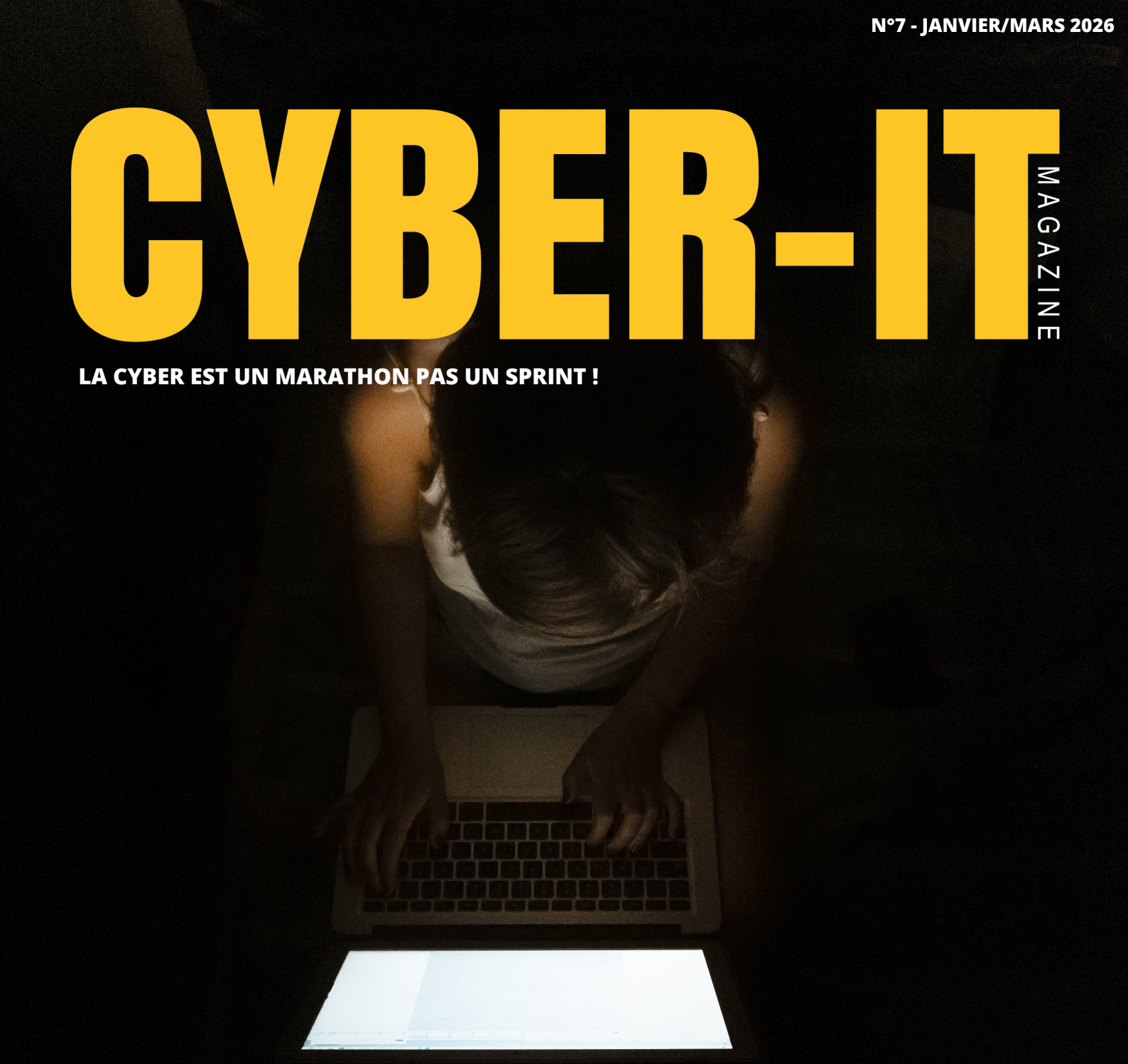
N°7 - JANVIER/MARS 2026

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !



DOSSIER SPECIAL

Données personnelles

Combien valent nos datas
et qui s'y intéresse ?

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Le choix du thème de ce numéro s'est progressivement imposé à la lumière des nombreuses fuites de données personnelles observées ces derniers mois. Il est difficile de ne pas éprouver un sentiment d'inquiétude à l'idée que nos informations puissent circuler librement, accessibles à des personnes mal intentionnées.

Il serait toutefois illusoire de nier notre propre responsabilité dans cette exposition. Par manque d'attention, nous acceptons souvent des conditions sans les lire, ou communiquons nos données en participant à des jeux ou en remplissant des questionnaires, parfois sans en mesurer les conséquences.

Nous verrons également que les outils de notre quotidien peuvent se transformer en véritables instruments de surveillance, à commencer par le smartphone. Nous nous intéresserons à ceux qui exploitent ces informations et ont fait de la donnée un modèle économique particulièrement lucratif.

Les données de santé occupent elles aussi une place centrale dans cette enquête. Plusieurs pistes ont été explorées, des témoignages recueillis, et des questions ont été portées jusqu'à l'Assemblée nationale.

Impossible enfin d'évoquer les fuites de données sans s'intéresser à la face la plus obscure d'Internet. Nous avons enquêté sur ces espaces où s'échangent et se concentrent d'innombrables informations sensibles.

Pour conclure, l'unité nationale cyber de la gendarmerie nous a exceptionnellement ouvert ses portes afin de mieux comprendre ses missions et son fonctionnement.

Bonne lecture et à très vite !

ARNAUD LEROY

SOMMAIRE

INTRO

DONNÉES PERSONNELLES

Florian Bayard
Journaliste 01Net

Journaliste depuis plus de huit ans, Florian traite des sujets d'actualité variés, aussi bien liés aux technologies du quotidien qu'à l'univers des cryptomonnaies.

Au fil de son parcours, il s'est spécialisé dans l'analyse des usages numériques et de leurs impacts. Aujourd'hui au sein de la rédaction de 01net, il s'attache à rendre les enjeux de la cybersécurité accessibles au plus grand nombre, en décortiquant de manière pédagogique les menaces qui pèsent sur Internet et sur les internautes.

Le fléau des fuites de données en France

Les fuites de données continuent de faire les gros titres en France. Entreprises, opérateurs, ministères... Personne n'échappe aux cybercriminels à la recherche d'informations sur les Français. On fait le point sur ce fléau. Pour rédiger cet intro de prévention à destination du grand public, je me suis appuyé sur mon expérience de journaliste spécialisé dans la cybersécurité chez 01net.

Ces dernières années, j'ai en effet consacré une partie de mes journées au suivi des fuites d'informations en France, y compris sur le dark web.

C'est quoi une donnée en fait ?

Une donnée désigne toute information concernant un internaute. Il s'agit tout d'abord de simples informations de contact, comme votre nom, notre prénom, votre adresse email, votre numéro de téléphone ou encore votre adresse postale.

Elles sont parfois accompagnées d'éléments plus sensibles, telles que des coordonnées bancaires (numéros de carte ou de compte IBAN), des mots de passe, l'historique médical, ou encore des données biométriques.

Celles-ci comprennent votre empreinte digitale, votre visage, ou encore votre iris. Mises bout à bout, les données permettent de dresser un portrait-robot très précis de qui vous êtes.

Qui détient vos données ?

Tous les services que vous utilisez, comme votre banque ou encore votre opérateur, collectent une montagne d'informations sur tous leurs clients, généralement au moment de l'inscription. En fait, une multitude d'organismes publics et privés est actuellement en possession d'informations sur votre compte.

C'est aussi le cas des réseaux sociaux, des moteurs de recherche, des boutiques en ligne, des administrations fiscales, des hôpitaux, de votre mutuelle et de votre employeur.

Trop souvent, des entités qui vous sont inconnues disposent également de vos données. Pourtant, vous n'avez pas communiqué d'informations à celles-ci.

C'est par exemple le cas des **data brokers** (courtiers en données), ces entreprises dont l'unique activité est la collecte et la revente de données à des fins publicitaires. Sans votre consentement clair, ces sociétés, dont le fonctionnement est généralement opaque, vont dresser votre profil publicitaire et le revendre à des marques ou des sociétés de marketing.

Malheureusement, vos données sont aussi entre les mains de **cybercriminels**. Sur des marchés noirs du dark web, les pirates s'échangent des répertoires composés de milliards de données concernant les internautes. Les données peuvent avoir été dérobées lors d'une cyberattaque ou durant une opération de « scraping » totalement légale.

