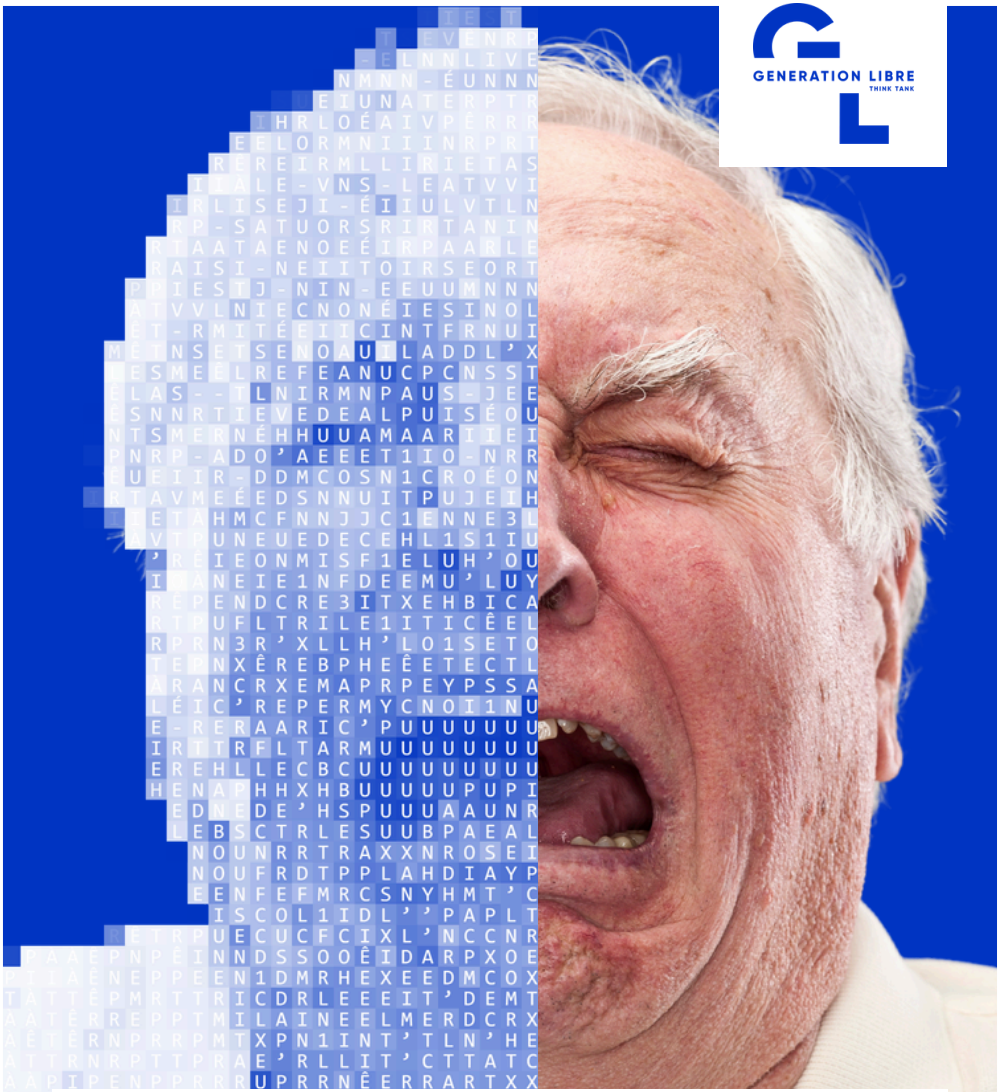
MAI 2026



NOTE

Fuites de données en France : l'échec du modèle réglementaire européen

Grégory Lenne

Génération Libre
est un **think tank**
indépendant qui vise
à promouvoir les libertés.
Toutes les libertés.

Table des matières

Le 21 avril 2026, le ministère de l'Intérieur confirmait la compromission du portail France Titres : une faille élémentaire permettait d'accéder aux données de n'importe quel usager en modifiant un simple identifiant dans l'URL, exposant jusqu'à 11,7 millions de comptes. Cette affaire, dernière d'une longue série, cristallise l'échec du modèle français de protection des données personnelles. La France se classe désormais au deuxième rang mondial des pays les plus touchés, et au premier rang rapporté à la population[1]. Les sanctions liées aux fuites de données restent d'une modestie dérisoire : 5 M€ pour France Travail[2] (36,8 millions de personnes concernées, soit 0,14 € par personne) et 42 M€ pour Free (24 millions de contrats, soit 1,75 € par contrat)[3]. La présidente de l'autorité estime pourtant que 80 % des grandes violations auraient pu être évitées avec des mesures élémentaires comme l'authentification multifacteur (MFA)[4]. Cette explosion des fuites, huit ans après l'entrée en vigueur du RGPD, invite à questionner l'efficacité du modèle réglementaire européen et à explorer des alternatives fondées sur la responsabilité individuelle et la propriété des données.

[1] IT Pro, « *Fuites de données : la France, 2ème pays le plus touché au monde début 2026* », 27 avril 2026.
[2] CNIL, « *Violation de données : sanction de 5 millions d'euros à l'encontre de FRANCE TRAVAIL* », 22 janvier 2026. Le chiffre de 36,8 millions correspond aux personnes effectivement concernées par la fuite ; le système d'information piraté couvrait au total 43 millions d'inscrits au titre des vingt dernières années.
[3] CNIL, « *Délibérations SAN-2026-001 et SAN-2026-002 du 8 janvier 2026* », sanctions de 27 M€ à l'encontre de FREE MOBILE et 15 M€ à l'encontre de FREE (cumul 42 M€).
[4] France 24, « *Face aux fuites de données massives, la Cnil va hausser le ton, annonce sa présidente* », 29 avril 2025.

