545 000 usagers : la région qui sous-traitait sa fuite

Le 3 octobre 2026, la Région Hauts-de-France a annoncé que deux prestataires, Atexo et Docaposte, avaient laissé fuir des données « traitées pour son compte ». Le droit est clair : la Région externalise le traitement, mais elle reste responsable de la fuite. Cette chronique soutient que l'incident ne vient pas de nulle part. Il clôt une période d'incubation, au sens de Barry Turner, ouverte un an plus tôt par l'attaque contre les lycées. Pendant ce temps, la collectivité a renforcé son propre périmètre et laissé grossir, chez ses prestataires, un stock de comptes dont aucune règle publique ne fixe la durée de vie.

Par Alexandre Berge · 12 octobre 2026 · 18 min de lecture · Chronique

Sous-traiter sa fuite, ce que le droit appelle encore une responsabilité

Le samedi 3 octobre 2026, la Région Hauts-de-France a indiqué à l'AFP que deux de ses prestataires, Atexo et Docaposte, avaient été « victimes d'une cyberattaque ayant permis un accès non autorisé à des données personnelles traitées pour son compte ». Selon la dépêche reprise par Techniques de l'Ingénieur, des noms, des prénoms, des adresses électroniques, « ainsi que potentiellement des RIB et d'autres données d'identification », figuraient parmi les données susceptibles d'avoir été compromises. La Région a déposé plainte et fermé les plateformes touchées. D'après Next, Atexo gérait la plateforme des aides régionales et Docaposte la carte Génération #HDF, par laquelle la Région verse une aide aux lycéens et aux apprentis. La collectivité ajoutait que « les prestataires ont identifié les failles ainsi que le mode opératoire de l'attaquant et engagé les travaux de correction ».

Le lundi 5 octobre, en séance plénière, Xavier Bertrand a donné un premier bilan : près de 545 000 personnes. Côté Atexo, les données « d'un maximum de 515 000 personnes sur les 745 000 enregistrées sur la plateforme » ont fuité, à savoir « noms, prénoms, mails, type de tiers, habilitations ». Il n'était pas encore établi si les RIB avaient « été consultés et ont pu être extraits ». Côté Docaposte, les données de près de 30 000 bénéficiaires et partenaires de la carte Génération #HDF « auraient fuité ». Il s'agirait surtout de contrats d'apprentissage et de RIB.

Le titre de cette chronique parle d'une région qui **sous-traite sa fuite**. L'expression désigne une situation précise. Une collectivité confie l'exécution d'un traitement à un tiers, mais garde

la qualité de *responsable de traitement* (l'entité qui fixe les finalités et les moyens du traitement, au sens de l'article 4 du RGPD). Elle externalise donc le risque technique sans pouvoir externaliser la responsabilité juridique. L'article 28 du RGPD oblige le responsable à ne faire appel qu'à des sous-traitants « qui présentent des garanties suffisantes ». Il impose aussi que le contrat permette « la réalisation d'audits, y compris des inspections ». La CNIL a précisé la répartition des rôles dans un scénario publié le 27 mai 2026, consacré au sous-traitant victime d'une cyberattaque. Le prestataire doit informer « le plus rapidement possible les responsables de traitement concernés ». La notification à l'autorité et, en cas de risque élevé, l'information des personnes restent des obligations du donneur d'ordre. La CNIL rappelle ailleurs que le responsable doit « rester maître de la décision de notifier ».

La formule employée par la Région, des données « traitées pour son compte », est donc juridiquement exacte. Elle est aussi révélatrice. Elle situe la fuite chez les prestataires alors que la responsabilité, elle, ne quitte pas l'hôtel de région. Sous-traiter sa fuite, ce n'est pas s'en décharger. C'est la laisser se préparer dans un endroit que la collectivité ne voit pas.

