ (art. 33-5)	Du 14 au 28 septembre 2018, exploitation d'une faille de la fonction « Voir en tant que », présente depuis juillet 2017, permettant de voler des jetons d'accès à des comptes ; près de 3 millions de personnes dans l'Union.	Notification incomplète à l'autorité et documentation insuffisante de la violation.
Meta (jetons d'accès) Irlande, DPC, 12/12/2024 IN-18-11-1 240 000 000 € 130 M€ (art. 25-1) et 110 M€ (art. 25-2)	Du 14 au 28 septembre 2018, exploitation d'une faille de la fonction « Voir en tant que », présente depuis juillet 2017, permettant de voler des jetons d'accès à des comptes ; près de 3 millions de personnes dans l'Union.	Service conçu sans analyse des risques ni règle interne sur l'usage des jetons d'accès.
City of Dublin ETB Irlande, DPC, 23/06/2025 IN-19-7-3 125 000 € 50 000 € (art. 5-1-f et 32), 15 000 € (art. 33-1), 10 000 € (art. 34-1) et 50 000 € (art. 34-4)	Logiciel malveillant introduit en janvier 2018 sur un serveur web conservant des demandes de bourses, détecté en octobre 2018 ; environ 13 000 personnes ; notification en novembre 2018.	Mesures de sécurité du serveur insuffisantes ; notification tardive à l'autorité ; information tardive des personnes, malgré l'injonction de l'autorité.
University of Limerick Irlande, DPC, 10/12/2025 IN-19-7-1 98 000 € 45 000 € (art. 5-1-f et 32), 3 000 € (art. 30), 35 000 € (art. 33) et 15 000 € (art. 34)	Hameçonnages répétés ; accès à plusieurs messageries de salariés et détournement de courriels.	Pas d'authentification multifacteur ; pas de formation du personnel à l'hameçonnage ; registre et information des personnes défaillants.
Permanent TSB Irlande, DPC, 08/05/2026 277 500 €	Fraudeurs appelant le service téléphonique de la banque avec des informations sur les clients pour modifier les comptes ; trois violations.	Protocoles de sécurité du centre d'appels non respectés ; notification tardive (art. 5-1-f, 32-1 et 33-1). 250 000 € et 27 500 €.
Midlands Regional Hospital Tullamore Irlande, DPC, 11/06/2026 300 000 €	Rançongiciel détecté le 14 novembre 2018 sur le système d'information du laboratoire ; environ 84 000 personnes.	Mesures de sécurité insuffisantes ; garanties du sous-traitant insuffisantes ; registre des traitements incomplet ; information incomplète des personnes (art. 5-1-f, 28, 30, 32 et 34).
Casa di cura Borghi Italie, Garante, 02/12/2021 9734884 30 000 €	Pirate ayant accédé aux données de patients et publié des images radiologiques sur Twitter ; simples mots de passe.	Pas de chiffrement des données en transit ; aucun contrôle de qualité des mots de passe, compte technique protégé par un mot de passe trivial.
Med Store Saronno Italie, Garante, 02/12/2021 9734934 7 000 €	Même attaque : pirate publiant des données et images de patients sur Twitter.	Pas de chiffrement des données en transit ; compte technique protégé par un mot de passe trivial.
Centro di Medicina preventiva Italie, Garante, 16/12/2021 9739609 10 000 €	Groupe de pirates ayant obtenu et publié sur Twitter une liste de patients et d'examens.	Serveur accessible depuis internet sans aucune procédure d'authentification.
ASL Napoli 3 Sud Italie, Garante, 28/09/2023 9941232 30 000 €	Rançongiciel ; accès frauduleux par l'accès à distance avec des identifiants volés et publiés sur le dark web ; 842 118 patients et salariés.	Accès à distance et postes de travail sans seconde preuve d'identité.
UniCredit Italie, Garante, 08/02/2024 9991020 2 800 000 €	Du 11 au 21 octobre 2018, attaque sur le portail de banque mobile ; l'identité de clients s'affichait même en cas d'échec de connexion ; 731 519 codes clients touchés, le mot de passe étant découvert pour 6 859 d'entre eux.	Deux vulnérabilités du portail : divulgation de données sans PIN, et aucune protection contre les essais illimités d'identifiants (PIN faibles acceptés) ; aucun mécanisme contre les robots.