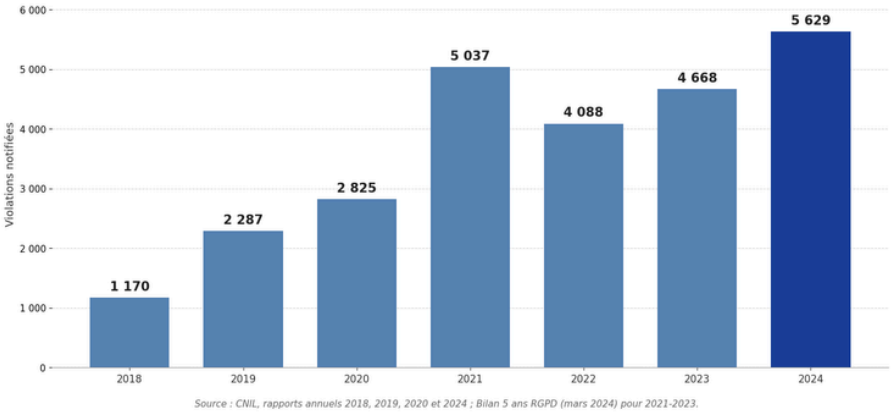
01

Partie 1
Un constat alarmant : l'explosion des fuites de données

Partie I — Un constat alarmant : l'explosion des fuites de données

A. Des chiffres en hausse constante

Les statistiques officielles révèlent une tendance préoccupante. Selon le Baromètre des fuites de données InCyber 2026[5], la France a enregistré en 2025 une moyenne de 24 fuites par jour à la CNIL, contre 16 en 2024 et 13 en 2023. Les fuites d'origine malveillante ont augmenté de 60 %, tandis que les attaques externes progressent de 58 %.



Évolution des violations de données notifiées à la CNIL (2018-2024)

Ce phénomène s'inscrit dans un contexte géopolitique tendu : selon l'ANSSI[6], les attaquants liés aux intérêts stratégiques russes ont intensifié leurs opérations depuis l'invasion de l'Ukraine en 2022, ciblant ministères, entreprises de défense et infrastructures critiques. La France a, pour la première fois, officiellement attribué des cyberattaques au renseignement militaire russe en avril 2025[7].

[5] Forum InCyber et Hexatrust, *Baromètre des fuites de données personnelles — Édition 2025*, mars 2025.
[6] ANSSI, *Panorama de la cybermenace 2024*, mars 2025.
[7] Ministère de l'Europe et des Affaires étrangères, « *Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28)* », communiqué du 29 avril 2025.

L'ampleur des violations récentes donne la mesure du problème : 36,8 millions de personnes exposées via France Travail[8], 33 millions via les gestionnaires de tiers payant Viamedis et Almerys[9], 24 millions via Free[10], et la séquence ne ralentit pas : entre 11 et 15 millions de dossiers patients compromis chez Cegedim Santé en février 2026[11], 11,7 millions de comptes du portail France Titres en avril 2026[12]. Selon Surfshark, la France a cumulé depuis 2004 environ 31 données personnelles compromises par habitant et a même pris la tête du classement mondial 2025 par densité de violations[13]. En cumulant les fuites massives de 2024 à 2026, la quasi-totalité de la population adulte française a vu ses données personnelles compromises au moins une fois (voir détails des principales fuites en annexe).

B. Des conséquences concrètes pour les citoyens

L'enjeu dépasse la vie privée : selon le cabinet Astères, le coût des cyberattaques réussies en France était évalué à 2 milliards d'euros pour la seule année 2022[14]. Ces fuites exposent les individus à des risques qui dépassent le cadre numérique. Usurpation d'identité, fraudes bancaires via les IBAN dérobés, phishing ciblé exploitant des données authentiques : le service Cybermalveillance.gouv.fr a enregistré une augmentation de 49 % des demandes d'assistance en 2024[15].

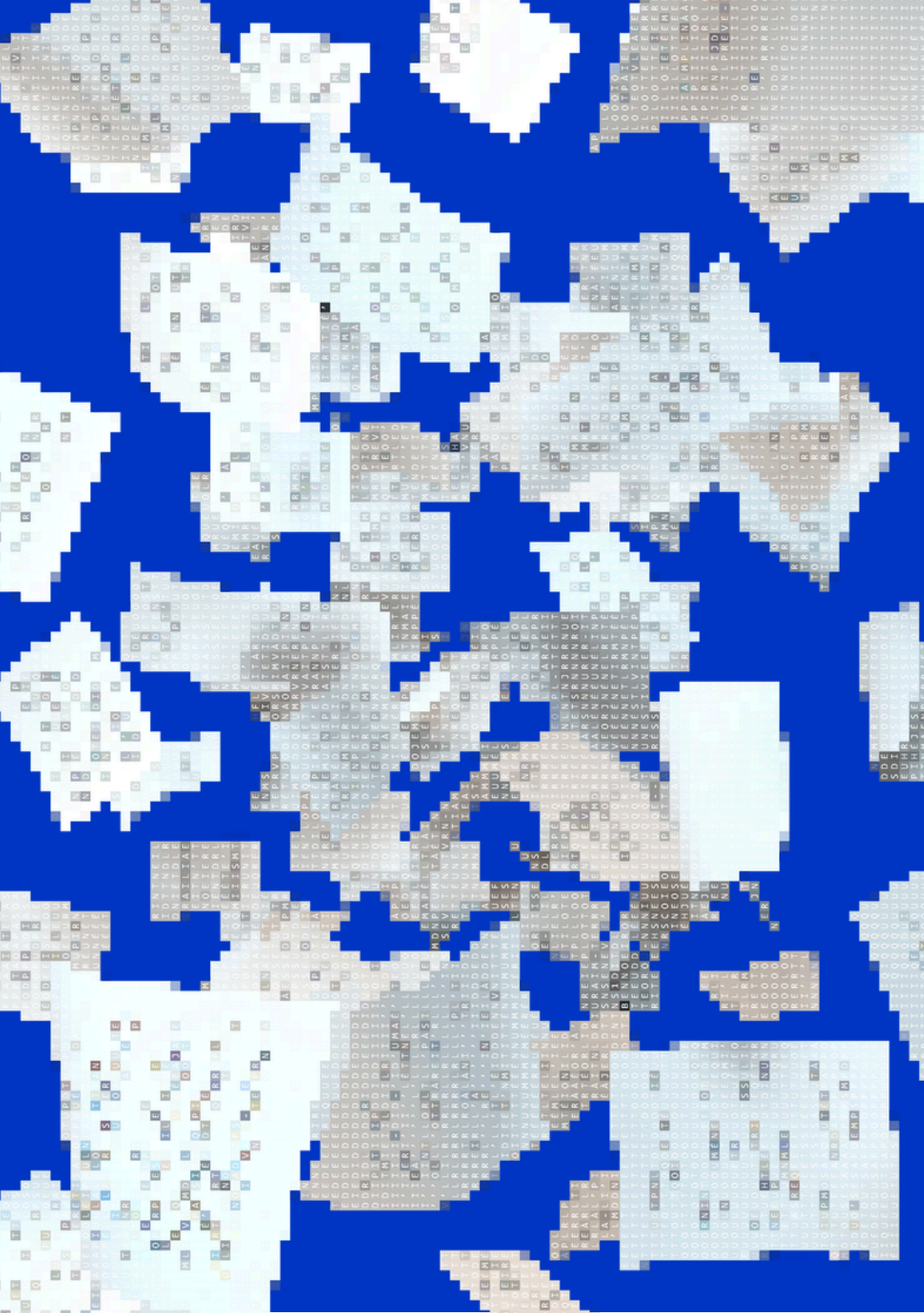
Certaines fuites génèrent des menaces physiques directes : le piratage de la Fédération française de tir en octobre 2025 a exposé les adresses de 250 000 adhérents actuels et 750 000 anciens adhérents, provoquant une série de cambriolages (20 à 30 selon le ministère de l'Intérieur, avril 2026) ciblés pour dérober des armes à feu[16]. La combinaison de données issues de plusieurs fuites permet désormais de constituer des « kits d'identité » complets facilitant home-jacking, extorsion de détenteurs de crypto-monnaies, parfois sous menace physique, et escroqueries de grande ampleur.

