Free : la CNIL juge les conditions latentes, pas l'attaque

En octobre 2024, Free et Free Mobile se présentent à leurs abonnés comme les victimes d'une cyberattaque. Les deux délibérations par lesquelles la CNIL les sanctionne, en janvier 2026, ne jugent pourtant pas l'attaque. Elles examinent ce qui l'a rendue possible, puis durable. Le dossier se lit avec un concept forgé par le psychologue James Reason, celui de conditions latentes (des failles installées par des décisions d'organisation antérieures, qui dorment dans le système jusqu'à ce qu'un acte les active). La tension tient en un fait consigné par le régulateur : l'opérateur a appris l'intrusion de l'attaquant lui-même.

DÉCLENCHÉE PAR

Sanction d'un régulateur · CNIL — formation restreinte · SAN-2026-001 — Free Mobile · 8 janvier 2026

Par Alexandre Berge · 27 novembre 2026 · 18 min de lecture · Chronique

De la victime d'une attaque au responsable d'un traitement

Entre le 24 et le 29 octobre 2024, les abonnés reçoivent un courriel les informant que la société a été victime d'une cyberattaque ciblant son outil de gestion, et que « toutes les mesures nécessaires ont été prises immédiatement ». La presse retient alors 19 millions d'abonnés et 5 millions d'IBAN (coordonnées bancaires) exposés. Devant la CNIL, Free Mobile soutient qu'elle serait le premier organisme, victime d'un acte de malveillance extérieur, poursuivi sur le fondement de l'article 32 du RGPD (l'obligation de sécurité). Après la sanction, l'opérateur qualifie la décision, auprès du Monde Informatique, de décision « d'une sévérité sans commune mesure au regard des précédents en matière de cyberattaques ». Son document d'enregistrement universel 2025 reprend la même présentation : les deux sociétés y « ont été victimes d'une cyberattaque ciblant un outil de gestion ».

Les documents opposables déplacent l'objet. Selon la délibération SAN-2026-001 du 8 janvier 2026, l'intrusion a duré du 28 septembre au 22 octobre 2024. L'attaquant s'est d'abord connecté au VPN de Free Mobile (le réseau privé virtuel qui permet aux salariés de rejoindre le système d'information à distance), puis à MOBO, l'outil de gestion des abonnés. Cet outil interroge aussi, pour les clients dits convergents, la base des abonnés fixes de Free. Une anomalie technique, apparue lors d'une mise à jour de MOBO et corrigée après la découverte de l'incident, renvoyait l'IBAN complet de ces clients. Free Mobile a notifié la violation à la CNIL

le 23 octobre 2024. Le contrôle sur place a eu lieu le 8 novembre 2024. La procédure a été disjointe le 24 juillet 2025, chaque société répondant de son propre système d'information.

La formation restreinte (l'organe de la CNIL chargé de prononcer les sanctions) a prononcé une amende administrative de 27 millions d'euros contre Free Mobile, pour des manquements aux articles 5-1-e (durée de conservation), 32 (sécurité) et 34 (information des personnes) du RGPD, et de 15 millions d'euros contre Free, pour des manquements aux articles 32 et 34. Ces montants tiennent compte du chiffre d'affaires de la maison mère Iliad (10,024 milliards d'euros en 2024), selon la notion d'entreprise du droit de la concurrence. Chaque société a reçu une injonction (un ordre de mise en conformité) de compléter ses mesures de sécurité sous trois mois. Free Mobile doit en outre achever le tri et la purge de ses données sous six mois. Les deux injonctions sont assorties d'une astreinte (une pénalité par jour de retard).

Les délibérations ont été publiées sur Légifrance le 14 janvier 2026. Le dernier document pris en compte est le document d'enregistrement universel 2025 d'Iliad, déposé le 24 avril 2026, qui indique que « Free et Free Mobile ont fait appel de la décision de la CNIL devant le Conseil d'État » sans mentionner de provision propre à ces amendes. Au 27 novembre 2026, aucune décision du Conseil d'État relative à ces sanctions ne figure dans la jurisprudence administrative publiée sur Légifrance, et aucune délibération de liquidation d'astreinte visant les deux sociétés n'apparaît dans le fonds CNIL du même site.