organisme et décision	ce qui s'est passé	ce qui a été reproché
LAZIOcrea Italie, Garante, 21/03/2024 10002324 271 000 €	Porte dérobée implantée le 25 mars 2021 sur l'ordinateur portable d'un agent en télétravail ; identifiants utilisés le 31 juillet 2021 ; rançongiciel découvert le 1er août au matin, paralysant les services de santé de la région.	Alertes mal traitées ; réseau non cloisonné, le logiciel malveillant ayant gagné environ 180 systèmes ; accès à distance par simple identifiant et mot de passe ; serveur dont le système n'était plus mis à jour.
Regione Lazio Italie, Garante, 21/03/2024 10002287 120 000 €	Rançongiciel de la nuit du 31 juillet au 1er août 2021 sur les systèmes régionaux gérés par LAZIOcrea ; services de santé indisponibles.	Défaut de surveillance de son prestataire LAZIOcrea ; amende de 120 000 € (décision 10002287).
ASL Roma 3 Italie, Garante, 21/03/2024 10002533 10 000 €	Même attaque : services de santé indisponibles.	Violation ni notifiée à l'autorité ni documentée (art. 33) : sanction portant sur la gestion de l'incident.
Innova Camera Italie, Garante, 11/04/2024 10013321 25 000 €	Injection SQL sur un composant du système de gestion de contenu fourni par un prestataire pour le portail de la chambre de commerce ; accès à la base, puis dépôt de portes dérobées.	Vulnérabilité applicative exploitable par injection SQL.
Postel Italie, Garante, 04/07/2024 10063782 900 000 €	Rançongiciel du groupe Medusa en août 2023 ; serveurs bloqués, données exfiltrées ; environ 25 000 personnes.	Correctifs Microsoft Exchange non appliqués malgré les alertes de l'éditeur et de l'agence italienne de cybersécurité ; aucune procédure de vérification régulière des mesures ; information insuffisante de l'autorité (art. 33). Art. 5(1)(f), 25 et 32.
ASL Matera Italie, Garante, 29/04/2026 10251777 8 600 €	Rançongiciel du groupe Rhysida ; comptes d'administration compromis, sauvegardes atteintes, 600 Go copiés ; 95 362 personnes.	Mêmes identifiants pour l'accès à distance et pour le domaine ; politique de mots de passe insuffisante.
Wind Tre Italie, Garante, 14/05/2026 10263796 1 715 600 €	En février 2025, des tiers obtiennent par téléphone la prise en main du poste de vendeurs de deux points de vente, puis interrogent en série la base clients (environ 2 millions de requêtes) ; données de 365 048 clients, dont moyens de paiement pour 41 359.	Pas de tests d'intrusion ni d'évaluations de vulnérabilité visant les interfaces (API) ; contrôles insuffisants sur des API exposées ; gestion non sécurisée des certificats et clés privées ; pas de gestionnaire de mots de passe.
Docplanner Italy Italie, Garante, 18/06/2026 10280177 10 000 €	Rançongiciels chez l'éditeur d'un logiciel hospitalier, sous-traitant ; accès à un disque contenant des données.	Pas d'authentification à plusieurs facteurs pour les comptes du domaine ; accès distant par VPN.
NIER Ingegneria Italie, Garante, 14/07/2026 10292124 120 000 €	Rançongiciel détecté le 9 octobre 2024 ; identifiants de l'entreprise retrouvés dans des bases de fuites, utilisés pour entrer par l'accès à distance ; sauvegardes atteintes, données publiées ; plus de 500 personnes.	Authentification multifacteur non étendue à tous les comptes ni au VPN ; pas de protection contre les essais répétés d'identifiants.
Prime Leasing (CityBee) Lituanie, VDAI, 29/11/2021 110 000 €	Sauvegarde non chiffrée de la base clients, créée en 2018 et restée accessible publiquement jusqu'au 16 février 2021 ; données de 110 302 clients mises en ligne.	Aucun enregistrement ni surveillance des accès ; mots de passe protégés par un procédé faible ; pas d'analyse de risque de la migration ; fonctions de développement et de sécurité non séparées (art. 32-1-a, b et d).
InMedica Lituanie, VDAI, 19/06/2026 3R-1143 450 000 €	Accès de tiers à des dossiers médicaux par un sous-traitant, puis chiffrement de quatre systèmes par un tiers.	Non détaillé dans les sources consultées.