545 000, 708 068, 745 000 : le vrai chiffre est celui du stock

Les chiffres circulent dans un ordre qui brouille la lecture. Le 3 octobre, la Région ne pouvait pas donner « le nombre exact de personnes concernées ». Le site FrenchBreaches, cité par l'AFP, faisait état d'un pirate qui revendiquait plus de 700 000 personnes. Clubic a précisé le 4 octobre que le pseudonyme ChimeraZ revendiquait une base de 782 583 lignes, dans laquelle apparaîtraient 708 068 personnes. Il revendiquait aussi un second ensemble de 48 Go et 90 011 fichiers PDF. Selon les mêmes revendications, rapportées par Clubic, ces fichiers contiendraient 36 720 RIB, 37 585 contrats d'apprentissage et 15 118 attestations d'hébergement. Aucun de ces chiffres n'a été validé par la collectivité, qui déclarait : « Nous ne sommes pas en mesure aujourd'hui de confirmer le volume et d'autres catégories de documents extraites ». Clubic relève un autre écart : le courrier envoyé aux usagers ne mentionnait que leur identité et leur adresse électronique.

L'AFP signale enfin un détail absurde. Dans la dépêche du 3 octobre reprise par CNews et Planète Grandes Écoles, le pirate revendique aussi des données de réservation de Gîtes de France allant de 1995 à 2026. Ce n'est qu'une revendication, que rien ne confirme. Aucun lien entre Gîtes de France, Atexo et la Région n'apparaît dans les sources consultées. En mai 2026, Gîtes de France avait d'ailleurs reconnu un vol de données lié à son prestataire Itea, et le pirate revendiquait alors déjà la même plage de 1995 à 2026, selon CNews et France 3 Occitanie. Le plus probable est donc un catalogue de butins mélangés, où une collectivité régionale côtoie trente ans de séjours à la campagne. L'anecdote dit au moins une chose : pour qui revend des données, le temps de conservation fait partie de la marchandise.

Le chiffre le plus instructif n'est ni 545 000 ni 708 068. C'est 745 000, le nombre de personnes « enregistrées sur la plateforme » d'Atexo selon Xavier Bertrand. Ce nombre mesure

un stock, pas un incident. La Région publie, sur les pages de protection des données de ses téléservices, des *durées d'utilité administrative* (la période pendant laquelle un document reste utile au service avant archivage définitif ou destruction). Elles sont raisonnées par dossier : dix ans pour une demande d'aide financée, deux ans si le financement a été refusé, et, en cas de cofinancement européen, « 3 ans après la fin période de validité du règlement européen – soit en moyenne, un maximum de 13 ans », selon la page de protection des données de hautsdefrance.fr. L'article 5 du RGPD exige pourtant que les données soient conservées « pendant une durée n'excédant pas celle nécessaire au regard des finalités ». Dans les pages consultées, la durée de vie d'un compte de tiers ne figure nulle part. Il s'agit pourtant de l'unité qu'énumère le bilan officiel : nom, mail, type de tiers, habilitations. Le danger ne tient pas d'abord à l'intrusion. Il tient à ce que l'intrusion a trouvé.

> **Extrait de source : ce que la Région publie sur la conservation**
>
> La page « Protection des données personnelles et Cookies » du site Génération #HDF (modifiée le 15 septembre 2026) fixe les principales durées d'utilité administrative de la Région : « demande d'information auprès de la Région : 2 ans », « demande d'aide régionale sans cofinancement européen : 10 ans pour un dossier ayant fait l'objet d'un financement, 2 ans si le financement a été refusé ». Pour le reste, elle renvoie à une information donnée « au moment de la collecte ». La seule durée chiffrée propre à ce site est celle d'un cookie de mesure d'audience : un an.

Octobre 2025 : l'incubation commence par un leurre

Un an avant la fuite, le 10 octobre 2025, le système d'information des lycées publics de la région était frappé par le rançongiciel Qilin. La Région indiquait alors que « près de 80 % des lycées publics de la région » étaient touchés. Dans un communiqué du 16 octobre 2025, elle reconnaissait « un accès non autorisé à certaines données personnelles concernant potentiellement des élèves, leurs familles et des personnels ». Elle précisait que la violation avait été notifiée à la CNIL. Le 20 novembre 2025, Xavier Bertrand annonçait en plénière un investissement de « plusieurs millions d'euros » pour sécuriser les systèmes d'information, montant que France 3 Hauts-de-France a chiffré le 11 décembre 2025 à 22,5 millions d'euros (3,25 millions engagés le 27 novembre, puis 19,25 millions votés en commission permanente), dont « 10 millions d'euros » pour le « renouvellement des équipements informatiques arrivés à échéance ». Il ajoutait : « ce n'est ni la première ni la dernière fois que nous subirons ce type de cyberattaques ». Aucun lien technique n'a été établi entre Qilin et la fuite d'octobre 2026, souligne Clubic. Le rapprochement entre les deux épisodes est organisationnel, pas criminel.