> **Chiffres structurants du dossier**
>
> 24 633 469 contrats concernés par la violation, dont 19 460 891 contrats mobiles et 5 172 577 contrats fixes. 2 614 plaintes reçues par la CNIL à la date de notification du rapport de sanction, un nombre qualifié de record par la formation restreinte. 58 239 appels traités par le numéro vert ouvert après l'incident. Astreintes de 50 000 euros par jour de retard pour Free Mobile et de 25 000 euros par jour pour Free.
>
> *Source : CNIL, délibérations SAN-2026-001 et SAN-2026-002 du 8 janvier 2026.*

Le régulateur sanctionne des défenses, pas un attaquant

L'obligation de sécurité est une obligation de moyens (une obligation de déployer des mesures adaptées, non de garantir un résultat) et la formation restreinte rappelle que la simple survenance d'une violation ne caractérise pas, à elle seule, un manquement à l'article 32. Elle s'appuie sur la Cour de justice de l'Union européenne, pour qui le RGPD instaure un régime de gestion des risques. Ce qu'elle se reconnaît le pouvoir de sanctionner est défini avec précision : « non pas la survenance d'une violation de données, mais le fait que celle-ci a été rendue possible ou a été facilitée » par l'insuffisance des mesures.

L'étalon retenu est la défense en profondeur telle que la formule l'ANSSI (l'agence nationale de la sécurité des systèmes d'information) : la sécurité ne doit reposer sur aucun élément

unique, et toute faille d'un composant doit être compensée par au moins un second niveau. Dans cette grille, l'attaquant n'apparaît que comme le révélateur d'un état antérieur.

Cette construction correspond presque terme à terme au modèle de James Reason. Dans son article du *BMJ* de mars 2000, il oppose une approche qui cherche le fautif au contact de l'événement à une approche systémique qui interroge les barrières : « When an adverse event occurs, the important issue is not who blundered, but how and why the defences failed » (quand un événement indésirable survient, la question importante n'est pas de savoir qui a commis l'erreur, mais comment et pourquoi les défenses ont cédé). Reason distingue deux origines aux brèches. Les défaillances actives ont un effet direct et bref. Les conditions latentes naissent de décisions prises en amont par les concepteurs, les rédacteurs de procédures et la direction, et peuvent rester en sommeil des années.

Transposé au cas, l'acte de l'attaquant occupe la place de la défaillance active. Le récit de la victime s'arrête à lui. La délibération remonte vers les conditions latentes, et c'est sur elles seules que porte la sanction.

> ***Les conditions latentes* (James Reason, 2000)**
>
> Dans le modèle dit du fromage suisse, chaque couche de défense d'un système (barrières techniques, procédures, contrôles humains) présente des trous. Un accident survient lorsque ces trous s'alignent. Les défaillances actives sont les actes dangereux commis au contact du système, à effet immédiat et bref. Les conditions latentes sont des faiblesses durables introduites par des décisions de conception, d'organisation ou de direction, qui peuvent dormir longtemps avant de se combiner à un déclencheur. À la différence des défaillances actives, elles peuvent être identifiées et corrigées avant l'événement.
>
> *James Reason, « Human error: models and management », BMJ, vol. 320, 18 mars 2000.*

Trois couches de défense, chacune trouée par un choix antérieur

La première couche est l'accès distant. Le rapporteur reprochait à Free Mobile l'absence d'authentification des postes nomades (la vérification que l'ordinateur qui se connecte appartient bien au parc de l'entreprise) et l'absence d'authentification multifacteur des utilisateurs (l'exigence d'un second élément de preuve en plus du mot de passe). Les développements correspondants de la délibération sont occultés pour des raisons de sécurité, mais la formation restreinte retient, dans sa motivation finale, l'absence de sécurisation de la connexion au VPN. Elle rappelle que l'ANSSI recommande depuis 2018 d'authentifier le poste nomade par un certificat machine. Ouvrir l'accès distant sans ces garde-fous relève d'une décision d'architecture et d'organisation du travail, non d'un incident.