Østre Toten Norvège, Datatilsynet, 07/01/2022 21/00480-14 398 900 € 4 000 000 NOK, convertis au cours de la BCE du 7 janvier 2022 (10,0288)	Rançongiciel découvert le 9 janvier 2021 : systèmes chiffrés, sauvegardes supprimées, environ 30 000 documents touchés, 31,5 Go transférés à l'étranger.	Pas de sécurité efficace à la connexion ; sauvegardes insuffisamment protégées ; journalisation insuffisante, qui a empêché de retracer l'exfiltration.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Stortinget Norvège, Datatilsynet, 04/03/2022 203 300 € 2 000 000 NOK, convertis au cours de la BCE du 4 mars 2022 (9,8358)	Connexions non autorisées, connues en septembre 2020, aux messageries de parlementaires et d'agents ; données exfiltrées.	Pas de double authentification sur les messageries.
Transavia Pays-Bas, AP, 23/09/2021 400 000 €	En 2019, attaque par mots de passe courants sur deux comptes du service informatique ; accès possible aux données de 25 millions de personnes, 83 000 exfiltrées.	Mots de passe faibles ; aucune segmentation du réseau, l'attaquant ayant eu accès à presque tout le domaine ; droits des utilisateurs trop étendus.
Morele.net Pologne, UODO, 10/09/2019 ZSPR.421.2.2019 660 000 € 2 830 410 PLN, soit 660 000 € selon la décision	Accès non autorisé aux données des clients du site marchand, qui en comptait environ 2,2 millions ; des clients reçoivent des SMS frauduleux en novembre 2018.	Contrôles d'accès renforcés seulement en décembre 2018, après l'attaque, alors qu'ils auraient nettement réduit le risque.
Virgin Mobile Polska Pologne, UODO, 03/12/2020 DKN.5112.1.2020 460 000 € 1 968 524 PLN, soit 460 000 € selon la décision	Accès de tiers, par une faille du service d'enregistrement des cartes prépayées, aux données de 114 963 abonnés, dont leur numéro national et leur pièce d'identité.	Aucun test de sécurité des applications visées avant l'incident ; tests menés seulement en cas de soupçon de faille.
ID Finance Poland Pologne, UODO, 17/12/2020 DKN.5130.1354.2020 250 000 € 1 069 850 PLN, soit 250 000 € selon la décision	Redémarrage du serveur par l'hébergeur, qui en réinitialise les protections ; base de 140 699 clients téléchargée puis effacée par un tiers qui réclame une rançon.	Mots de passe des utilisateurs conservés en clair ; mesures techniques insuffisantes (art. 5-1-f, 25 et 32).
Fortum et PIKA Pologne, UODO, 19/01/2022 DKN.5130.2215.2020 1 135 000 € Fortum : 4 911 732 PLN (1 080 000 €) ; PIKA, son sous-traitant : 250 135 PLN (55 000 €), selon la décision	Base clients créée par le sous-traitant lors d'une modification technique, copiée par des tiers ; 120 428 personnes.	Sous-traitant non vérifié avant le contrat ; modification technique menée sans analyse préalable du risque.
Commune (rançongiciel) Pologne, UODO, 16/05/2023 DKN.5131.56.2022 6 400 € 30 000 PLN, convertis au cours légal polonais de 2023 (4,7160)	Rançongiciel exploitant une vulnérabilité du système de la commune ; environ 9 400 personnes ; serveur de sauvegarde en panne, 80 % des données récupérées.	Aucun test régulier de l'efficacité des mesures de sécurité ; sauvegardes défaillantes.
Société (rançongiciel) Pologne, UODO, 31/05/2023 DKN.5131.8.2021 10 000 € 47 160 PLN, soit 10 000 € selon la décision	Rançongiciel ; notification tardive.	Absence de mesures techniques adaptées ; données chiffrées jamais récupérées ; notification tardive.
American Heart of Poland Pologne, UODO, 20/05/2024 DKN.5112.35.2021 330 000 € 1 440 549 PLN, convertis au cours légal polonais de 2024 (4,3653)	Rançongiciel sur les systèmes du groupe hospitalier ; notification puis enquête ; le nombre de personnes est occulté dans la décision.	Analyse de risque incorrecte ; aucun test régulier de l'efficacité des mesures (art. 32-1-d).
Centre de santé de Pajęczno Pologne, UODO, 13/06/2024 DKN.5131.57.2022 9 200 € 40 000 PLN, convertis au cours légal polonais de 2024 (4,3653)	Rançongiciel du 10 février 2022 rendant indisponibles les données de 30 331 patients et de 1 129 salariés et collaborateurs.	Pas de sauvegardes régulières, en violation de ses propres règles internes ; aucune capacité de restauration rapide.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Centre social d'Aleksandrów Pologne, UODO, 03/06/2025 DKN.5131.30.2022 3 600 € 5 000 PLN pour le centre social et 10 000 PLN pour le maire, sanctionné en qualité de sous-traitant, convertis au cours légal polonais de 2025 (4,2092)	Rançongiciel de 2022 ; perte d'accès aux données d'environ 1 500 usagers ; sauvegarde chiffrée elle aussi.	Mesures inadaptées au regard de l'analyse de risque ; aucun test régulier de leur efficacité ; sous-traitant choisi sans vérification de ses garanties ; notification hors délai (art. 24, 25, 28, 32 et 33).