Le « scraping » consiste à se servir d'un programme automatisé pour aspirer un océan de données accessibles publiquement, sur les réseaux sociaux par exemple

Pourquoi c'est de l'or pour les cybercriminels ?

Les données sont essentielles aux activités des pirates. Sans informations sur leurs cibles, ils ne peuvent tout simplement pas travailler. C'est grâce à vos coordonnées et à vos informations personnelles que les cybercriminels peuvent mettre au point des attaques personnalisées, susceptibles de vous berner.

Avec vos données, les pirates peuvent tout d'abord mettre au point des attaques de **phishing** très convaincantes. Une attaque phishing, ou hameçonnage en français, consiste à usurper l'identité de banques ou de services officiels pour aspirer des données.

En général, ces offensives cherchent à s'emparer de vos coordonnées bancaires... pour vider l'argent sur votre compte. Plus un message de phishing contient des données personnelles, plus il est susceptible d'être pris au sérieux.

Fort logiquement, vous ferez davantage confiance à un message portant votre nom, votre adresse postale, ou d'autres informations, qu'à une communication générique.

Citons aussi les risques d'**usurpation d'identité**. En utilisant toutes les données en sa possession, un cybercriminel peut tenter de se faire passer pour vous auprès d'une entité quelconque, comme une banque ou un opérateur. Il peut par exemple ouvrir une ligne de crédit à votre nom ou souscrire des abonnements en votre nom. Les possibilités sont presque infinies pour un pirate un peu débrouillard.

Les fuites de données en quelques chiffres

Les chercheurs de Surfshark, un VPN populaire basé à Vilnius, estiment que la France cumule environ **682,8 millions de comptes compromis depuis 2004**. La France fait d'ailleurs partie des pays les

plus touchés au monde. Les études de Surfshark montrent que la France s'est imposée comme le pays le plus touché par les violations de données au cours du 3e trimestre 2025, devant les Etats-Unis. En vérité, un compte français est piraté chaque seconde.

Environ 40 millions de comptes de Français ont été compromis au cours de l'année écoulée.

Quels secteurs sont les plus vulnérables ?

Au vu de la sensibilité des données en leur possession, les **établissements de santé** font partie des secteurs les plus touchés par les cybercriminels.

En mettant la main sur des informations médicales, les pirates espèrent en effet pousser leurs victimes à verser une rançon. C'est pourquoi les établissements médicaux sont progressivement devenus l'une des cibles principales des voleurs de données.

En France, **749 incidents ont été déclarés en 2024** au CERT Santé, l'équipe dédiée à la réponse aux incidents pour les systèmes d'information des établissements de santé et médico-sociaux en France.

Par ailleurs, les hôpitaux pèchent bien souvent par des mesures de sécurité insuffisantes, qui découlent d'un budget cybersécurité qui n'est pas à la hauteur. C'est également le cas des administrations publiques, l'une des autres cibles privilégiées des cybercriminels.

Mythes et idées reçues sur les fuites de données

L'internaute lambda est trop souvent persuadé que **ses informations personnelles ne valent rien**. Interrogés par nos soins, plusieurs de nos proches ne comprennent pas pourquoi ils devraient s'inquiéter de la quantité de leurs données circulant en ligne. Ils prétendent qu'ils n'ont « rien à cacher ».

Comme on l'a vu plus haut, une fuite peut pourtant avoir des conséquences dramatiques, surtout pour votre compte bancaire.

Certaines personnes se disent aussi sereines... parce qu'elles ont installé un antivirus sur leur ordinateur.

Or, **un antivirus n'empêche pas les attaques**, le phishing et n'empêche pas votre opérateur ou votre banque de se faire pirater, et de divulguer sans le vouloir vos données.

En clair, un antivirus ne suffit pas à garantir votre cybersécurité. C'est aussi le cas d'un VPN ou du mode Incognito de votre navigateur. Ces précautions, bien qu'utiles, ne suffisent pour vous protéger.

Mais alors, que pouvez-vous vraiment faire ?

Les bonnes pratiques pour se protéger

Bien souvent, on conseille aux internautes de tout faire pour sécuriser leurs comptes en ligne, tout d'abord en choisissant un bon mot de passe sécurisé. Il est recommandé d'opter pour un code de minimum 12-15 caractères, qui mélange majuscules, minuscules, chiffres, et des caractères spéciaux.

L'idéal est de passer par un **générateur de mots de passe**. En parallèle, on vous recommande d'activer la **double authentification** dès que celle-ci est disponible. Ce mécanisme de sécurité va exiger deux preuves distinctes d'identité pour accéder à un compte, en plus du mot de passe. C'est indispensable de le configurer sur tous vos comptes.

Néanmoins, je me suis rendu compte au fil des ans que ces précautions ne suffisent pas à protéger un internaute contre les fuites de données. Une fois que vos données ont été communiquées à une entreprise, c'est elle qui est chargée de les protéger contre les attaques.

Que votre compte soit protégé avec un bon mot de passe ou un système de double authentification, vos données restent dépendantes de la sécurité mise en place par l'entité qui possède vos informations.

En clair, vous ne pouvez pas faire grand chose pour

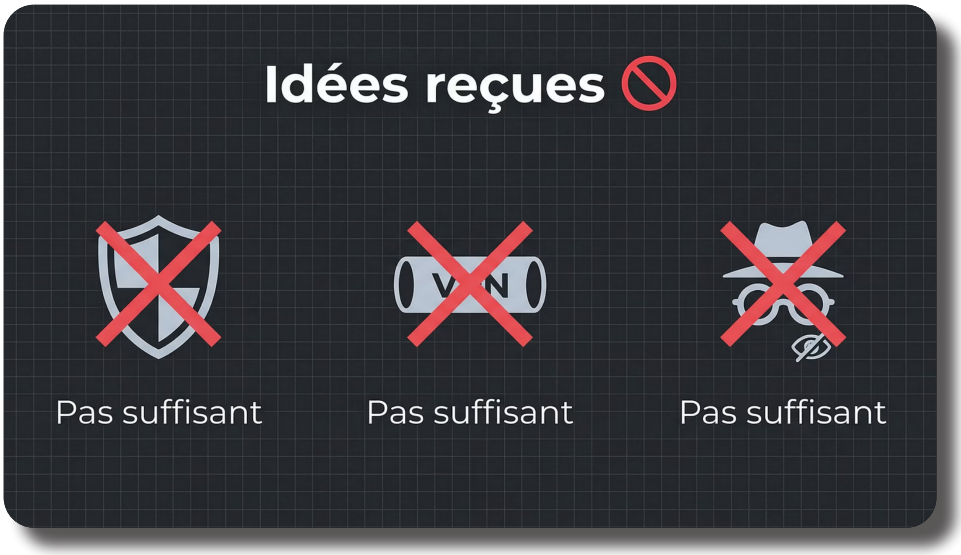
empêcher un vol. La seule chose que vous pouvez faire est de limiter au maximum la quantité de données que vous partagez avec autrui.

Tout d'abord, limitez les informations que vous publiez sur les réseaux sociaux, comme Facebook ou Instagram. Ces données peuvent être récupérées et combinées à d'autres informations plus sensibles, issues de piratages, et servir à tout type de cyberattaques.

Ensuite, tentez tant que possible de restreindre le nombre d'entités qui détiennent des informations sur votre compte. Si vous ouvrez un compte sur une banque en ligne ou un autre service quelconque, et que vous ne vous en servez plus, fermezle. Contactez le service client et demandez la suppression de vos données, en vertu du RGPD (Règlement Général sur la Protection des Données).

Enfin, optez pour des informations factices tant que c'est possible. Avec ces précautions, vous réduirez la surface d'attaque sur votre personne. Une bonne hygiène numérique réduit en effet les risques de se retrouver ciblé par des cybercriminels armés de données précises sur votre compte.

Florian Bayard



Votre smartphone vous espionne

En France, chaque utilisateur installe en moyenne près de 90 applications sur son smartphone. Celles-ci collectent en permanence des informations sur nos habitudes, parfois très personnelles. Or, ces données sont censées rester sur nos appareils. Peut-on réellement affirmer que notre vie privée est protégée ?

Afin de comprendre de quelle manière les smartphones peuvent surveiller leurs utilisateurs, nous nous sommes basé sur le reportage de l'équipe de **Cash Investigation** sur les données personnelles. Ils ont fait l'expérience en faisant l'acquisition d'un appareil neuf.