C'est précisément ce que permet de penser Barry Turner. Ce sociologue britannique a étudié les rapports d'enquête publics consacrés à des catastrophes industrielles. Il en a tiré un modèle séquentiel, présenté en 1976 dans l'*Administrative Science Quarterly* puis développé en 1978 dans *Man-Made Disasters*. Ce modèle ne cherche pas le composant défaillant. Il

cherche pourquoi une organisation n'a pas vu venir ce qu'elle avait les moyens de voir.

> **Concept : la période d'incubation (Barry A. Turner, 1976 et 1978)**
>
> Dans « The Organizational and Interorganizational Development of Disasters » (*Administrative Science Quarterly*, vol. 21, n° 3, septembre 1976) et dans *Man-Made Disasters* (Wykeham Publications, 1978), Turner décrit les catastrophes comme des *échecs de prévoyance*. La séquence part d'un état jugé normal, passe par une période d'incubation, puis par un événement déclencheur, la survenue de la catastrophe, le sauvetage, et enfin un *réajustement culturel* complet. Le résumé de l'article de 1976 en donne la thèse : « Such features form part of the incubation stage in a sequence of disaster development, accumulating unnoticed until a precipitating event leads to the onset of the disaster and a degree of cultural collapse » (ces caractéristiques forment l'étape d'incubation d'une séquence de développement des catastrophes, et s'accumulent sans être remarquées jusqu'à ce qu'un événement déclencheur provoque la catastrophe et un certain effondrement culturel). Parmi ces caractéristiques, Turner range les *phénomènes leurres*, la négligence des alertes extérieures, les difficultés de circulation de l'information, l'aggravation des risques par des « étrangers » au système et la tendance à minimiser le danger qui émerge.

Appliqué au cas, le modèle a un effet précis. Il ne fait pas de l'attaque des lycées la cause de la fuite. Il en fait le moment où la Région a choisi ce qu'elle regardait. Le premier mécanisme est le *phénomène leurre* (un problème visible et urgent qui détourne l'attention d'un danger moins visible). En 2025, la crise portait sur le parc informatique interne : 269 lycées publics à remettre en état, selon le point de situation régional du 31 octobre 2025, et 70 000 ordinateurs pédagogiques sur 100 000 retraités au 20 novembre, selon le vice-président Laurent Rigaud cité par Incyber. Le réajustement s'est logiquement concentré sur ce périmètre. Le 3 octobre 2026, la Région insistait encore sur le fait que son « système d'information interne » n'avait pas été touché. La phrase est vraie. Elle montre aussi où se trouvait le leurre : le risque avait déménagé hors les murs, chez les éditeurs des téléservices.

Le deuxième mécanisme est l'aggravation par des étrangers. Turner désigne ainsi les personnes extérieures à l'organisation, présentes sur le site et qui ne partagent pas ses règles de prudence. Une plateforme d'aides ouverte à 745 000 tiers en est la version numérique. Une revendication relayée par Clubic, invérifiable mais parlante, affirme que des usagers auraient saisi leur mot de passe dans le champ du numéro de téléphone. Le troisième mécanisme tient aux difficultés de circulation de l'information. En trois jours, la Région, les prestataires, FrenchBreaches et la presse ont fait circuler des périmètres incompatibles. Les rattachements de plateformes eux-mêmes divergent entre la version officielle et les revendications. Le quatrième est la minimisation : le 3 octobre, la Région déclarait l'incident « désormais résolu », alors qu'elle ignorait encore combien de personnes étaient touchées et si les RIB avaient été extraits.