[8] CNIL, « *Délibération SAN-2026-001 du 22 janvier 2026* », sanction de FRANCE TRAVAIL.
[9] CNIL, « *Violation de données de deux opérateurs de tiers payant : la CNIL ouvre une enquête* », 7 février 2024.
[10] CNIL, « *Délibérations SAN-2026-001 et SAN-2026-002 du 8 janvier 2026* », sanctions à l'encontre de FREE et FREE MOBILE.
[11] Franceinfo, « *Enquête francetv : une fuite massive de données médicales inquiète en France* », *L'Œil du 20 heures, France 2*, 26 février 2026.
[12] CNIL, *Notifications de violations de données 2024, et bilans 2025* (*DPO Partage*, mars 2026) ; pour les fuites 2026, voir également les notes infra : Cegedim Santé (*Franceinfo*, 27 février 2026) et France Titres (ministère de l'Intérieur, 21 avril 2026).
[13] Surfshark, « *Data Breach Monitoring* » : (a) sur le cumul des données compromises depuis 2004, la France figure au 3e rang mondial (environ 31 données par habitant) ; (b) sur la densité 2025 (violations rapportées à la population), la France se classe au 1er rang mondial.
[14] Astères, « *Le coût des cyberattaques réussies en France* », juin 2023 (données 2022).
[15] Cybermalveillance.gouv.fr, *Rapport d'activité 2024*, mars 2025, p. 31.
[16] « *Cyberattaques : la France confrontée à une multiplication des fuites de données* », *Le Journal du Dimanche*, 2 février 2026.

L'usurpation d'identité est devenue une industrie. Plus de 200 000 Français en sont victimes chaque année, avec un préjudice moyen de 19 000 euros pour les crédits frauduleux[17]. Les deepfakes utilisés à des fins de fraude ont explosé de 700 % au niveau mondial entre le premier trimestre 2024 et le premier trimestre 2025, et de près de 100 % en France sur l'exercice antérieur (Q1 2023-Q1 2024)[18]. Et les victimes entament un parcours du combattant pouvant s'étaler sur plusieurs années : dépôt de plainte, signalement Banque de France, contestation crédit par crédit, reconstitution de leur historique.

Paradoxalement, le RGPD impose des contraintes considérables sans endiguer ces violations. Les PME consacrent des dizaines de milliers d'euros annuels à leur conformité (DPO, audits, registres). Après une cyberattaque, 47 % des entreprises rencontrent des difficultés à attirer de nouveaux clients, et 43 % perdent des clients existants[19]. Le règlement a créé une industrie de la conformité formelle ; les 5 629 violations notifiées en 2024 démontrent qu'il n'a pas instauré une culture effective de la sécurité.

[17] France Info, « *Usurpation d'identité : des milliers de Français en sont victimes chaque année* », janvier 2025.
[18] Sumsub, *Identity Fraud Report 2025-2026*, novembre 2025 (chiffre +700 % mesuré au niveau mondial entre Q1 2024 et Q1 2025, données internes Sumsub). Pour la France, la même série Sumsub mesure une progression de près de 100 % sur la période précédente. Ce chiffre émane d'un prestataire commercial de vérification d'identité. L'ordre de grandeur est corroboré par le rapport Europol IOCTA 2025 qui relève une « augmentation exponentielle » de l'usage des deepfakes à des fins frauduleuses.
[19] Hiscox, *Rapport Hiscox 2024 sur la gestion des cyber-risques*, octobre 2024.



02

Partie 2

Le paradoxe du RGPD : beaucoup de règles, peu de protection réelle

Partie II — Le paradoxe du RGPD : beaucoup de règles, peu de protection réelle

A. Une régulation qui agit après coup

Le Règlement Général sur la Protection des Données (RGPD) impose aux entreprises de notifier les violations de données à la CNIL sous 72 heures. Ce mécanisme crée une illusion de contrôle : les entreprises déclarent la fuite, la CNIL enregistre, parfois sanctionne, mais les données sont déjà dans la nature, revendues sur le dark web ou exploitées par des criminels. L'affaire France Travail l'illustre crûment : la CNIL a révélé que 9 gigaoctets de données, soit l'équivalent de 13 millions de fiches, avaient été extraits lors de cette seule journée (sur les 36,8 millions de personnes finalement notifiées comme exposées), sans déclencher la moindre alerte[20].

Comme le note la CNIL elle-même dans son bilan 2024[21] : « Les modes opératoires des attaquants sont souvent similaires et exploitent des failles de sécurité prévisibles. » Le règlement organise la gestion bureaucratique des incidents, mais n'empêche pas leur survenue.