Il s'agit d'un téléphone totalement vierge, ne contenant aucune donnée personnelle. Ils le confient à l'experte en informatique : **Esther Onfroy**, spécialiste de l'analyse des applications mobiles.

Depuis quatre ans, cette ingénieure s'engage pour la défense de la vie privée. Elle a conçu un boîtier capable d'intercepter, en temps réel, les informations que les téléphones transmettent à l'insu de leurs propriétaires.

Dès l'allumage du smartphone, celui-ci commence immédiatement à échanger des données.

Sans aucune action de la part de l'utilisateur, l'appareil communique déjà : il entre en contact avec onze serveurs différents.

Il s'agit d'un téléphone Samsung, qui échange donc avec des services appartenant à Samsung, mais aussi à Google. Une situation logique, puisque Google est propriétaire d'Android, le système d'exploitation du téléphone.

Android équipe 86 % des smartphones dans le monde.

Deuxième étape de l'expérience : le téléchargement d'une application.

Esther intercepte alors les données émises par le téléphone.

Certaines sont transmises à Flurry, une société spécialisée dans le marketing. Il s'agit principalement de données techniques, peu compréhensibles pour le grand public.

Parmi elles figurent la date de mise en route du téléphone, le niveau de batterie, son état de charge ou encore le nom de l'opérateur. À quel moment le téléphone est-il allumé ? Combien de temps est-il utilisé ? Quelles actions sont effectuées ? Toutes ces informations sont collectées en temps réel par plusieurs entreprises.

Depuis le début de l'expérience, le téléphone a déjà échangé plus d'une centaine de fois avec des serveurs externes, dont ceux de Facebook. Et ce, alors même qu'aucun compte Facebook n'est installé sur l'appareil. Pourtant, Facebook sait que l'application est utilisée.

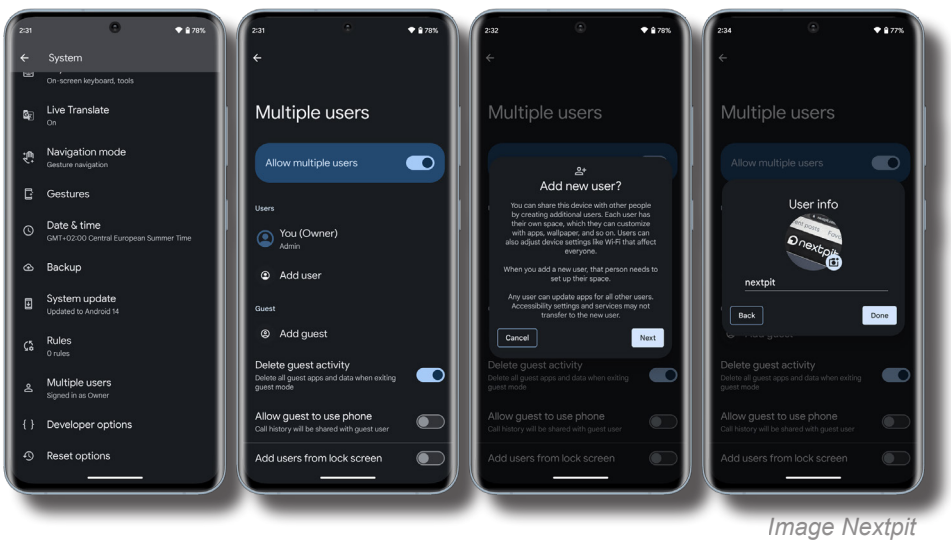


Image Nextpit

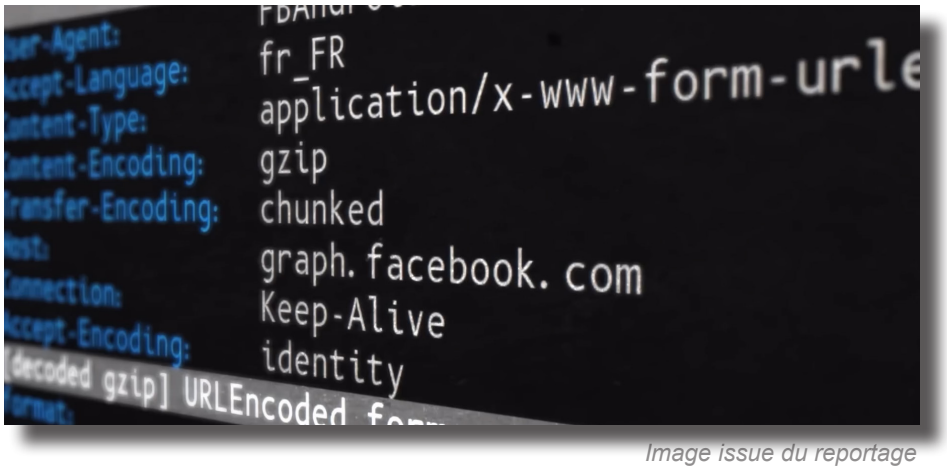


Image issue du reportage

Comment cela est-il possible ? Parce que la majorité des applications Android intègrent des traceurs développés par Facebook. Des programmes chargés de collecter des données pour le compte de l'entreprise américaine. Parmi les informations recueillies figure notamment la religion des utilisateurs.

Or, la loi interdit la collecte ou le traitement de données personnelles révélant, directement ou indirectement, les convictions religieuses. À quelles fins ces informations sont-elles utilisées ? Comment sont-elles exploitées ?

Des questions qui ne relèvent pas de la paranoïa, car en novembre 2020, un scandale éclate : l'application de prière Muslim Pro est accusée d'avoir transmis à l'armée américaine les données de localisation de millions de musulmans. Parmi eux, des milliers de Français, dont certains ont porté plainte.

Mais l'intrusion peut aller encore beaucoup plus loin :

Parmi les applications de santé les plus téléchargées en France figure Ma grossesse, une application appartenant au groupe Doctissimo.

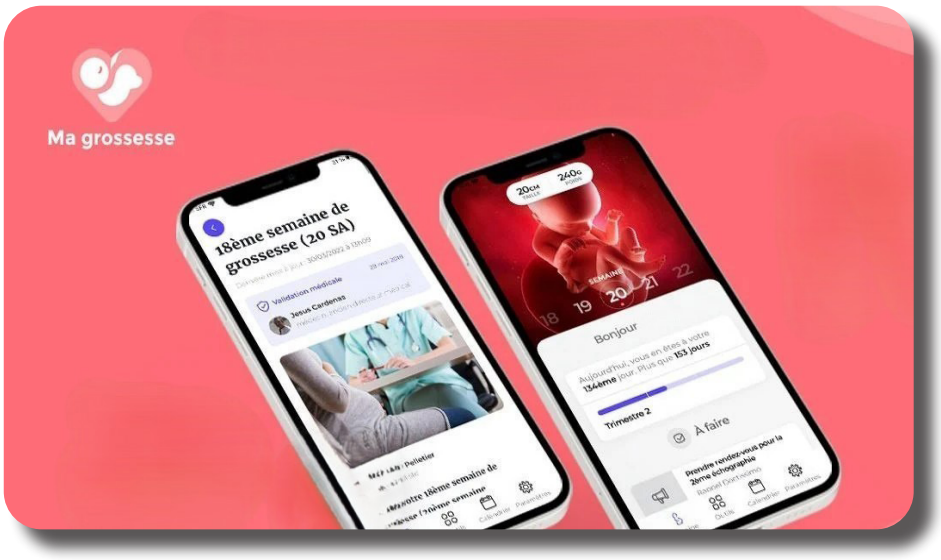
Elle permet aux utilisatrices de suivre le développement de leur bébé et d'y renseigner de nombreuses informations personnelles : le poids, l'établissement où aura lieu l'accouchement, ou encore le suivi des contractions. Ils y enregistrent par exemple un poids, puis vérifient si cette donnée a été transmise.

Ils constatent alors que des informations ont été envoyées vers le site profile.localitx.com. Y apparaissent notamment la date prévue d'accouchement, le début de la grossesse et le poids. Cela signifie que l'application a communiqué à Localitx des données permettant de déduire le rapport poids-taille, donc l'indice de masse corporelle.

Il s'agit clairement de données de santé. Or, en principe, la transmission de ce type d'informations est interdite sans le consentement explicite de la personne concernée. En l'absence d'accord préalable, ces données ne devraient pas être collectées ni quitter le téléphone.

Pourtant, en seulement vingt minutes d'utilisation, Doctissimo a transmis une trentaine de lignes de données médicales à trois partenaires commerciaux.