Hôpital pédiatrique Zamenhof de Białystok Pologne, UODO, 30/06/2025 DKN.5131.48.2022 15 800 € 66 500 PLN, convertis au cours légal polonais de 2025 (4,2092)	Rançongiciel du 12 janvier 2020 sur les systèmes de l'hôpital ; données d'environ 2 000 salariés.	Logiciels non à jour ou non vérifiés ; aucune vue centralisée de la sécurité ; aucun test régulier ; analyse de risque incorrecte.
Curtea Veche Publishing SRL Roumanie, ANSPDCP, 21/09/2022 5 000 €	Base des clients de l'éditeur pour 2019-2021 publiée sur un forum public (10 739 clients), puis rançongiciel touchant une centaine de salariés et collaborateurs.	Art. 32-1-b et c et 32-2.
Finopro IFN SA Roumanie, ANSPDCP, 06/03/2023 2 250 €	Rançongiciels ; accès non autorisé et perte d'intégrité et de disponibilité des données (pièces d'identité, relevés de compte).	Art. 32-1-b et c et 32-2.
Integral Collection SRL Roumanie, ANSPDCP, 06/03/2023 3 000 €	Rançongiciels ; accès non autorisé et perte d'intégrité et de disponibilité des données.	Art. 32-1-b et c et 32-2.
Partidul Uniunea Salvați România Roumanie, ANSPDCP, 15/03/2023 4 000 €	Hameçonnage ; accès aux données d'adhérents, dont l'appartenance politique.	Données ni chiffrées ni pseudonymisées dans l'application.
Farmacia Ardealul SRL Roumanie, ANSPDCP, 27/06/2023 2 500 €	Logiciel malveillant installé sur le site : faux formulaire de collecte de données bancaires des clients.	Mesures de sécurité du site insuffisantes.
UiPath Roumanie, ANSPDCP, 18/07/2023 70 000 €	Données d'environ 600 000 utilisateurs de la plateforme Academy publiées sur un forum de pirates fin novembre 2020 ; notification.	Paramétrage de l'espace de stockage permettant un accès non autorisé aux données ; accès restreint et authentification multifacteur mis en place seulement après.
Softehnica S.R.L. Roumanie, ANSPDCP, 23/01/2025 5 000 €	Rançongiciel : accès à l'infrastructure informatique de l'entreprise.	Mesures inadaptées ; aucun test ni évaluation périodique de leur efficacité.
Agricola International SA Roumanie, ANSPDCP, 23/07/2025 5 000 €	Cyberattaque notifiée par l'entreprise.	Art. 32-1-b et d et 32-2.
La Fântâna S.R.L. Roumanie, ANSPDCP, 01/09/2025 10 000 €	Attaque informatique notifiée par l'entreprise.	Art. 32-1-b et 32-2.
Unita Turism Holding S.A. Roumanie, ANSPDCP, 09/09/2025 5 000 €	Attaque informatique ; données divulguées et extraites.	Art. 32-1-b et 32-2.
Primonet RO Roumanie, ANSPDCP, 25/09/2025 20 000 €	Modification du code du site marchand ; données bancaires de clients compromises, avec pertes financières.	Plateforme du site dans une version obsolète, sans mesure limitant le risque de modification du code.
PGS SOFA & CO SRL Roumanie, ANSPDCP, 17/11/2025 8 000 €	Cyberattaque : accès à l'infrastructure et blocage de l'accès de l'entreprise ; données de salariés, clients et partenaires, dont comptes bancaires.	Mesures inadaptées.
Greencorp S.R.L. Roumanie, ANSPDCP, 19/11/2025 3 000 €	Attaque ayant permis d'accéder à toute la base de données et de chiffrer l'infrastructure.	Aucune mesure de sécurité spécifique ; aucun test périodique.

organisme et décision	ce qui s'est passé	ce qui a été reproché
Nițu A. Cleopatra – Expert Accountant Roumanie, ANSPDCP, 27/11/2025 2 000 €	Cyberattaque : accès à l'infrastructure et blocage ; données d'identité et financières divulguées.	Mesures inadaptées.