La deuxième couche est la détection. Free Mobile disposait d'une solution de notation des connexions au VPN, fournie par un prestataire. La formation restreinte constate qu'elle était

paramétrée pour accepter par défaut l'ensemble des connexions, sauf dans deux cas. Le nombre anormal de connexions, sans rapport avec un usage standard, n'a pas suffi à déclencher une réaction, et l'attaquant a pu accéder aux données « pendant presque un mois, à de très nombreuses reprises ». Le réseau interne ne faisait l'objet d'aucun dispositif suffisant de détection des comportements suspects. Chez Free, la journalisation (l'enregistrement des accès) de l'outil de gestion des abonnés fixes produisait des rapports adressés au responsable de la sécurité, qui supposaient une intervention humaine, sans blocage automatique. La délibération SAN-2026-002 relève que le 15 octobre 2024, l'attaquant a pu exfiltrer les données d'un volume de contrats fixes dont le chiffre est occulté, sans alerte ou sans que l'alerte entraîne le blocage du compte.

La troisième couche est l'outil métier lui-même. La mise à jour qui a fait remonter l'IBAN complet des clients convergents est une modification ordinaire de logiciel, dont l'anomalie n'a été corrigée qu'après la découverte de la violation. C'est la forme la plus discrète de condition latente, celle du changement quotidien.

Aucune de ces défenses n'était absente. Chacune existait sous une forme réglée pour le fonctionnement normal : un score qui laisse passer, des journaux lus en différé, une mise à jour non évaluée du point de vue de la confidentialité. **La faute retenue n'est pas l'absence d'outils, c'est leur paramétrage pour la routine.** Les mesures qui manquaient sont celles que la société a déployées ensuite. Selon Free Mobile, son centre opérationnel de sécurité (une équipe chargée de surveiller en continu les événements de sécurité) a été déployé à l'issue du contrôle. Selon Free, le blocage automatique des comptes suspects date du 28 octobre 2024, après la violation. La chronologie des remèdes confirme la lecture de Reason : ces conditions étaient identifiables avant l'événement.

Une simplification a rendu une fonction invisible

Dans MOBO, les fonctions « recherche » et « consultation » étaient toutes deux journalisées, mais seule la consultation était analysée par un système produisant des alertes. Free Mobile justifiait ce choix par la structure de l'interface : une recherche n'affiche pas de données personnelles à l'écran, et seule la consultation d'une fiche permet d'y accéder. La formation restreinte constate que la réponse renvoyée par le serveur à une recherche contenait ces données, lisibles par l'outil de développement de n'importe quel navigateur, et que cette vulnérabilité a été exploitée par l'attaquant.

Le contrôle de sécurité avait donc été calé sur une représentation fonctionnelle de l'outil (ce que l'écran montre à l'utilisateur) et non sur son fonctionnement réel (ce que le serveur transmet). Karl Weick, Kathleen Sutcliffe et David Obstfeld ont décrit, dans leur étude de 1999 sur les organisations à haute fiabilité, ce que coûtent de telles réductions. Parmi les cinq processus qu'ils associent à la *vigilance collective*, la *réticence à simplifier les interprétations* repose sur une observation : « Simplifications increase the likelihood of eventual

surprise » (les simplifications augmentent la probabilité d'une surprise à terme). La simplification était une hypothèse raisonnable sur l'outil, devenue règle de surveillance, puis angle mort.

Les mêmes auteurs décrivent un second processus, la *sensibilité aux opérations*, c'est-à-dire l'attention portée à l'activité réelle du système au moment où elle se déroule. Le dossier en documente l'envers : les deux sociétés n'ont pas détecté l'intrusion, elles en ont été informées par son auteur.

> **Extrait de la délibération SAN-2026-002 du 8 janvier 2026 (point 109)**
>
> « […] l'attaquant a pu accéder aux données des clients convergents contenues dans l'outil SIEBEL de la société, et ce pendant presque un mois, sans qu'une alerte ne soit émise ou, à supposer qu'une alerte ait bien été émise, sans que celle-ci soit traitée, ce qui a eu pour conséquence que la société n'a pas eu connaissance de l'accès non autorisé aux données avant que l'attaquant l'en informe lui-même. »

La conservation : une faute sanctionnée sans lien établi avec la fuite

Une partie de la presse a associé la conservation excessive des données à l'ampleur de la fuite, en écrivant que l'attaquant avait eu accès aux données d'anciens abonnés. La délibération est plus prudente, et cette prudence est instructive.