Les informations relatives aux



contractions et à la maternité ont été envoyées à l'entreprise française Xiti. La date d'accouchement a été transmise à la société américaine Localitx. La 35e semaine de grossesse, quant à elle, a été communiquée à Google.

L'application agit ainsi comme un véritable outil de traçage.

L'application rend indéniablement service en permettant le suivi de la grossesse. Cependant, ce que les utilisateurs ignorent le plus souvent, c'est qu'une partie des informations saisies peut être transmise et exploitée par des partenaires commerciaux de Doctissimo.

Une question se pose alors, ces transferts de données sont-ils autorisés par la loi ?

Pour y répondre, **Gaëtan Goldberg**, avocat spécialisé en protection de la vie privée est consulté.

Doctissimo est-il en droit de transmettre ces informations, qui relèvent clairement des données de santé, à des entreprises tierces ?

Selon lui, le principe est clair : le traitement et le partage de données de santé avec des partenaires commerciaux sont en principe interdits.

Pour y déroger, l'entreprise doit impérativement recueillir le consentement explicite de l'utilisateur.

Que recouvre précisément cette notion de consentement explicite ? Il s'agit de présenter à l'utilisateur une information claire et compréhensible, quelles données sont collectées, à qui elles sont transmises, pour quelles raisons, et dans quel objectif.

L'utilisateur doit notamment savoir si ces informations peuvent servir à un ciblage publicitaire fondé sur des données de santé, et être libre d'accepter ou de refuser. Or, dans ce cas précis, aucun consentement explicite n'a jamais été sollicité.

En l'absence d'accord exprimé, le traitement de ces données est donc illégal.

Gaëtan Golberg

Ils ont pourtant recherché ce bandeau d'information partout. Lors de la première ouverture de l'application, une fenêtre demande l'autorisation de traiter certaines données, mais sans jamais mentionner les données de santé. Ils consultent également la politique de confidentialité.

Ils découvrent alors la charte des données personnelles de Doctissimo : un document très long, comptant près de 5 800 mots, qu'ils prennent le temps de lire intégralement.

Trente-cinq minutes de lecture sont nécessaires pour en venir à bout. Une épreuve longue et fastidieuse. À l'issue de cette lecture, une grande partie du contenu reste difficilement compréhensible.

Le texte est truffé d'alinéas,

Image issue du reportage

Image site Doctissimo.fr

de jargon juridique et de termes techniques, donnant l'impression que tout est fait pour désorienter le lecteur.

Pour l'avocat, la situation est problématique. Le droit des données personnelles repose sur un principe fondamental : la transparence et l'accessibilité.

Les traitements de données doivent être expliqués de manière claire, précise et compréhensible par tous.

Toute personne utilisant l'application devrait pouvoir savoir ce qu'il advient de ses données.

Or, ce qui ressort ici, c'est une opacité généralisée, rendant très difficile pour les utilisateurs d'identifier où se trouvent leurs données personnelles et quels risques elles impliquent.

Et la situation réserve une dernière surprise : lorsqu'ils contactent Doctissimo en se présentant comme utilisatrices de MaGrossesse afin d'obtenir des explications, **l'équipe du site leur répond simplement qu'aucune donnée n'est transmise à des partenaires**

Ils décident alors de mener une expérience directement sur Internet. Cela tombe bien les tests psychologiques font partie des spécialités de Doctissimo, qui propose près de 300 quiz gratuits. « Quel type de féministe êtes-vous ? », « Êtes-vous plutôt chien ou chat ? ». Parmi ces questionnaires, une question retient particulièrement leur attention : **« Coup de blues ou dépression ? »**. Treize questions plus tard, un verdict tombe : le test conclut à un état dépressif.

Mais une autre information va s'avérer bien plus préoccupante. Avant de consulter le site, ils ont installé un logiciel gratuit appelé Disconnect, un outil de protection permettant d'identifier, en temps réel, les acteurs qui suivent la navigation sur Internet. Il révèle quelles entreprises collectent des données à l'insu des internautes. Sur Doctissimo, l'activité est intense.

Des dizaines de sociétés gravitent autour des utilisateurs, dont beaucoup sont totalement inconnues du grand public. Ont-elles été informées du fait qu'ils ont répondu à un test portant sur la dépression ?

Par écrit, l'équipe de Doctissimo se veut rassurante : le site affirme ne pas collecter de données de navigation pouvant être assimilées à des données sensibles, notamment des données de santé, et assure que ces informations ne sont pas transmises à des partenaires commerciaux.

Pourtant, quelques jours plus tard, l'équipe de cash met la main sur un document prouvant le contraire. Ce fichier détaille les données collectées par l'un des partenaires de Doctissimo lors de leur navigation sur le site.

Il contient l'intitulé précis de toutes les pages consultées, ligne par ligne : plus d'un millier d'entrées, dont celle correspondant au test « Coup de blues ou dépression ».

Pourquoi les partenaires de Doctissimo suivent-ils ainsi les internautes sur le web ?

L'objectif est clair : affiner le profil des utilisateurs afin de leur adresser des publicités ciblées. Une personne lisant plusieurs articles sur le stress se verra proposer des annonces pour des tisanes relaxantes ; un internaute fréquentant des sites sportifs recevra des publicités pour des chaussures de sport.

Ces annonces ciblées sont facturées trois à quatre fois plus cher que les publicités classiques.

Ce sont elles qui constituent le principal modèle économique de sites gratuits comme Doctissimo.

La face cachée de nos données : enquête sur les Data Brokers

Partout où nous allons, ils sont là. Dans l'ombre de nos écrans, au comptoir de nos pharmacies, jusque dans les secrets de nos dossiers médicaux. Une armée d'entreprises invisibles, les "data brokers", a transformé nos existences en une marchandise cotée à prix d'or.

Les maîtres de l'ombre et un marché à 400 milliards

Chaque clic sur Internet, chaque achat en pharmacie, chaque recherche de vol est consigné par des entreprises dont vous n'avez jamais entendu parler...

Cette enquête explore les dessous d'un marché colossal de la donnée personnelle, où nos secrets les plus intimes sont vendus au plus offrant. Ces entreprises agissent dans l'ombre pour préserver leur modèle économique

Cela démontre qu'il semble de ces entreprises ont sans doute conscience du caractère discutable, voire illégitime, de leurs pratiques.

Un rapport de la société **Knowledge Sourcing** indique que le marché mondial des data brokers connaît une forte dynamique de croissance : il devrait enregistrer un taux de **croissance annuel de 7,29 % et atteindre environ 616,5 milliards de dollars à l'horizon 2030, contre près de 434 milliards de dollars en 2025.**

L'ampleur de ces acteurs est difficilement concevable. L'entreprise américaine **Acxiom Holdings** disposerait d'une base de données **concernant 2,5 milliards d'individus**.

Selon ***Sarah Spickerman***, directrice de l'Institut des systèmes d'information et de la société de Vienne, aucun État ne possède, à l'échelle mondiale, un registre d'une telle envergure.

Un data broker (courtiers en données) est une entreprise spécialisée dans la collecte massive, l'agrégation et la revente de données provenant de multiples sources (sites web, applications, programmes de fidélité, bases publiques, partenaires commerciaux) afin de construire des profils très détaillés sur des individus ou des organisations.

Ces acteurs nettoient et recoupent les informations (âge, adresse, habitudes de consommation, navigation en ligne, centres d'intérêt, données socio-démographiques, parfois éléments financiers ou de santé non directement identifiants) pour créer des segments ciblés ou des scores qui seront utilisés par des annonceurs, des banques, des assureurs ou d'autres sociétés pour affiner le marketing, évaluer un risque, personnaliser une offre ou piloter une stratégie commerciale.

Des organisations comme **Acxiom** ou **Experian** détiennent des données décrites comme « quasi exhaustives » sur des centaines de millions de personnes, avec des milliers d'attributs par individu.

Le data broker irlandais Experian détient des informations sur plus de 95 % de la population américaine

Source : Blog de la société Experian

En Europe, le courtier détiendrait des informations sur près de 90 % de la population française.

Les data brokers se distinguent des grandes plateformes numériques par leur invisibilité fonctionnelle. Là où un utilisateur sait qu'il interagit avec Google, Amazon ou Meta, il ignore généralement l'existence des entreprises qui collectent et croisent ses données en arrière-plan.

La CNIL décrit ce phénomène comme un « écosystème complexe de reventes successives », dans lequel une donnée peut être copiée, enrichie et transférée de multiples fois sans que la personne concernée en soit informée.