Roumasport S.R.L Roumanie, ANSPDCP, 30/12/2025 10 000 €	Cyberattaques répétées sur la plateforme informatique ; accès non autorisés aux données.	Mesures inadaptées pour empêcher l'accès illégal aux comptes clients de la plateforme (art. 32 et 24).
PREMIER RESTAURANTS ROMANIA SRL Roumanie, ANSPDCP, 13/01/2026 8 000 €	Attaque sur une application de l'entreprise ; accès aux données de salariés.	Mesures inadaptées ; recours à un sous-traitant sans garanties suffisantes (art. 32 et 28).
GENPACT ROMANIA SRL Roumanie, ANSPDCP, 04/02/2026 10 000 €	Attaque exploitant la faiblesse de mots de passe et la procédure de réinitialisation d'un compte compromis ; données professionnelles de salariés dans plusieurs pays de l'Union.	Mesures inadaptées au risque d'accès non autorisé (art. 32).
Renault Commercial Roumanie Roumanie, ANSPDCP, 25/03/2026 125 000 €	Cyberattaque sur une application gérée par un sous-traitant ; données d'un très grand nombre de personnes publiées sur une plateforme.	Mesures inadaptées ; sous-traitant ne présentant pas de garanties suffisantes.
Poliserv JG (PJG) SRL Roumanie, ANSPDCP, 19/08/2026 3 000 €	Identifiants d'un compte administrateur volés par hameçonnage ; accès aux données de clients.	Mesures inadaptées.
GEROCOSSEN S.R.L. Roumanie, ANSPDCP, 28/08/2026 5 000 €	Attaque sur l'infrastructure informatique de l'entreprise ; données d'identification et de contact consultées ou divulguées.	Mesures inadaptées pour garantir la confidentialité et l'intégrité des systèmes (art. 32) ; l'autorité impose l'enregistrement des accès et sa conservation au moins trente jours.
Global Customer Care Services S.R.L. Roumanie, ANSPDCP, 02/10/2026 5 000 €	Cyberattaque sur l'infrastructure ; données de salariés et anciens salariés consultées, confidentialité et disponibilité atteintes.	Mesures inadaptées.
MYCONNECTOR PLATFORM SRL Roumanie, ANSPDCP, 16/10/2026 6 000 €	Attaque sur le serveur de test de l'entreprise ; accès d'un tiers à des données.	Aucune mesure adaptée pour les tests de l'application.
Auchan România S.A. Roumanie, ANSPDCP, 30/10/2026 8 000 €	Attaque sur un compte administrateur d'un des systèmes de sécurité ; données d'utilisateurs internes divulguées.	Mesures inadaptées.
HORA CREDIT IFN S.A. Roumanie, ANSPDCP, 11/11/2026 10 000 €	Cyberattaque sur l'infrastructure ; données de clients, salariés et partenaires consultées.	Mesures inadaptées.
Sportadmin Suède, IMY, 26/01/2026 564 600 € 6 000 000 SEK, convertis au cours de la BCE du 26 janvier 2026 (10,6265)	Intrusion du 16 janvier 2025 par injection SQL, par une variable non protégée d'un site ; données de 2 126 075 personnes publiées sur le dark web.	Protection contre les injections SQL non appliquée lors d'une modification du code le 28 juin 2022, alors que l'entreprise disposait de la méthode.
Miljödata Suède, IMY, 22/09/2026 160 050 € 1 800 000 SEK, convertis au cours de la BCE du 22 septembre 2026 (11,2463)	Cyberattaque d'août 2025 chez l'éditeur de logiciels de ressources humaines de la majorité des communes suédoises ; données de 2,2 millions de personnes, selon l'entreprise, publiées sur le dark web.	Contrôles insuffisants lors de l'installation de nouveaux logiciels ; aucune surveillance automatisée en temps réel ; négligence retenue (art. 32).

LAZARÈGUE AVOCATS

Cabinet d'avocats en droit du numérique. Données personnelles, cybersécurité, intelligence artificielle, contrats informatiques, contentieux.

Les missions de conformité et d'audit sont conduites par les avocats du cabinet avec le concours d'experts techniques en cybersécurité.

18 rue de tilsitt, 75017 paris · 01 81 70 62 00 · contact@lazaregue-avocats.fr · lazaregue-avocats.fr

Ce document est une étude d'information générale. Il ne constitue pas une consultation juridique et ne formule aucune appréciation sur la responsabilité des organismes dont les affaires sont en cours.