La délégation de contrôle a constaté la présence de données relatives à plus de quinze millions de contrats résiliés depuis plus de cinq ans, dont trois millions depuis plus de dix ans. Pour 2 806 690 de ces derniers, la société reconnaît une conservation excessive. Elle l'explique par une purge non achevée, par une activité commencée en 2012 qui n'aurait posé la question de la suppression que récemment, et par une architecture qui se prête mal aux purges à grande échelle sans risque de blocage des services métiers. La formation restreinte écarte ces justifications et retient la négligence : une société qui conserve les données cinq ans après la fin du contrat à des fins de lutte contre la fraude aurait dû, pour un abonné parti en 2012, commencer à les supprimer en 2017.

En revanche, la formation restreinte déclare que les éléments du dossier ne lui permettent pas de dire si l'absence de purge a donné à l'attaquant accès à une profondeur historique plus grande, ni donc de considérer que ce manquement a aggravé celui de l'article 32. La société soutenait que le compte usurpé ne donnait accès qu'aux contrats en cours et à ceux résiliés depuis moins d'un an. La conservation est sanctionnée comme une faute autonome, sans lien causal établi avec la violation.

Cette autonomie est le cœur du raisonnement. Une condition latente n'a pas besoin d'avoir été activée pour être sanctionnée. La même délibération retient d'ailleurs un manquement à l'article 32 pour le mode de stockage des mots de passe des utilisateurs de MOBO, en

précisant que l'attaquant ne l'a pas exploité et que ce point est indifférent. La délibération SAN-2026-016 du 12 novembre 2026 pousse la logique à son terme. Elle sanctionne de 5 millions d'euros un assureur-vie, que la décision ne nomme pas, pour avoir conservé en clair près de 1,8 million de mots de passe de clients et partagé entre huit personnes un compte générique d'accès à sa base, hors de toute violation de données. La formation restreinte y juge la vulnérabilité constituée, « peu important que cette vulnérabilité ait été exploitée ou non par un attaquant ». **Ce que le régulateur sanctionne, dans les deux dossiers, est le risque laissé ouvert, non le dommage.**

TalkTalk, 2015 : la même grammaire, dix ans plus tôt

Le précédent le plus proche par sa structure est britannique. Entre le 15 et le 21 octobre 2015, un attaquant exploite, chez l'opérateur TalkTalk, trois pages web héritées du rachat des activités britanniques de Tiscali en 2009, qui donnaient accès à une base de clients. Selon l'Information Commissioner's Office (ICO), le régulateur britannique, l'attaque est une injection SQL (l'insertion de commandes dans un formulaire pour interroger directement une base), technique connue depuis plus de dix ans, et le correctif du logiciel existait depuis plus de trois ans et demi. Deux attaques par injection SQL avaient déjà visé les mêmes pages le 17 juillet et entre le 2 et le 3 septembre 2015, sans réaction de l'opérateur faute de surveillance. Les données de 156 959 clients ont été consultées, dont les coordonnées bancaires de 15 656 d'entre eux.

L'ICO a infligé le 5 octobre 2016 une amende de 400 000 livres, alors la plus élevée de son histoire. Sa commissaire, Elizabeth Denham, a résumé la position du régulateur en reconnaissant le caractère illicite du piratage, tout en ajoutant, selon The Register, « but that is not an excuse for companies to abdicate their security obligations » (mais ce n'est pas une excuse pour que les entreprises se dérobent à leurs obligations de sécurité).

La proximité avec le dossier Free tient à trois traits : un opérateur grand public, une condition latente installée par une décision ancienne et étrangère à la sécurité (une acquisition chez TalkTalk, une politique de conservation jamais exécutée chez Free Mobile), et une détection absente, que l'ICO établit par les tentatives antérieures restées inaperçues et la CNIL par un mois d'accès. Dans les deux cas, le régulateur sépare explicitement la faute de l'attaquant de l'obligation du responsable. Plus récemment, le président de Marks & Spencer, Archie Norman, a décrit devant une sous-commission parlementaire britannique, le 8 juillet 2025, une intrusion par usurpation d'identité qu'il jugeait sophistiquée, tout en posant pour principe qu'une entreprise de sa taille doit « assume that the perimeter is permeable » (partir du principe que le périmètre est perméable), ce qui reporte la question sur la capacité à détecter.