B. La conformité comme substitut à la sécurité

Le RGPD a engendré une industrie de la conformité : DPO (Délégués à la Protection des Données), registres de traitement, études d'impact, politiques de confidentialité interminables. À titre d'exemple, un DPO interne représente une rémunération médiane de 65 à 75 000 euros bruts annuels selon le baromètre AFCDP, un DPO externalisé entre 200 et 1 500 euros par mois, une analyse d'impact 3000 € pièce[22]. À l'échelle nationale, des milliards d'euros sont ainsi consacrés à la conformité réglementaire.

Mais conformité juridique ne signifie pas sécurité technique. Le système incite à cocher des cases plutôt qu'à investir dans la cybersécurité réelle. Les incidents de 2024-2025 le démontrent : des entreprises conformes sur le papier (France Travail, Free, Viamedis) ont subi des attaques massives parce que leurs systèmes d'information présentaient des failles élémentaires : absence d'authentification multifacteur, habilitations trop larges, données non chiffrées, API mal sécurisées. On a créé des armées de juristes spécialisés dans la conformité documentaire, pas des armées d'ingénieurs capables de sécuriser les infrastructures.

---

[20] CNIL, « *Délibération n° SAN-2026-003 du 22 janvier 2026 — Sanction de 5 M€ à l'encontre de FRANCE TRAVAIL* ».
[21] CNIL, « *Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ?* », janvier 2025.
[22] FCN Data, « *Le véritable coût de la conformité RGPD* ».

Un phénomène qui ne devrait pas décroître avec l'essor du « vibe coding », ces sites et applications développés à la va-vite à l'aide d'assistants IA, sans audit de sécurité. En janvier 2026, le site de campagne de Sarah Knafo pour les municipales parisiennes en a fourni une illustration spectaculaire : dès sa mise en ligne, les données personnelles des 607 contributeurs (noms, emails, numéros de téléphone, adresses IP) étaient accessibles à n'importe qui depuis la console du navigateur, sans la moindre compétence technique requise[23]. Le hacker éthique *SaxX*, qui a révélé la faille, a relevé que le site était bâti sur le framework Next.js et contenait des références explicites à Claude dans son code, signe d'un développement en « vibe coding ». La conformité RGPD affichée dans les mentions légales du site n'avait aucune traduction technique : les données des personnes ayant explicitement demandé l'anonymat étaient tout autant exposées.

L'affaire France Titres, annoncée le 21 avril 2026, en fournit l'illustration la plus récente, et la plus accablante pour l'État lui-même. Le portail de l'Agence nationale des titres sécurisés (ANTS), par lequel les citoyens demandent passeports, cartes d'identité et permis de conduire, a été compromis via une faille IDOR[24] élémentaire : il suffisait de modifier un identifiant dans une requête pour accéder aux données d'un autre citoyen. Selon le ministère de l'Intérieur, 11,7 millions de comptes sont concernés[25]. L'enquête a été confiée à l'Office anti-cybercriminalité et notifiée au parquet de Paris[26]. Quelques semaines plus tôt, en février 2026, la fuite Cegedim Santé avait exposé les données administratives d'entre 11 et 15 millions de personnes, dont 164 000 avec des annotations médicales sensibles, via le logiciel[27] de cabinets médicaux MonLogicielMédical. Ces deux affaires partagent un trait commun : la faille n'a rien de sophistiqué, et le RGPD n'a rien empêché.

C. Des sanctions déconnectées du préjudice individuel

L'exemple de Free est emblématique. En janvier 2026, la CNIL a infligé à l'opérateur, à la suite de la fuite massive d'octobre 2024, deux sanctions cumulant 42 millions d'euros. Il s'agit de la plus lourde pénalité française jamais prononcée pour défaut de sécurité après une fuite de données. Cette somme va intégralement au budget de l'État. Comme le souligne 60 Millions de consommateurs, aucun mécanisme automatique de redistribution n'est prévu pour les abonnés lésés[28]. Rapportée aux 24 millions de contrats concernés, l'amende représente 1,75 euro par contrat (somme dont les abonnés ne verront jamais la couleur).

---

[23] « *Noms, emails, adresses IP… le nouveau site de Sarah Knafo était une véritable passoire* », *Next.ink*, 9 janvier 2026 ; voir également *Libération CheckNews*, même date.

[24] Ministère de l'Intérieur, *communiqué du 21 avril 2026 sur la fuite du portail ANTS* (l'estimation initiale de 19 millions de personnes a été ramenée à 11,7 millions de comptes après expertise). Voir aussi RGPD Kit, « *Piratage ANTS* », 24 avril 2026.

[25] Franceinfo, « *Fuite de données sur le portail de l'ANTS : près de 12 millions de comptes concernés, annonce le ministère de l'Intérieur* », 21 avril 2026.

[26] Franceinfo, « *Informations personnelles volées, appel à la vigilance… Ce que l'on sait de la fuite de données de l'ANTS* », 21 avril 2026.

[27] Franceinfo / L'Œil du 20 heures, « *Une fuite de données médicales inquiète en France, entre 11 et 15 millions de personnes touchées* », 27 février 2026. V. aussi Caducee.net, « *Cegedim : l'État acte l'ampleur de la fuite et précise le risque « données sensibles » pour 164 000 personnes* », 28 février 2026.