L'incubation, chez Turner, n'est pas une fatalité. C'est une accumulation qui reste invisible parce que les catégories de l'organisation ne la saisissent pas. Ici, la catégorie dominante était « notre système d'information ». Les comptes de tiers hébergés par Atexo et les RIB d'apprentis conservés par Docaposte n'en relevaient pas.

France Travail, le précédent qui avait déjà tout écrit

Parmi les antécédents possibles, l'affaire France Travail de 2024 est structurellement la plus proche. Au premier trimestre 2024, des attaquants ont usurpé des comptes de conseillers de Cap Emploi, c'est-à-dire de partenaires extérieurs habilités à accéder au système de l'opérateur. Selon la CNIL, ils ont ainsi atteint les données de toutes les personnes inscrites ou l'ayant été « au cours des 20 dernières années ». Le 22 janvier 2026, la formation restreinte a prononcé une amende de 5 millions d'euros. Elle a relevé des modalités d'authentification insuffisamment robustes, une journalisation insuffisante et des habilitations définies de manière trop large. Dans sa délibération, elle souligne que la violation portait sur vingt ans d'inscrits, une durée fixée à l'époque par le code du travail et depuis réduite.

Trois traits rapprochent les deux cas : un organisme public, un accès passé par des tiers, et un stock historique qui démultiplie la fuite. Un quatrième trait est le plus utile pour lire la séquence de Turner. Pour fixer la sanction, la CNIL a tenu compte du fait que « la plupart des mesures de sécurité adéquates avaient été identifiées par FRANCE TRAVAIL, en amont de la mise en œuvre du traitement, dans les analyses d'impact, sans pour autant avoir été effectivement mises en œuvre ». Le savoir existait, mais l'organisation ne l'avait pas converti en action. C'est presque mot pour mot ce que Turner appelle un échec de prévoyance.

Le précédent indique aussi le calendrier. France Travail a notifié la violation le 8 mars 2024, et la sanction est tombée le 22 janvier 2026, un peu plus de vingt-deux mois plus tard. Pour un organisme public, la CNIL précise que le plafond de l'amende pour un manquement à la sécurité ne peut dépasser 10 millions d'euros. L'incident Viamedis et Almerys de février 2024 a fixé l'autre versant de la doctrine. Selon la CNIL, le 7 février 2024, cette fuite « concerne plus de 33 millions de personnes », et l'autorité a rappelé qu'il appartenait « à chacune des complémentaires santé faisant appel aux prestataires Viamedis et Almerys », et non au seul prestataire, d'informer les personnes. Le responsable de traitement ne disparaît pas derrière son sous-traitant.

Ce cas s'inscrit enfin dans une série. Le gouvernement reconnaissait le 30 avril 2026, selon la question écrite n° 17888 publiée au Journal officiel du 1er septembre 2026, que la France enregistrait « en moyenne trois vols de données par jour ». Le premier point de situation de l'ANSSI, publié le 30 septembre 2026 et rapporté par Acteurs publics, recense 99 violations de données portées à sa connaissance depuis le 1er août. Le cas des Hauts-de-France ne se distingue pas par sa taille. Il se distingue par sa forme : une collectivité territoriale, une chaîne de plateformes d'aides et un stock dont la durée n'est pas publique. Les chroniques

précédentes sur FICOBA ou l'ANTS portaient sur des fichiers d'État et sur des accès délégués.

L'angle mort : la durée de vie d'un compte de tiers

Le discours officiel parle de prestataires victimes, de failles corrigées et de plateformes fermées. Il ne parle pas de deux choses. La première est la règle qui fait sortir un tiers de la base. Les durées publiées par la Région suivent la logique archivistique du dossier d'aide. Un compte créé pour une demande refusée, ou pour une carte Génération #HDF d'un apprenti aujourd'hui salarié, ne relève visiblement d'aucune des lignes du tableau publié. Sur les pages consultées le 8 octobre 2026, ni le site Génération #HDF ni la page générale de protection des données de la Région ne fixent de durée pour les comptes inactifs, les RIB ou les contrats d'apprentissage. Aucune ne nomme les sous-traitants : la Région renvoie aux « éventuels autres destinataires » mentionnés « lors de la collecte ». Les mentions propres aux plateformes Atexo et Docaposte n'ont pas pu être consultées, puisque ces plateformes sont fermées depuis le 3 octobre.