Quand l'alerte vient de l'extérieur, le mécanisme est déjà installé

Une intrusion banale devient une violation massive lorsque plusieurs conditions latentes, chacune issue d'une décision raisonnable dans son propre périmètre, s'alignent sur une même trajectoire. L'accès distant relève de l'organisation du travail, le paramétrage de la détection d'un arbitrage entre fausses alertes et charge des équipes, le périmètre de la surveillance de la représentation que les concepteurs se font de leur outil, la conservation d'une politique juridique dont l'exécution bute sur la continuité des services. Aucune de ces décisions n'appartient au même responsable, et aucune ne se présente comme un choix de sécurité.

Le mécanisme se reproduit lorsque l'accès distant est pensé pour la commodité avant de l'être pour l'authentification des postes, lorsque la détection laisse passer par défaut et repose sur des rapports périodiques plutôt que sur un traitement en temps réel, lorsque la surveillance porte sur les fonctions visibles d'une application plutôt que sur ses flux, et lorsque la purge des données est reportée parce qu'elle menace le fonctionnement courant. Plus le volume de données est grand, plus l'alignement de ces trous produit un événement massif.

Plusieurs signes rendent ce mécanisme visible ailleurs. Le premier est l'origine externe de l'alerte : un attaquant qui se signale, une mise en vente découverte par un tiers, un chercheur qui prévient. La CNIL en a fait un constat général dès janvier 2025. Dans les violations massives de 2024, observe-t-elle, les intrusions et les exfiltrations n'avaient pas été détectées par les organismes avant la mise en vente des données, et les modes opératoires exploitaient régulièrement les mêmes failles. Le deuxième signe est la chronologie des remèdes : une mesure déployée après l'incident était, le plus souvent, connue et disponible avant. Le troisième est la justification par l'architecture : l'argument selon lequel le système d'information « s'accorde difficilement » avec une exigence réglementaire décrit, dans le vocabulaire de Reason, une condition latente reconnue et conservée.

Le praticien y reconnaît une difficulté de gouvernance plus qu'un défaut technique : réparties entre plusieurs responsables, les conditions latentes ne deviennent un objet de décision qu'au moment où un acte extérieur les aligne.

Un recours annoncé, une question ouverte

L'opérateur a bien été victime d'une attaque, et cette qualité n'a pas pesé sur l'appréciation de ses obligations. La CNIL a jugé les conditions latentes qui ont rendu l'attaque possible et durable, et elle a sanctionné l'une d'elles sans même établir qu'elle avait joué. Le fait le plus lourd du dossier n'est ni le montant ni le nombre de contrats. C'est que l'alerte est venue de l'attaquant.

Free et Free Mobile ont saisi le Conseil d'État. La délibération rappelle que la haute juridiction

a déjà admis qu'un manquement à l'article 32 soit caractérisé à la lumière des recommandations publiques de la CNIL et de l'ANSSI. Si la lecture proposée ici est juste, le contentieux portera davantage sur le montant et sur l'assiette du chiffre d'affaires du groupe que sur l'existence des manquements de détection, qui reposent sur des constats matériels peu contestables. L'indicateur est public : une décision du Conseil d'État relative aux délibérations SAN-2026-001 et SAN-2026-002, consultable sur Légifrance, d'ici le 30 novembre 2028. Un second indicateur est observable plus tôt. La délibération Free cite elle-même quatre précédents de sanctions prononcées après une violation. Si elle fait jurisprudence, les sanctions de la CNIL fondées sur l'article 32 après une intrusion la citeront à leur tour parmi leurs précédents, ce que les délibérations publiées d'ici le 30 novembre 2027 permettront de vérifier. La question plus large prolonge celle de Reason : combien d'organisations savent aujourd'hui, autrement que par leur attaquant, ce que leurs journaux enregistrent sans être lus ?