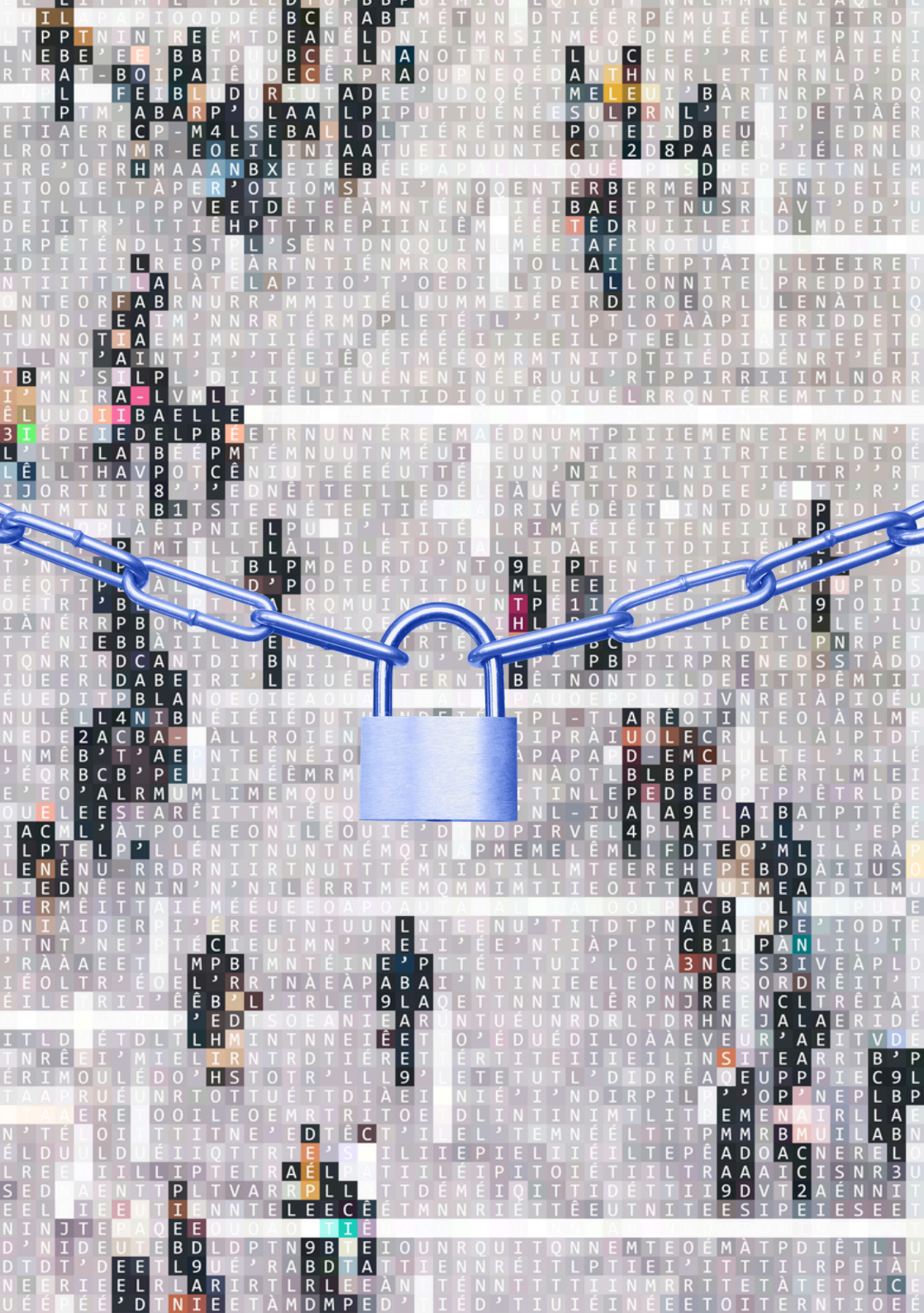
[28] 60 Millions de consommateurs, « *Sanction de Free par la Cnil : une aubaine pour les victimes ?* », 15 janvier 2026.

Pour obtenir réparation, les victimes doivent entreprendre des démarches judiciaires individuelles, prouver l'existence d'un préjudice réel et établir un lien de causalité direct, véritable parcours du combattant que peu de citoyens peuvent ou veulent affronter. Sur le montant de la réparation, la Cour de justice de l'Union européenne renvoie au droit national : ce sont les principes dégagés par la jurisprudence française qui s'appliquent. Or le préjudice moral, souvent le seul invocable, reste historiquement faiblement indemnisé : dans l'affaire de référence européenne, le requérant demandait 1 000 euros de dommages et intérêts pour préjudice moral, et fut débouté en première et seconde instance[29]. Pour les actions de groupe en droit de la consommation, le préjudice moral était jusqu'à récemment exclu : l'ancien article L. 623-2 du Code de la consommation limitait la réparation aux seuls préjudices patrimoniaux résultant de dommages matériels. La loi DDADUE n° 2025-391 du 30 avril 2025, transposant la directive (UE) 2020/1828, a abrogé cette restriction : l'action de groupe peut désormais porter sur la réparation des préjudices « quelle qu'en soit la nature », préjudice moral inclus. Reste qu'une action de groupe effective sur les fuites de données suppose une association de consommateurs agréée disposant des moyens d'agir, condition rarement réunie : le passage du droit textuel au droit effectif demeure l'obstacle principal[30]. En présence de coresponsables, situation de plus en plus fréquente avec la sous-traitance, la victime peut certes agir contre n'importe lequel d'entre eux en vertu de la responsabilité solidaire prévue à l'article 82 §4 du RGPD ; mais l'absence de mécanisme automatique de réparation, la complexité de la preuve et le jeu des exonérations possibles (art. 82 §3) la dissuadent en pratique d'engager une action et d'obtenir une compensation directe[31].

[29] CJUE, 4 mai 2023, *aff. C-300/21, Ul c. Österreichische Post AG.*

[30] *Ancien article L. 623-2 du Code de la consommation*, abrogé par la *loi n° 2025-391 du 30 avril 2025* (loi DDADUE transposant la directive (UE) 2020/1828 relative aux actions représentatives), article 16. Le nouveau régime ouvre l'action de groupe à la réparation des préjudices « quelle qu'en soit la nature ».

[31] Règlement (UE) 2016/679, article 82 §§ 3-4. Voir Les Électrons Libres, « *Data : l'exceptionnelle passoire française* », *lel.media,* 3 mars 2026.