La seconde est le contenu des contrats. L'article 28 du RGPD fait de l'audit du sous-traitant une faculté contractuelle du responsable. Rien de ce qui a été rendu public depuis le 3 octobre n'indique si la Région a audité Atexo ou Docaposte, à quelle fréquence, ni si les marchés imposaient une purge des comptes. L'effet de chaîne est pourtant visible ailleurs. Le syndicat Mégalis Bretagne, qui utilise des solutions du même éditeur, a dû préciser sur son portail que la cyberattaque visait « une application de gestion de subventions » et qu'« aucune application » utilisée par ses usagers n'était concernée. Atexo revendique sur son site « + de 200 grands comptes publics (Etats, régions…) » et, pour sa plateforme de subventions, « + d'un million de bénéficiaires », et chaque collectivité responsable de traitement découvre l'étendue de sa dépendance au moment de la fuite.

Cet angle mort n'est pas propre à la Région. Il tient à une division du travail. La conservation se pense en archiviste, par dossier. La sécurité se pense en RSSI, par périmètre. Le contrat se pense en acheteur, par lot. Le compte de tiers inactif, chez un éditeur, ne relève d'aucun des trois.

Le réajustement aura-t-il lieu dans un cahier des clauses ?

Le titre posait un paradoxe : une région qui sous-traite sa fuite. L'analyse en précise les termes. La Région a sous-traité le traitement, pas la responsabilité. Elle a surtout sous-traité l'endroit où son stock vieillissait. Lue avec Turner, la séquence est cohérente. L'attaque d'octobre 2025 était un signal. Le réajustement qui a suivi a porté sur le périmètre interne, ce qui en a fait un leurre. Le 3 octobre 2026 a été l'événement déclencheur. Reste la dernière étape du modèle, le réajustement culturel complet. Turner le voit comme le moment où un problème mal structuré entre enfin dans les catégories de l'organisation.

Cette lecture conduit à une hypothèse vérifiable. Si le réajustement porte cette fois sur la

chaîne de sous-traitance, deux documents publics devraient apparaître avant le 31 décembre 2027. Le premier est une durée de conservation explicite des comptes de tiers et des pièces bancaires dans les mentions d'information des plateformes d'aides et de la carte Génération #HDF, à leur réouverture. Le second est une clause d'audit de sécurité et de purge dans le prochain avis de marché régional sur la gestion des subventions, publié au BOAMP. Si, au 31 octobre 2028, la CNIL n'a publié ni sanction, ni mise en demeure rendue publique, ni clôture de contrôle visant la Région ou ses prestataires, il faudra en conclure autre chose. Ce délai correspond à environ vingt-quatre mois après les faits, l'ordre de grandeur observé pour France Travail. Dans ce cas, la doctrine du responsable de traitement aura fonctionné pour un opérateur d'État mais pas pour une collectivité. La question n'est plus de savoir si la Région aurait pu prévoir. Elle est de savoir si l'institution apprendra à regarder là où elle a placé ses données.

Note méthodologique

L'article s'appuie sur les dépêches AFP des 3 et 5 octobre 2026, sur les communiqués régionaux d'octobre et novembre 2025, sur les publications de la CNIL et sur les deux textes de Turner. Les chiffres divergent selon les sources publiques. Le bilan officiel est de 545 000 personnes. Le pirate revendique plus de 700 000 personnes selon l'AFP, et 708 068 personnes dans 782 583 lignes selon Clubic. Le bilan officiel est retenu comme seule base, les revendications sont signalées comme telles. Les données de Gîtes de France sont présentées comme une revendication non confirmée, sans lien établi avec la Région. Les affirmations d'absence se limitent aux pages consultées le 8 octobre 2026 : hautsdefrance.fr (page de protection des données), generation.hautsdefrance.fr et la presse indexée. Les mentions des plateformes fermées, les registres et les données essentielles de la commande publique n'ont pas pu être exploités. Le précédent France Travail a été retenu de préférence à Viamedis et Almerys parce qu'il réunit un organisme public, un accès par des tiers et un stock historique.