Note méthodologique

L'article repose sur le texte intégral des délibérations SAN-2026-001, SAN-2026-002 et SAN-2026-016, sur le communiqué de la CNIL et sur la note 35 du document d'enregistrement universel 2025 d'Iliad. Les causalités relatives à la sécurité sont établies par la formation restreinte, qui déclare en revanche ne pas pouvoir établir le lien entre conservation excessive et ampleur de la fuite. Trois divergences entre sources publiques ont été arbitrées en faveur des délibérations : la date des décisions (13 janvier 2026 selon le communiqué, 8 janvier selon les délibérations), le volume (19 millions d'abonnés et 5 millions d'IBAN dans la presse, 24 633 469 contrats dans la délibération) et la date du contrôle (2025 dans une partie de la presse, 8 novembre 2024 dans la délibération). Les affirmations d'absence portent sur la jurisprudence administrative et le fonds CNIL de Légifrance, consultés le 27 novembre 2026. L'assureur-vie n'est pas nommé, conformément au choix de la formation restreinte. Le choix de Reason comme cadre central, de Weick, Sutcliffe et Obstfeld en appui et de TalkTalk comme parallèle relève de l'auteur. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Décisions et documents d'autorités

- CNIL, formation restreinte, « Délibération de la formation restreinte n° SAN-2026-001 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE MOBILE », 8 janvier 2026, publiée sur Légifrance le 14 janvier 2026, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352664

- CNIL, formation restreinte, « Délibération de la formation restreinte n° SAN-2026-002 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE », 8 janvier 2026, publiée sur Légifrance le 14 janvier 2026, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352643
- CNIL, « Violation de données : sanction de 42 millions d'euros à l'encontre des sociétés FREE MOBILE et FREE », 14 janvier 2026, https://www.cnil.fr/fr/sanction-free-2026
- CNIL, formation restreinte, « Délibération de la formation restreinte n° SAN-2026-016 du 12 novembre 2026 prononçant une sanction pécuniaire à l'encontre de la société X », 12 novembre 2026, publiée sur Légifrance le 18 novembre 2026, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000055097962
- CNIL, « Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ? », 28 janvier 2025, https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre

Documents de l'organisation

- Iliad S.A., « Document d'enregistrement universel 2025 », déposé auprès de la CSSF le 24 avril 2026, section 2.1 (facteurs de risques) et note 35.5 « Procès et litiges », p. 318, https://www.iliad.fr/media/Iliad_DEU_2025_FR_240426_da32cc9496.pdf

Cadres théoriques

- James Reason, « Human error: models and management », BMJ, vol. 320, n° 7237, 18 mars 2000, p. 768 à 770, https://pmc.ncbi.nlm.nih.gov/articles/PMC1117770/
- Karl E. Weick, Kathleen M. Sutcliffe et David Obstfeld, « Organizing for High Reliability: Processes of Collective Mindfulness », dans R. I. Sutton et B. M. Staw (dir.), Research in Organizational Behavior, vol. 21, JAI Press, 1999, p. 81 à 123, version consultée le 27 novembre 2026, http://wendynorris.com/wp-content/uploads/2018/08/Weick-et-al-2008-Organizing-for-High-Reliability-Processes-of-Collective-Mindfulness.pdf.pdf

Parallèle historique

- Information Commissioner's Office, « TalkTalk cyber attack - how the ICO's investigation unfolded », page consultée le 27 novembre 2026, https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/
- Alexander J. Martin, « TalkTalk gets record £400k slap-slap from Brit watchdog », The Register, 5 octobre 2016, https://www.theregister.com/2016/10/05/ico_finally_delivers_record_400k_fine_to_talktalk_over_breach/
- House of Commons, Business and Trade Sub-Committee, « Oral evidence: UK economic security, HC 835 », audition d'Archie Norman, 8 juillet 2025, https://committees.parliament.uk/oralevidence/16268/html/

Presse de référence

- Le Monde Informatique, « Vol de données : la Cnil inflige 42 M€ d'amende à Free », 14 janvier 2026, https://www.lemondeinformatique.fr/cybersecurite-conformite/2026-01-14-vol-de-donnees-la-cnil-inflige-42-m-d-amende-a-free