Ces entreprises concluent entre elles des partenariats afin d'échanger des informations et d'enrichir les profils individuels. Certaines d'entre

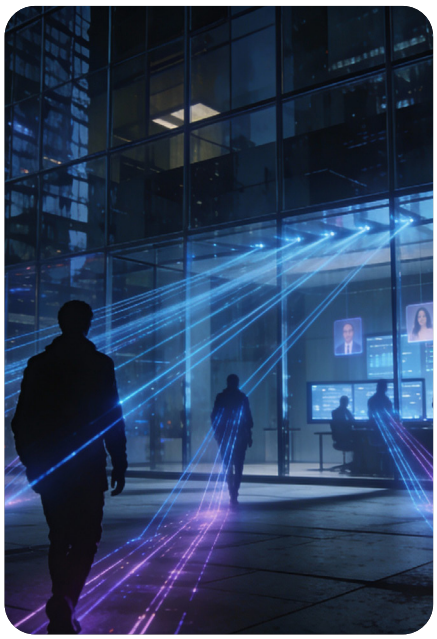
elles accumulent jusqu'à **30 000 données distinctes** pour chaque personne suivie

Ces profils reposent d'abord sur des informations classiques, comme l'âge ou le genre, mais vont bien au-delà. Ils incluent les lieux fréquentés, les destinations de voyage, les habitudes quotidiennes jusqu'au café pris chaque matin et les relations sociales.

Les centres d'intérêt sont analysés, tout comme les habitudes de consommation de contenus pour adultes et leurs préférences, le niveau de revenus, l'appartenance à une catégorie sociale, les orientations politiques ou encore les convictions religieuses.

Et encore, il ne s'agit là que d'une vingtaine de critères, loin des 30 000 réellement exploités par ces sociétés.

Ce profilage permet de dessiner un portrait psychologique qui **influe directement sur ce que vous voyez sur Internet.**



Les utilisateurs ignorent souvent qu'ils sont traités de manière inégale selon leur profil lorsqu'ils naviguent en ligne.

Cela se remarque, par exemple, lors de la réservation d'un billet d'avion via des comparateurs de vols ou les sites des compagnies aériennes.

L'algorithme prend en compte la relation à l'argent des utilisateurs, s'ils sont attentifs à chaque euro ou prêts à dépenser davantage. Le prix proposé s'adapte donc à leur profil : ceux capables de payer plus se voient afficher des tarifs supérieurs à ceux présentés à d'autres utilisateurs.

L'Illusion de l'Anonymisation

Pour se justifier, les courtiers en données avancent un argument désormais bien rodé : les informations collectées seraient anonymisées. En l'absence de nom ou de prénom, ils affirment qu'il serait impossible d'identifier les individus concernés.

Depuis plusieurs années pourtant, des chercheurs alertent sur les risques considérables que ces bases de données font peser sur la vie privée.

Yves-Alexandre de Montjoye, chercheur à l'Imperial College de Londres est l'un des spécialistes mondiaux les plus reconnus de l'anonymisation des données, démontre que cette promesse relève largement de l'illusion. Avec des chercheurs de nombreux pays, son équipe

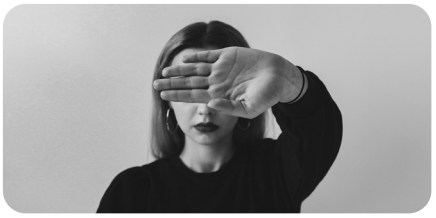
a développé un outil permettant d'illustrer concrètement à quel point il est facile de réidentifier une personne à partir de données prétendument anonymes.

Il dispose ainsi d'une base de données anonymisée contenant les profils de 66 millions de Français.

En utilisant seulement quelques informations une date de naissance, une ville de résidence, le genre, la situation matrimoniale et le fait d'être en emploi, sans même connaître le secteur d'activité il est possible, en quelques minutes, d'identifier précisément un individu dont l'identité est pourtant supposée protégée.

Ces six informations, relativement simples à obtenir, suffisent à lever l'anonymat d'une personne dans une base de données présentée comme sécurisée.

Une fois le profil identifié, il devient alors possible d'accéder aux milliers d'informations détaillées que cette base conserve précieusement sur l'individu concerné.



L'Europe à la rescousse ?

Depuis 2018, les internautes sont sollicités en permanence pour donner leur accord à la collecte de leurs données. En cas de refus, il est possible de tout désactiver, option par option. Une démarche qui peut sembler fastidieuse, mais qui constitue en réalité une avancée majeure.

Pour la première fois, les citoyens disposent d'un véritable levier pour reprendre la maîtrise de leurs informations personnelles.

Une évolution qui n'a pas été accueillie favorablement par les géants du numérique.

Pour tenter de combattre le RGPD, Google a investi près de 15,5 millions d'euros en actions de lobbying. Amazon a consacré plus de 4 millions d'euros à cette stratégie, tandis que Facebook et Apple ont chacun dépensé environ 3 millions d'euros.

Cette pression a conduit au dépôt de quelque 4 000 amendements, faisant de cette bataille réglementaire la plus vaste opération de lobbying jamais menée au sein de l'Union européenne. Des dizaines d'avocats ont afflué à Bruxelles, multipliant les rencontres avec les institutions européennes, se rendant dans les capitales et cherchant à influencer gouvernements et parlementaires afin de freiner l'adoption du texte.

Si ces entreprises ont opposé une telle résistance, c'est parce que les enjeux économiques étaient considérables. Reconnaître que les données n'appartiennent pas aux plateformes mais aux citoyens revenait à remettre en cause, voire à démanteler, le cœur même de leur modèle économique.

Dans la pratique, même lorsqu'une demande d'accès est correctement formulée et précise la volonté d'obtenir une copie des données détenues par une entreprise, rares sont celles qui respectent le délai légal d'un mois. Certaines ne répondent pas, d'autres affirment ne détenir aucune information, tout en continuant à les exploiter ou à les revendre.

Dans ces conditions, comment accorder du crédit à leurs déclarations lorsqu'elles assurent ne pas commercialiser nos données, alors même qu'il est pratiquement impossible de le vérifier par soi-même ?

Le RGPD prévoit toutefois un recours : tout citoyen peut saisir la CNIL. Si les faits sont établis, l'autorité est tenue d'intervenir et de prononcer des sanctions à l'encontre des entreprises concernées.

En 2025, le montant cumulé des sanctions financières a dépassé les 55 millions d'euros, en tenant compte de plusieurs amendes d'un niveau inédit. Cette hausse s'accompagne d'une augmentation marquée des mesures correctrices par rapport aux années antérieures.

La CNIL a ainsi clairement affirmé sa détermination à exercer pleinement ses pouvoirs de sanction, notamment en s'appuyant sur la procédure simplifiée, conçue pour apporter une réponse rapide aux manquements les plus courants.

IQVIA
Le géant qui ausculte la France

Une délibération de la CNIL datant de septembre 2018 autorise les pharmaciens à collecter plusieurs types de données : le numéro de sécurité sociale, l'année de naissance, le prénom, le sexe, ainsi que les données dites de délivrance, c'est-à-dire l'ensemble des médicaments achetés. Ces informations peuvent ensuite être transmises à une entreprise américaine peu connue du grand public en France : **IQVIA.**

Pourtant, il s'agit du plus important courtier mondial de données médicales.

L'activité principale de cette société consiste à récupérer des données auprès des hôpitaux, des cabinets médicaux et des laboratoires, afin de les revendre, notamment aux industries pharmaceutiques. Une activité particulièrement lucrative : le groupe affiche un chiffre d'affaires avoisinant les 15 milliards d'euros en 2024. Cette pratique a suscité une vive contestation outre-Atlantique.

IQVIA est aujourd'hui le plus grand détenteur de données

parmi les plus sensibles, celles qui concernent directement la santé physique et mentale des individus. Elle collecte tout ce qui est accessible : prescriptions, dossiers médicaux, données issues de la recherche clinique, retraçant l'ensemble du parcours de soins des patients.

En revanche, l'usage précis de ces données et la fréquence à laquelle elles sont revendues restent largement opaques.

Aux États-Unis, l'entreprise a été poursuivie par des pharmaciens pour avoir collecté leurs données sans consentement. Elle a été condamnée à verser 10 millions de dollars de dommages et intérêts. En France, en revanche, IQVIA a obtenu de nombreuses autorisations officielles.