03

Partie 3
La proposition de Génération Libre : vers une propriété des données

Partie III — La proposition de Génération Libre : vers une propriété des données

Avant d'examiner la proposition de *Génération Libre*, une question préalable mérite réponse : pourquoi un régime d'exception pour les données personnelles ? Le droit privé classique sait, en règle générale, indemniser les préjudices. Quatre raisons justifient pourtant un traitement particulier. D'abord, l'irréversibilité : une donnée fuitée ne se « répare » pas, contrairement à un bien matériel ; elle circule, se duplique et s'agrège indéfiniment. Ensuite, l'asymétrie d'information radicale entre l'individu et les plateformes qui exploitent ses données rend illusoire la négociation contractuelle de droit commun. Vient s'y ajouter le caractère démultiplicateur des fuites, qui exposent à des risques systémiques (usurpation d'identité, profilage politique, ingérences étrangères) sans commune mesure avec l'atteinte à un bien classique. Enfin, la défaillance avérée des régimes de droit commun, dont huit années de RGPD apportent la démonstration empirique.

A. Le principe : mes données m'appartiennent

Depuis 2018 et la publication du rapport de *Génération Libre* « Mes data sont à moi » par le *Collectif data*[32] et prolongé en 2019 par « Aux data, citoyens ! » de *Lucas Léger* et *Pierre Bentata*[33], *Génération Libre* défend une approche différente : reconnaître un droit de propriété sur les données personnelles. Cette thèse, qui s'inspire notamment des travaux de *Jaron Lanier* aux États-Unis, croise par ailleurs en France des positions défendues côté académique par *Pierre Bellanger*[34].

Comme le formulent *Lucas Léger* et *Pierre Bentata* dans leur rapport pour *Génération Libre*, « nier un droit de propriété sur les données revient à interdire aux internautes de les vendre, mais aussi à leur ôter toute possibilité de les protéger en faisant le choix d'un autre moyen de paiement »[35].

Le RGPD accorde des droits d'usage et de possession, mais pas de véritable propriété. Cette différence est juridiquement et économiquement fondamentale. Cette approche ne fait pas l'unanimité. Une partie de la doctrine, attachée à la conception personnaliste héritée de la loi de 1978, y voit un risque de marchandisation contraire à la dignité de la personne.

[32] Gérard Peliks, Virginie Pez, Nicolas Binctin, Isabelle Landreau, *Mes Data sont à moi*, *Génération Libre*, janvier 2018.
[33] Génération Libre, *Mes datas sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018.
[34] Pierre Bellanger, *La souveraineté numérique*, *Paris, Stock*, 2014.
[35] Lucas Léger et Pierre Bentata, *Aux data, citoyens ! Pour une libération des données personnelles*, *rapport pour Génération Libre*, 2019.

Génération Libre assume au contraire la voie propriétariste : comme l'écrivent *Léger et Bentata*, « la patrimonialité introduit un prix individualisé de l'usage de la donnée », condition d'une responsabilisation effective des acteurs et d'une protection ancrée dans l'autonomie individuelle plutôt que dans la tutelle technologique. Dans le modèle de propriété privée des données personnelles défendu par *Génération Libre*, les individus recourraient à des intermédiaires privés de la donnée qui géreraient à la fois la valeur de leurs données personnelles et qui offriraient par les instruments contractuels une propriété de leurs données comme bien à part entière. Face au modèle de la conformité réglementaire, *Génération Libre* propose l'efficacité d'acteurs en concurrence sur un marché pour s'assurer de l'effectivité du droit de propriété.

B. Application au problème des fuites de données

Dans un régime de propriété des données, une fuite ne serait plus un simple manquement administratif, mais une atteinte à un bien appartenant à l'individu. Les conséquences seraient transformées :

1. D'abord, la responsabilité civile s'exerce directement. Dès lors que mes données sont un bien et qu'une entreprise les perd par négligence, je peux demander réparation comme pour tout bien détruit ou volé. La charge de la preuve s'inverse au passage : c'est à l'entreprise de démontrer qu'elle a pris toutes les précautions nécessaires. Les entreprises intermédiaires de la donnée auraient une incitation très forte avec à faire respecter ce bien pour leurs clients : l'usager contracte avec elles pour valoriser et sécuriser ses données.
2. Les incitations économiques basculent ensuite. Face au risque d'actions de groupe et d'indemnisations massives, les entreprises ont intérêt à investir dans la cybersécurité avant qu'une fuite ne survienne. L'assurance cyber devient alors un mécanisme central, avec des primes calibrées sur le niveau réel de protection. Le marché américain de la cyber insurance en offre déjà l'illustration : les assureurs y imposent des standards techniques (authentification multifacteur, chiffrement, sauvegardes hors ligne) comme conditions de couverture, et produisent ainsi une incitation à la sécurité que la réglementation seule ne parvient pas à créer[36].
3. La relation entre individu et entreprise se contractualise par ailleurs. La gestion des données reposerait sur des contrats explicites définissant les usages autorisés, les niveaux de sécurité garantis et les responsabilités en cas de manquement. L'internaute retrouverait une maîtrise pleine et entière de ses données et pourrait en contractualiser l'usage : céder ses données contre rémunération, ou refuser la collecte en payant pour le service.
4. Le cadre devient enfin, paradoxalement, plus clair pour les entreprises. Ce régime de responsabilité accrue offrirait aux acteurs économiques une sécurité juridique supérieure à celle du RGPD, qui fait peser la menace d'une hyper-judiciarisation d'internet pouvant entraîner un blocage de l'innovation[37]. À l'inverse, un contrat de cession de données définit précisément ce qui est autorisé : l'entreprise qui respecte les termes négociés dispose d'une base juridique solide pour exploiter les données acquises. Plus de responsabilité, mais aussi plus de liberté d'action sur les données légitimement obtenues.

[36] Marsh et Microsoft, *By the Numbers: Global Cyber Risk Perception Survey*, février 2018, p. 10-11.
[37] Édouard Fillias, « *Face aux GAFA, nos données sont notre liberté* », tribune pour *Marianne*, juin 2019.

Le système actuel, où le consentement RGPD (basé sur des CSV quasiment illisibles) peut être retiré à tout moment et où les règles d'interprétation évoluent au gré des décisions de la CNIL, génère une incertitude permanente qui pénalise les acteurs économiques sans véritablement protéger les individus.