Sources

Sources primaires institutionnelles

- Région Hauts-de-France, « Communiqué de presse : cyberattaque contre le système d'information des lycées en Hauts-de-France, deuxième point de situation », 16 octobre 2025, https://www.hautsdefrance.fr/communique-de-presse-cyberattaque-contre-le-systeme-dinformation-des-lycees-en-hauts-de-france-deuxieme-point-de-situation/
- Région Hauts-de-France, « Communiqué de presse : cyberattaque contre le système d'information des lycées en Hauts-de-France, point de situation au 31 octobre 2025 », 1er novembre 2025, https://www.hautsdefrance.fr/communique-de-presse-cyberattaque-contre-le-systeme-dinformation-des-lycees-en-hauts-de-france-point-de-situation-au-31-octobre-2025/

- Région Hauts-de-France, « Protection des données personnelles et Cookies », site Génération #HDF, page modifiée le 15 septembre 2026, consultée le 8 octobre 2026, https://generation.hautsdefrance.fr/protection-des-donnees-personnelles-et-cookies/
- Mégalis Bretagne, « Portail des marchés publics, espace entreprise », consulté le 8 octobre 2026, https://marches.megalis.bretagne.bzh/entreprise
- Assemblée nationale, « Question écrite n° 17888 : Multiplication des cyberattaques et des fuites de données », publiée au Journal officiel le 1er septembre 2026, https://questions.assemblee-nationale.fr/q17/17-17888QE.htm

Textes normatifs et doctrine de l'autorité de contrôle

- Parlement européen et Conseil, « Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel » (RGPD), 27 avril 2016, articles 4, 5 et 28, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679
- CNIL, « Cyberattaque : le sous-traitant au centre de la crise », 27 mai 2026, https://www.cnil.fr/fr/cyberattaque-le-sous-traitant-au-centre-de-la-crise
- CNIL, « Violations de données personnelles : les règles à suivre », consulté le 8 octobre 2026, https://www.cnil.fr/fr/violations-de-donnees-personnelles-les-regles-suivre
- CNIL, « Violation de données : sanction de 5 millions d'euros à l'encontre de FRANCE TRAVAIL », 29 janvier 2026, https://www.cnil.fr/fr/violation-de-donnees-sanction-5millions-france-travail
- CNIL, formation restreinte, « Délibération SAN-2026-003 du 22 janvier 2026 prononçant une sanction pécuniaire à l'encontre de l'opérateur FRANCE TRAVAIL », 22 janvier 2026, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053408671
- CNIL, « Violation de données de deux opérateurs de tiers payant : la CNIL ouvre une enquête et rappelle aux assurés les précautions à prendre », 7 février 2024, https://www.cnil.fr/fr/violation-de-donnees-de-deux-operateurs-de-tiers-payant-la-cnil-ouvre-une-enquete-et-rappelle-aux

Cadres théoriques

- Barry A. Turner, « The Organizational and Interorganizational Development of Disasters », *Administrative Science Quarterly*, vol. 21, n° 3, 1er septembre 1976, p. 378 à 397, DOI 10.2307/2391850, notice consultée le 8 octobre 2026, https://www.semanticscholar.org/paper/The-Organizational-and-Interorganizational-of-Turner/30cc0359599216e7ce636f616444592a9a8a3b6e
- Barry A. Turner, *Man-Made Disasters*, Londres, Wykeham Publications, Wykeham Science Series n° 53, 1978, notice consultée le 8 octobre 2026, https://books.google.com/books/about/Man_made_Disasters.html?id=AjmwAAAAIAAJ

Presse (dépêches et enquêtes primaires)