Pour certains observateurs, la situation est alarmante. Peu de personnes accepteraient que des informations aussi sensibles que leur état de santé ou leur équilibre psychologique puissent être achetées et revendues. Une question se pose alors : le data broker américain utilise-t-il en France les mêmes méthodes de collecte qu'ailleurs ? Ce qui frappe en premier lieu, c'est qu'**IQVIA s'est déjà implantée discrètement dans près de la moitié des pharmacies françaises.**

Comme dans toute officine, un logiciel enregistre l'ensemble des clients via une fiche dédiée regroupant le nom, coordonnées, numéro de sécurité sociale, médecin traitant.

Le logiciel est configuré pour transmettre en continu certaines données à IQVIA.

En 2021, 10 000 officines collectaient des données pour IQVIA, en France soit 1 sur 2.

Les informations envoyées correspondent aux ventes réalisées par la pharmacie, qu'il s'agisse de produits de parapharmacie ou de médicaments délivrés sur ordonnance. En contrepartie de ces données portant sur l'ensemble de leur clientèle, les pharmaciens perçoivent quelques euros par mois et reçoivent une étude de marché personnalisée pour leur officine.

Chaque mois, un tableau de synthèse leur est transmis, récapitulant les ventes et leur permettant d'ajuster leurs stocks, leurs achats et d'identifier les tendances de consommation de leur clientèle. Par exemple, ils peuvent observer l'évolution de la demande en homéopathie ou en compléments alimentaires, afin d'anticiper les besoins.

Des données issues des pharmacies, échangées contre une somme modeste et quelques graphiques, mais qui, une fois agrégées à grande échelle, sont ensuite revendues par IQVIA.

Dès que le patient insère sa carte Vitale dans la borne, un identifiant unique est généré chez IQVIA.

Celui-ci le suivra tout au long de ses visites dans les différentes pharmacies du panel. Grâce à ce système, chaque transaction peut être reliée à un individu précis, permettant de regrouper l'ensemble des informations de délivrance de médicaments le concernant. Ce type de traçage individualisé est ensuite vendu à un prix très élevé.

Pourquoi une telle valeur ? Parce qu'il s'agit de la seule base en France permettant de réaliser des études de marché aussi détaillées et précises. Certaines études peuvent ainsi atteindre jusqu'à 500 000 euros.

Et les patients dans tout ça ?

Leur consentement est-il réellement demandé avant que leurs données ne soient transmises à IQVIA ? Selon l'autorisation délivrée par la CNIL, les pharmaciens doivent informer individuellement chaque client et lui donner la possibilité de s'opposer à la collecte de ses données.

Dans la pratique, cette obligation est quasiment impossible à appliquer. Pourquoi ? Pour des raisons de temps et d'organisation : un pharmacien, pour maintenir l'efficacité de son activité et dispenser les médicaments, ne peut consacrer 5 à 10 minutes à expliquer à chaque patient comment ses données sont traitées et transmises.

En conséquence, cette information n'est pas réellement communiquée et le droit d'opposition reste largement théorique.

Chez Cyber-IT on s'est alors mis en tête de démarcher plusieurs pharmacies du nord de la France afin de leurs demander concrétement s'ils savaient comment était traités les

données personnelles de leurs clients. Résultat accablant …

La quasi-totalité ne semblent savoir précisément répondre à la cette question. Un pharmacien souhaitant rester anonyme nous confie même n'avoir jamais su que les données seraient traitées comme des marchandises sinon il n'aurait jamais accepté de participer.

Pourtant, chez IQVIA, on sait depuis longtemps que les données médicales ne peuvent pas réellement être anonymes.

Et ce constat ne vient pas de n'importe qui : c'est Jean-Marc Aubert qui l'affirme. Entre 2019 et 2023, Jean-Marc Aubert a occupé le poste de président de la filiale française d'IQVIA. Depuis janvier 2023, il est devenu vice-président Healthcare du groupe.

En janvier 2016, il intervient dans une école de commerce pour évoquer les enjeux liés aux données de santé.

Lors de cette conférence, il explique concrètement comment il est possible de retrouver une personne au sein d'une base de données dite « anonymisée ».

Il reconnaît également que rendre les données véritablement anonymes n'est pas dans l'intérêt économique des data brokers.

Anonymiser des données consiste soit à les rendre plus générales, soit à supprimer certaines informations trop identifiantes.

Par exemple, au lieu d'indiquer la date de naissance précise d'une personne, on va simplement mentionner une tranche d'âge.Dans certains cas, certaines variables sont même retirées de la base de données pour éviter toute ré-identification. Mais ce processus a une conséquence directe : il dégrade la qualité des données. Or, dégrader la qualité des données revient à en diminuer la valeur commerciale. Plus les informations sont précises, plus elles sont exploitables, et donc plus elles se vendent cher.

Interrogé par Élise Lucet en 2021, Jean-Marc Aubert est questionné sur l'anonymisation des données de santé collectées par IQVIA.

La journaliste l'interpelle directement : *comment l'entreprise peut-elle garantir aux patients que ces données extrêmement sensibles, puisqu'elles concernent leur santé, sont totalement anonymes ?*

Jean-Marc Aubert répond alors qu'IQVIA travaille sur l'anonymisation des données depuis près de soixante ans. Selon lui, en six décennies d'activité, aucun incident n'aurait été constaté sur ces questions.

Dans une notice publiée par IQVIA sur son propre site internet, l'entreprise indique que les mesures de sécurité mises en place « visent à réduire les possibilités d'identification ».

Une formulation qui interroge. Réduire les possibilités d'identification signifie qu'un risque subsiste. Celui qu'une personne mal intentionnée puisse, à un moment donné, accéder à l'ensemble des informations médicales d'un patient. Jean-Marc Aubert précise alors que ce sont les termes retenus par la CNIL elle-même.

Il reconnaît également l'existence d'une limite majeure : certaines pathologies ne concernent que quelques milliers de personnes, ce qui rend l'anonymisation beaucoup plus fragile.

Depuis la fin de l'année 2021, IQVIA a mis en place un dispositif permettant aux pharmaciens de bloquer la transmission des données des patients qui s'y opposeraient.

Lors de nos visites dans plusieurs pharmacies du nord de la France, aucune affichette n'était visible. Aucune information n'était communiquée aux patients concernant la collecte et la transmission de leurs données de santé.

Dès lors, une question fondamentale se pose : si les patients ignorent que leurs données médicales sont collectées, ne sont-ils pas, de fait, privés de leurs droits ? Notamment du droit d'opposition, l'un des principes fondamentaux du RGPD.

Comment exercer un droit lorsque l'on ne sait même pas que l'on est concerné ?

Nous avons sollicité la CNIL sur ces points précis. Malgré un premier échange encourageant et plusieurs relances ultérieures, l'autorité n'a finalement pas souhaité s'exprimer sur ces questions.

Depuis plusieurs années, la société américaine IQVIA, spécialisée dans l'analyse de données de santé, cherche à accéder à des informations médicales de plus en plus détaillées, notamment les dossiers médicaux hospitaliers.

L'entreprise s'intéresse tout particulièrement aux données liées au cancer, une pathologie centrale pour l'industrie pharmaceutique en raison des enjeux médicaux et financiers qu'elle représente. Cela nous amène à nous pencher sur nos données de santé en France ...

Un changement d'échelle se dessine avec la mise en place d'un dispositif national de centralisation des données de santé. Annoncé publiquement par le président de la République en mars 2018, ce projet ambitieux vise à créer un véritable « hub des données de santé », destiné à rassembler et organiser l'ensemble des données issues du système de soins français.

L'objectif affiché est de centraliser les données remboursées par l'Assurance maladie, les informations cliniques hospitalières, les données de la médecine de ville, ainsi que de grandes cohortes et registres scientifiques, afin de les rendre plus facilement mobilisables pour la recherche et l'amélioration des parcours de soins. Ce dispositif, connu sous le nom de **Health Data Hub**, agrège les données provenant des hôpitaux, cliniques, établissements pour personnes âgées, laboratoires d'analyses, pharmacies, cabinets médicaux et centres de radiologie.

Il rassemble ainsi près de douze années de données concernant l'ensemble de la population française

dans une plateforme technologique sécurisée qui doit permettre leur stockage, leur traitement et leur analyse dans des conditions strictement encadrées., selon la CNIL.

Dans le cadre juridique qui régit le Health Data Hub, le ministère de la Santé assouplit les conditions d'accès aux données médicales. Il n'est désormais plus nécessaire de justifier de travaux de recherche, d'études ou d'évaluations pour y accéder.