Comparaison : modèle RGPD actuel vs. propriété des données

	Modèle RGPD actuel	Propriété des données
Nature du droit	Droit d'usage et de contrôle	Droit de propriété patrimonial
Responsabilité en cas de fuite	Amende administrative (à l'État) et recours limité pour la victime	Indemnisation directe (aux victimes)
Charge de la preuve	Victime doit prouver le préjudice	Entreprise doit prouver sa diligence
Incitation à la sécurité	Risque d'amende plafonnée	Risque d'indemnisation illimitée + assurance
Sécurité juridique entreprise	Règles interprétées au fil de la jurisprudence	Contrat définissant précisément les droits cédés
Monétisation	Extraction gratuite par les plateformes	Rémunération possible de l'individu

C. Esquisse d'un cadre législatif

Pour passer du principe à la mise en œuvre, *Génération Libre* propose les premières étapes d'une réforme législative articulant trois piliers :

Premier pilier : consacrer un droit de propriété sur les données personnelles.
Un nouvel article du Code civil, dans la continuité logique de l'article 544, établirait que toute personne physique dispose d'un droit de propriété sur les données à caractère personnel qu'elle génère tel que décrit dans le premier rapport de *Génération Libre* sur la question[38]. Le générateur de la donnée personnelle est le propriétaire de ces données par le choix d'usage grâce à son consentement spécifique. Le choix du Code civil n'est pas indifférent. Loger ce droit dans le Code de la consommation le cantonnerait à la seule relation entre un consommateur et un professionnel, alors que les fuites concernent aussi les administrations, les associations, les employeurs ou les collectivités locales. Construire un régime *sui generis* dédié aux données réclamerait des années de jurisprudence pour stabiliser ses contours et risquerait de mal s'articuler avec les régimes voisins (responsabilité civile, contrat, propriété intellectuelle). À l'inverse, l'article 544 offre depuis 1804 un cadre éprouvé, intelligible des juges comme des justiciables, et immédiatement compatible avec l'ensemble des mécanismes du droit privé : preuve, prescription, succession, démembrement, action en revendication. Y rattacher les données personnelles, c'est leur appliquer une grammaire juridique déjà partagée plutôt que d'en inventer une nouvelle. Ce droit serait inaliénable mais cessible par contrat à durée déterminée, sur le modèle d'une licence. Une fois propriétaire, l'individu dispose des outils du droit civil pour défendre son bien sans recourir à une autorité administrative.

[38] Gérard Peliks, Virginie Pez, Nicolas Binctin, Isabelle Landreau, *Mes Data sont à moi*, *Génération Libre*, janvier 2018.

Deuxième pilier : ouvrir le droit à réparation intégrale.

L'action de groupe en matière de données personnelles, qui demeure cependant marginale en France, trouverait un terrain plus favorable avec une perspective de la reconnaissance d'un droit de propriété plein et entier, donnant accès à des sanctions classiques attachées au régime du bien. Ce mécanisme permettrait aux victimes de fuites d'obtenir une indemnisation directe, là où le système actuel ne rétribue que l'État. Le risque contentieux créerait en retour une incitation économique puissante : les entreprises auraient naturellement intérêt à investir dans la cybersécurité et à souscrire des assurances cyber dont les primes seraient calibrées sur le niveau réel de protection. Ce mécanisme de marché est déjà à l'œuvre aux États-Unis, où les assureurs imposent des standards techniques (MFA, chiffrement, tests d'intrusion) comme conditions de couverture[39].

Troisième pilier : simplifier la conformité réglementaire en utilisant un des droits les plus anciens : le droit de propriété.

Le régime de propriété ne se substitue pas intégralement au RGPD (qui nécessite des ajustements au niveau européen) : les droits fondamentaux des personnes, les obligations de sécurité minimale et l'existence d'une autorité de contrôle indépendante sont conservés. En revanche, dès lors que la relation entre l'individu et l'entreprise repose sur un contrat définissant précisément les usages autorisés et les niveaux de sécurité garantis, une part significative de l'appareil bureaucratique du RGPD devient redondante : registres de traitement systématiques, analyses d'impact obligatoires, désignation d'un DPO pour les structures de taille intermédiaire, formalisme du consentement réitéré. La liberté contractuelle offrirait aux entreprises une sécurité juridique supérieure à l'incertitude actuelle, tout en exposant directement aux tribunaux celles qui manquent à leurs engagements.

Le régime de propriété vient renforcer le contrôle sur ses données à caractère personnel déjà amorcé dans l'article 20 du RGPD. Cette liberté contractuelle est aussi en droite ligne avec le Data Act et le Data Gouvernance Act, qui confirme le marché de la donnée.

Dans ce contexte, l'instrument qu'offre la propriété pour le citoyen, devient encore plus pertinent contre les usages illégaux de données à caractère personnel.

[39] Cf. supra, note 35 (Marsh / Microsoft, Global Cyber Risk Perception Survey ; GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, juin 2022).

CONCLUSION : DE LA CONFORMITÉ À LA RESPONSABILITÉ

Huit ans après son entrée en vigueur, le RGPD a démontré ses limites. Il a créé un cadre administratif complexe, mais n'a pas enrayé l'explosion des fuites de données. Il a permis de sanctionner des entreprises, mais n'a pas protégé les citoyens. Le modèle actuel repose sur une fiction : l'État, via la CNIL, serait capable de protéger les données de 68 millions de Français dispersées dans des millions de systèmes d'information. Cette prétention est techniquement impossible.

Ainsi, la proposition de *Génération Libre* invite à un changement de paradigme : passer d'une logique de régulation bureaucratique à une logique de propriété et de responsabilité. La protection réelle ne peut venir que de trois sources complémentaires : les incitations économiques (le coût de l'insécurité doit être supérieur au coût de la sécurité), la responsabilité juridique (les entreprises doivent être responsabilisées et non contrôlées), et le pouvoir des individus (chacun doit pouvoir agir directement pour défendre ses intérêts).