- AFP, reprise par Techniques de l'Ingénieur, « Cybersécurité : la région Hauts-de-France victime d'une large fuite de données personnelles », 3 octobre 2026, https://www.techniques-ingenieur.fr/actualite/breves-afp/cybersecurite-la-region-hauts-de-france-victime-dune-large-fuite-de-donnees-personnelles-164416/
- AFP, reprise par Techniques de l'Ingénieur, « Cyberattaque dans les Hauts-de-France : plus de 500 000 personnes touchées, selon la région », 5 octobre 2026, https://www.techniques-ingenieur.fr/actualite/breves-afp/cyberattaque-dans-les-hauts-de-france-plus-de-500-000-personnes-touchees-selon-la-region-164436/
- AFP, reprise par France 24, « Cyberattaque dans les Hauts-de-France : plus de 500 000 personnes touchées, selon la région », 5 octobre 2026, https://www.france24.com/fr/info-en-continu/20261005-cyberattaque-dans-les-hauts-de-france-plus-de-500-000-personnes-touch%C3%A9es-selon-la-r%C3%A9gion
- CNews (dépêche AFP), « Cybersécurité : la région Hauts-de-France victime d'une large fuite de données personnelles », 3 octobre 2026, https://www.cnews.fr/vie-numerique/2026-10-03/cybersecurite-la-region-hauts-de-france-victime-dune-large-fuite-de
- France 3 Hauts-de-France, « La région Hauts-de-France victime d'une cyberattaque : des noms, prénoms, adresses électroniques et potentiellement des RIB parmi les données volées », 3 octobre 2026, https://france3-regions.franceinfo.fr/hauts-de-france/nord-0/la-region-hauts-de-france-victime-d-une-cyberattaque-des-noms-prenoms-adresses-electroniques-et-potentiellement-des-rib-parmi-les-donnees-volees-3427614.html
- Clubic, Mélina Loupia, « Une cyberattaque frappe les Hauts-de-France et expose potentiellement des RIB », 4 octobre 2026, https://www.clubic.com/actualite-632503-une-cyberattaque-frappe-les-hauts-de-france-et-expose-potentiellement-des-rib.html
- Next, Sébastien Gavois, « Fuite de données à la région Hauts-de-France, avec "potentiellement des RIB" », 5 octobre 2026, https://next.ink/brief-article/fuite-de-donnees-a-la-region-hauts-de-france-avec-potentiellement-des-rib/
- Planète Grandes Écoles, Baptiste Basillais, « Fuite de données en Hauts-de-France : 545 000 personnes concernées, ce que l'on sait », 6 octobre 2026, https://www.planetegrandesecoles.com/fuite-donnees-hauts-de-france-atexo-docaposte
- France 3 Hauts-de-France, « Cyberattaque dans les lycées : élèves, personnels, familles… leurs données potentiellement piratées dans les Hauts-de-France », 16 octobre 2025, https://france3-regions.franceinfo.fr/hauts-de-france/nord-0/lille/cyberattaque-dans-les-lycees-eleves-personnels-familles-leurs-donnees-potentiellement-piratees-dans-les-hauts-de-france-3234518.html
- Incyber News, « La région Hauts-de-France fait le point sur la cyberattaque contre ses lycées », compte rendu de la séance plénière du 20 novembre 2025, consulté le 8 octobre

2026, https://incyber.org/article/region-hauts-de-france-fait-point-sur-cyberattaque-contre-ses-lycees/

- CNews (dépêche AFP), « "La France est une passoire en matière de cybersécurité" : ce qu'il faut savoir de l'attaque visant Gîtes de France », 18 mai 2026, https://www.cnews.fr/france/2026-05-18/la-france-est-une-passoire-en-matiere-de-cybersecurite-ce-quil-faut-savoir-de
- France 3 Occitanie, « Cyberattaque massive chez Gîtes de France, près de 400 000 clients concernés par le vol de données », consulté le 8 octobre 2026, https://france3-regions.franceinfo.fr/occitanie/haute-garonne/toulouse/cyberattaque-massive-chez-gites-de-france-pres-de-400-000-clients-concernes-par-le-vol-de-donnees-troisieme-acteur-du-tourisme-hacke-en-3-jours-3352276.html
- Acteurs publics, Victoria Beurnez, « DGFiP : l'Anssi détaille les angles morts cyber de l'État », 30 septembre 2026, https://acteurspublics.fr/articles/cyberattaque-de-la-dgfip-lanssi-detaille-les-angles-morts-cyber-de-ladministration/