Il suffit d'invoquer la notion d'« intérêt public », un concept volontairement large et peu défini. Cette imprécision soulève de nombreuses interrogations : que recouvre exactement l'intérêt public et jusqu'où peut-il être invoqué ? Une compagnie d'assurance qui sollicite l'accès au Health Data Hub en expliquant vouloir réduire ses coûts pour une population donnée peut-elle se prévaloir de l'intérêt public ? La question se pose, tant la notion demeure floue. Un autre élément vient complexifier davantage la situation. La mise en place du Health Data Hub est confiée par le gouvernement à Jean-Marc Aubert, alors haut cadre d'IQVIA. Il quitte temporairement son poste au sein de l'entreprise pendant deux ans afin de piloter ce projet.

Le fait que le Health Data Hub ait été pensé et conçu par une personne issue du secteur de la revente de données suscite de vives critiques. Le malaise est renforcé par un constat : une semaine seulement après le lancement du dispositif, Jean-Marc Aubert retourne chez IQVIA France, où il devient président. La question des conflits entre intérêts publics et intérêts privés se trouve ainsi au cœur du débat.

Jean-Marc Aubert explique que, durant sa mission pour l'État, il remplit des déclarations auprès de la Haute Autorité pour la transparence de la vie publique et passe devant la commission de déontologie, chargée de vérifier l'absence de conflit d'intérêts. Son retour chez IQVIA fait également l'objet d'une déclaration officielle et d'un avis de cette même commission.

De son côté, IQVIA France affirme, qu'il n'existe « aucun conflit d'intérêts dans le parcours » de Jean-Marc Aubert.

Certains anciens responsables et autre politiques, inquiets des risques potentiels pour la confidentialité, la gouvernance et l'usage économique des données de santé, choisissent de s'exprimer publiquement.

Parmi eux figure Adrien Parrot, alors chargé de la gestion des bases de données de l'Assistance publique Hôpitaux de Paris au moment de la mise en place du Health Data Hub en 2019. Mais également, Philippe Latombe, député et secrétaire de la Commission permanente des lois constitutionnelles.

INTERVIEW ADRIEN PARROT

Bonjour Adrien, merci d'avoir répondu à notre invitation à vous exprimer. Nous souhaiterions en savoir un peu plus sur la situation en 2019 lors de la mise en place du Health Data Hub si tu veux bien.

A l'époque, j'étais ingénieur à l'entrepôt de données de santé l'AP-HP, l'assistance publique des hôpitaux de Paris, qui est un peu le pendant du Health Data Hub. Donc j'avais un devoir de réserve un peu plus contraignant en tant qu'ingénieur. On démarrait l'initiation de l'entrepôt de données de santé des hôpitaux de Paris à ce moment-là.

Les technologies qui avaient été choisies par les ingénieurs à cette époque, dont Nicolas Paris, qui est arrivé avant moi, et d'autres personnes aussi, étaient des logiciels open source et le tout auto hébergé sur les serveurs de l'AP-HP. Il se trouvait qu'on arrivait à avoir, grosso modo, les mêmes fonctionnalités que celles attendues par le Health Data Hub au moment de sa phase de préfiguration.

Finalement, en lisant nos mails courant mai-juin 2019, on a réalisé que le projet du Health Data Hub, pour lequel nous n'étions pas opposé sur le principe allait être hébergé chez Microsoft Azure. A partir de ce moment-là, il y a eu de plus en plus d'opposition en interne.

Une tribune a été faite dans Le Monde en fin 2019, puis nous avons enchaîné sur des attaques au Conseil d'État, pour finalement quitter l'APHP avec Nicolas Paris.

L'entrepôt de l'APHP était en production au moment où on a fait la tribune dans Le Monde. Ce n'était pas des conjectures, ni des vues de l'esprit. On savait qu'il y avait une alternative qu'on pouvait faire, que l'APHP l'avait fait. Qui plus est était de l'open source et les technologies choisies était maitrisées et connues.

Les problématiques de souveraineté étaient moins présentes ou quasi inexistantes à l'époque. Mais c'est en faisant le tour des risques juridiques avec des avocats et des jurys d'avocats qu'on s'est dit que c'était totalement impossible de choisir des technologies américaines, c'était purement la fin du secret médical.

Les données étaient trop facilement accessibles par des entités extra-européennes sans contrôle conforme aux règles de l'Union Européenne. C'était un conflit idéologique, technique, moral, éthique, déontologique. **Nous étions obligé de prendre position.**

Je ne sais pas si vous pouvez en parler mais, nous avons beaucoup entendu parler de Jean-Marc Aubert, de la société IQVIA. La position qui lui a été confiée pour la mise en place du HDH. Que pensez-vous de cette situation ?

Je vais être très factuel, sur le fait de Jean-Marc Aubert d'autres ont évoqués le risque de conflit d'intérêt et le pantouflage, notamment Le Monde.

Après, dans le choix de Microsoft, à savoir s'il y a eu des sommes de versées, je n'ai aucune info à partager là-dessus.

Ce qui est au moins sûr, c'est que des technologies comme celles d'IQVIA, par la force des choses, on les met en avant aussi par commodité intellectuelle, on met en avant les technologies que l'on connaît sans être forcément rétribué d'une façon ou d'une autre.

Mécaniquement, quand on connaît quelque chose on va plutôt dans ce sens pour remplir le besoin. C'est aussi normal. Mais ce qui est sûr, c'est qu'IQVIA n'utilise pas des technologies européennes open source pour traiter ces données.

Ce sont des clouds qu'à l'époque, ils avaient l'habitude d'utiliser et qu'ils doivent sûrement utiliser.

Et donc, il y a au moins eu cet aspect mécanique de promotion de solutions qu'ils connaissaient, mais qui n'était peut-être pas dans l'intérêt public et dans l'intérêt des Français, de l'État français.

Selon vous, quel est le réel danger que nos données soient justement dans les mains d'acteurs qui ne sont pas européens ?

C'est avant tout les libertés fondamentales et le secret médical.

C'est exactement ce que Snowden a démontré en parlant de la surveillance généralisée, les programmes de PRISM ou autres, le Cloud Act etc …

Il y a des lois sécurité-défense qui, elles, pour le coup, sont beaucoup plus permissives et permettent des accès larga manu aux données. Et c'est ces textes-là qui, d'ailleurs, ont fait l'objet d'attaques de Maximilien Schrems et d'invalidations des traités d'adéquation successifs transatlantiques, des traités qui permettent les échanges de part et d'autre de l'Atlantique. Donc voilà, un des risques est celui de l'accès aux données de façon non encadrée.

Pour les citoyens européens, quand leurs données sont chez des clouders extra-européens, ils sont dans une sorte de no-man's land juridique, s'ils ont envie de se retourner contre les juridictions ou pour tout simplement exercer leurs droits, c'est au moins beaucoup plus compliqué, voire impossible d'exercer ces droits. Et donc, pour nous, ce n'est pas pensable. Il ne faut pas rester

dans un environnement juridique qui ne permet pas d'exercer ses droits de rectification de données, tous les droits liés au RGPD : l'opposition, la rectification, la suppression etc...

Pour nous c'est d'abord une problématique de liberté fondamentale et de secret médical. Mais il y en a plein d'autres, comme les blocages des plateformes premièrement,

il y a eu par exemple un juge de la Cour pénale internationale qui s'est vu supprimer ses accès à ses clouds et Teams par Microsoft de façon brutale par l'administration Trump. En cas de coupure de service, il y a des risques importants,

Également, un risque qui parle de plus en plus aux directions des systèmes d'information, c'est les risques de coûts et de licences qui augmentent. Pour des services d'intérêt vitaux, pour la recherche d'un pays, pour des services dont on a besoin, la solution, une fois qu'on est bloqué chez un clouder, c'est de subir les montées de prix successifs et de ne plus pouvoir payer. C'est ce qui se passe typiquement dans les hôpitaux en ce moment.

C'est très compliqué avec les technologies de virtualisation ou même tout simplement de mail. De fait, financièrement, c'est compliqué. En gros, liberté fondamentale, coupure de service, coupure des accès et risque financier, sont les risques réels que l'on peut entrevoir.

Nous avons été deux fois au Conseil d'État avec l'association Interop, enfin trois fois mais sur deux sujets, sur le sujet du coup du Health data hub et sur la campagne de vaccination lors de la COVID où on attaquait à peu près les mêmes problématiques puisque certains des plateformes de prise de rendez-vous étaient chez des clouders américains. Doctolib est chez Amazon par exemple. Il y aurait tant à dire…

INTERVIEW PHILIPPE LATOMBE

À l'époque, nous nous étions émus dans notre rapport que le HDH puisse héberger l'ensemble de ces données chez Microsoft, en particulier son cloud Azure, et ce sans appel d'offres. On nous avait expliqué que, dans la phase de construction du HDH, le recours à l'Union des groupements d'achats publics (Ugap) était suffisant et permettait d'éviter de passer par la commande publique.