Ce changement de paradigme est d'autant plus urgent que de nouvelles surfaces d'attaque se profilent. L'Assemblée nationale a adopté en première lecture, dans la nuit du 26 au 27 janvier 2026, une proposition de loi visant à interdire l'usage des réseaux sociaux aux moins de 15 ans ; le Sénat a modifié ce texte le 31 mars 2026 et la navette parlementaire se poursuit[40]. Pour l'appliquer, il faudra vérifier l'âge de tous les utilisateurs, et parmi les pistes envisagées figure le recours à l'application France Identité, adossée à la carte d'identité électronique. Autrement dit, au moment même où l'État peine à protéger nos numéros de sécurité sociale et nos adresses, il s'apprête à centraliser les documents d'identité officiels de plus de 50 millions d'internautes (Baromètre numérique CREDOC/ARCEP) dans des circuits de vérification supplémentaires : autant de nouvelles cibles pour les attaquants. Un pays incapable d'empêcher l'extraction de 13 millions de fiches en une journée est-il vraiment prêt à piloter l'identité numérique de toute sa population ?

Points clés à retenir :

- Les fuites de données explosent malgré le RGPD : 24 fuites/jour en 2025, soit +50 % vs 2024 (16/jour) ;
- Les sanctions vont à l'État, pas aux victimes ;
- La conformité juridique ne garantit pas la sécurité technique ;
- Un droit de propriété créerait des incitations économiques à la sécurité.

[40] Assemblée nationale, *Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*, adoptée en première lecture le 26 janvier 2026 (T.A. n° 217), texte modifié par le Sénat le 31 mars 2026. Voir Les Électrons Libres, op. cit. (note 31).

ANNEXE - LISTE DES FUITES MAJEURES EN 2024-2026 (NON-EXHAUSTIVE)

Sources détaillées en note de bas de page[41].

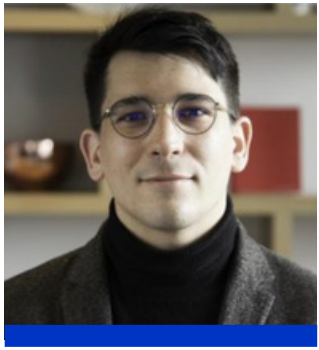
Organisation	Dates	Données concernées	Personnes touchées
France Titres (ex-ANTS)	Avril 2026	Identité, email, date de naissance, identifiant de connexion	11,7 millions
Basic-Fit	Avril 2026	Identité, coordonnées bancaires	1 million
Cegedim Santé (MLM)	Fév. 2026	Identité, coordonnées, annotations médicales sensibles (164 000)	11 à 15 millions
Pass'Sport (Min. Sports)	Déc. 2025	Identité, coordonnées, bénéficiaires Pass'Sport	3,5 millions (foyers)
Bouygues Telecom	Août 2025	Identité, coordonnées, IBAN	6 millions
Free	Oct. 2024	Identité, IBAN (5,1M), coordonnées	24 millions (contrats)
Molotov TV	Oct. 2024	Email, identité, date de naissance	10,8 millions
SFR	Sept./Nov. 2024	Identité, coordonnées, IBAN (50k)	3,6 millions
Boulanger	Sept. 2024	Adresse de livraison, email, téléphone	~27 millions (lignes)
Cultura	Sept. 2024	Identité, email, téléphone, achats	1,5 million
France Travail	Mars 2024	Identité, NIR, coordonnées, identifiants	36,8 millions
Viamedis / Almerys	Fév. 2024	État civil, NIR, assureur santé, garanties	33 millions

[41] Sources du tableau :
– France Titres (ex-ANTS) : Franceinfo, « *Fuite de données sur le portail de l'ANTS : près de 12 millions de comptes concernés, annonce le ministère de l'Intérieur* », 21 avril 2026.
– Basic-Fit : CNEWS, « *Basic-Fit piraté : 1 million de membres touchés* », 14 avril 2026.
– Cegedim Santé (MLM) : *Caducee.net*, « *Incident MLM chez Cegedim : anatomie d'une fuite de données estimée à 11-15 millions de dossiers patients* », février 2026.
– Pass'Sport (Min. Sports) : Franceinfo, « *Le ministère des Sports victime d'une cyberattaque : 3,5 millions de foyers concernés* », 19 décembre 2025.
– Bouygues Telecom : Le Monde, « *Six millions de comptes clients Bouygues Telecom touchés par une cyberattaque* », 6 août 2025.
– Free : CNIL, « *Délibérations SAN-2026-001 et SAN-2026-002 du 8 janvier 2026* ».
– Molotov TV : IT-Connect, « *Cyberattaque Molotov TV : fuite de données 2024* », octobre 2024.
– SFR : Le Monde Informatique, « *Plus de 3,6 millions de données clients de SFR vendues sur le dark web* », novembre 2024.
– Boulanger : L'Usine Digitale, « *Boulanger victime d'une fuite de données : des millions de Français concernés* », septembre 2024.
– Cultura : Franceinfo, « *Cultura victime d'une cyberattaque : les données de 1,5 million de clients dérobées* », septembre 2024.
– France Travail : CNIL, « *Délibération SAN-2026-003 du 22 janvier 2026* ».
– Viamedis / Almerys : CNIL, « *Communiqué du 7 février 2024* ».

L'AUTEUR

Grégory Lenne

Grégory est conseiller stratégique pour l'équipe dirigeante. Diplômé de l'école polytechnique et de Sciences Po, titulaire d'un master de philosophie politique sur le libéralisme de Hayek, Gregory travaille actuellement dans le conseil stratégique pour de grandes entreprises.



ACTIONS

Génération Libre est un think-tank indépendant qui vise à promouvoir les libertés. Toutes les libertés.

Le combat de Génération Libre.

Nos objectifs.

1. **Vivre et laisser vivre,** pour permettre à chacun de définir ses propres valeurs dans une société ouverte.

2. **Briser les rentes,** parce que la libre concurrence des échanges comme des idées est le meilleur moyen de contester l'ordre établi.

3. **Penser le progrès,** pour que les innovations technologiques demeurent au service de l'individu.

GENERATION LIBRE
THINK TANK

Soutenir de nouvelles idées.

Génération Libre est un think tank libéral fondé en 2013. Le think tank propose une nouvelle approche pour mener ses projets d'influence pour disséminer et faire la pédagogie les idées de liberté en France. Son financement repose exclusivement sur la générosité de ses donateurs, seule garantie de sa liberté de ton et de son indépendance. Il refuse toute subvention publique et n'effectue aucune activité de conseil.

Nous écrire, nous rencontrer.

www.generationlibre.eu