Des parlementaires ont ensuite interrogé les ministres concernés lors de séances de questions d'actualité au Gouvernement. Le ministre de la santé et le secrétaire d'État au numérique ont apporté une réponse identique au Sénat et à l'Assemblée nationale concernant la réversibilité de l'hébergement, de Microsoft vers une entité souveraine, conformément à la doctrine du « cloud au centre » à l'époque « cloud de confiance ».

Ce processus devait être mis en oeuvre dans un délai de dix-huit mois. Toutefois, trois ans plus tard, il n'est toujours pas d'actualité.

Depuis des mois, je pose des questions au HDH sans obtenir de réponses. Je demande des documents précis, comme la communication des contrats, du nombre de consultants et de leurs tarifs horaires ou journaliers, ainsi que des travaux réalisés par ces consultants pour le HDH, afin de comprendre la stratégie qui a conduit ce dernier à ne pas obéir aux instructions successivement données par les ministres.

En réponse, la directrice du Health Data Hub m'a simplement indiqué de formuler une demande auprès de la Commission d'accès aux documents administratifs (Cada).

Le HDH a indiqué qu'il n'y avait pas de solution française, et de façon assez lunaire qu'un appel d'offres serait même préjudiciable à notre tissu industriel, car aucune entreprise nationale ou européenne ne serait retenue, mettant en lumière leur retard sur les américains.

Avons-nous des solutions pour héberger ces données ? Oui. Parmi toutes les entreprises françaises qui peuvent le faire, je citerai OVH, Scaleway et NumSpot ou encore Outscale et Cloud Temple. Les possibilités sont très importantes, et les universités et certains laboratoires de recherche ont déjà recours au Centre d'accès sécurisé aux données (CASD), solution qui avait d'ailleurs été mise en avant par M.Marchand-Arvier, conseiller d'État et actuellement directeur de cabinet de Mme Vautrin, dans son rapport sur les données de santé. Je ne renoncerai pas à l'idée que le HDH rencontre un problème d'adhérence à Microsoft et à son cloud Azure ; nous devons approfondir cette question pour aller au bout de la démarche. Je ne suis pas adepte des théories du complot, mais l'absence totale de réversibilité depuis plus de cinq ans, en dépit des demandes des ministres, pose problème.

" La loi devra changer cela en obligeant l'immunité aux règles extraterritoriales non européennes d'être la règle pour les données sensibles (notamment de santé) de nos concitoyens français et européens.

Le 1er juillet 2025 le Health Data Hub, constatant une inadéquation entre l'extraterritorialité des lois américaines et un besoin de souveraineté, lance un appel d'offres. Ce projet, estimé à 6,2 millions d'euros sur quatre ans, était ouvert jusqu'au 4 août 2025 avec une mise en service prévue à l'été 2026. OVHcloud et Cloud Temple se sont déclarés candidats

Credit photo : Philippe Latombe - JOEL SAGET / AFP

DARKWEB le nouveau far west numérique

LA REVENTE DE NOS DONNÉES PERSONNELLES - UN BUSINESS LUCRATIF

DOSSIER SPECIAL

Un marché criminel qui génère des milliards de dollars en dehors de tout contrôle légal.

Tandis que les grandes entreprises technologiques construisent leurs empires sur nos données, un marché parallèle prospère dans l'ombre du web.

Sur le darkweb (ensemble de réseaux décentralisés cachés derrière des couches de chiffrement) les données personnelles volées se vendent comme des actions en bourse.

Et le volume de ce commerce clandestin est vertigineux.

Les chiffres parlent d'eux-mêmes. Selon les dernières statistiques de 2025, plus de 3 millions de personnes accèdent quotidiennement aux plateformes du darkweb, et environ 60% des domaines actifs sur le darkweb sont impliqués dans des activités illégales.

L'économie souterraine du darkweb génère une somme estimée à 1,5 milliard de dollars par année

à partir de la vente de données volées, de biens contrefaits et d'autres produits illégaux. Parmi ces activités criminelles, le commerce de données personnelles occupe une place de choix.

15 milliards de comptes volés circulent actuellement sur le darkweb

en très nette augmentation de 82% depuis 2022.

Cette explosion du marché reflète une réalité simple : moins les données sont accessibles, plus elles valent cher.

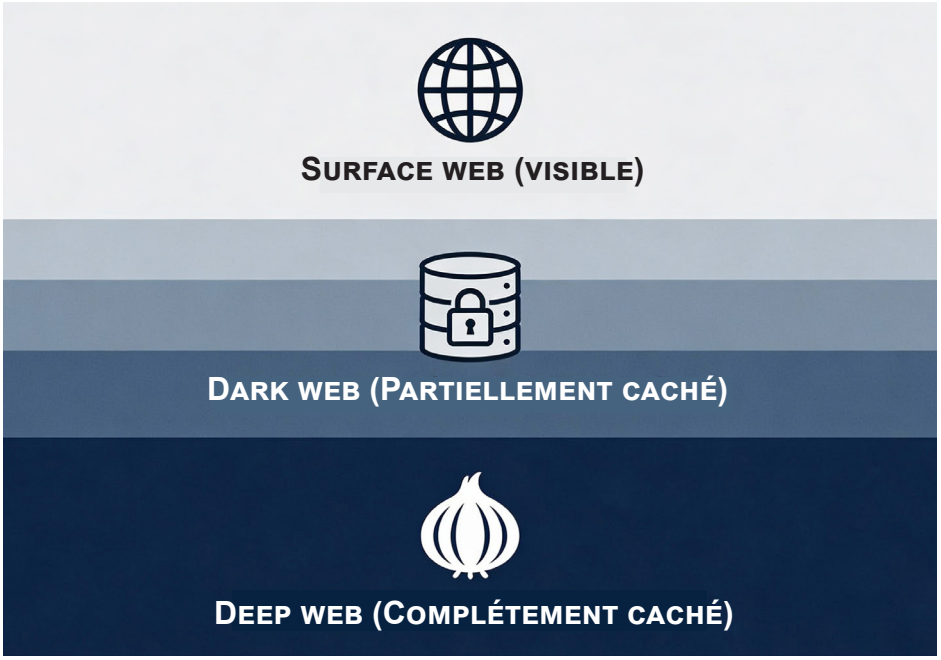
QU'EST-CE QUE LE DARKWEB ?

Le darkweb est une partie spécialisée d'Internet qui nécessite des logiciels spécifiques pour y accéder et qui est délibérément cachée aux moteurs de recherche traditionnels. Contrairement à ce que certains croient, le darkweb n'est pas synonyme du "deep web" une confusion courante mais importante à clarifier.

Le deep web désigne simplement la partie d'Internet qui n'est pas indexée par les moteurs de recherche (environ 96% d'Internet). Cela comprend votre boîte email, vos relevés bancaires en ligne, vos dossiers médicaux numériques et les bases de données scientifiques payantes.

L'histoire du darkweb remonte aux années 1990. Le projet Tor a été développé initialement par le laboratoire de recherche Naval américain en 1995 pour protéger les communications gouvernementales. L'idée était simple : utiliser une série de relais cryptographiques pour masquer la source et la destination des données, rendant ainsi quasi impossible la traçabilité des utilisateurs.

Ce qui commença comme un outil de sécurité gouvernementale devint rapidement disponible au public. En 2003, le code source de Tor fut rendu open source, et la communauté informatique mondiale commença à développer des applications et des services dessus. Ce qui aurait pu rester un outil de protection de la vie privée pour les dissidents et les journalistes en zones de répression est devenu, progressivement, le havre de prédilection pour les criminels.



COMMENT FONCTIONNE TOR ET LE DARKWEB ?

Pour comprendre pourquoi le darkweb est si difficile à réguler et à surveiller, il est essentiel de comprendre comment fonctionne techniquement le réseau Tor.

Quand vous envoyez des données sur Internet de manière normale, elles voyagent directement de votre ordinateur au serveur de destination. Chaque étape de ce voyage laisse des traces : votre adresse IP est enregistrée, les serveurs intermédiaires savent d'où et vers où vont les données.

C'est pour cette raison que les gouvernements et les fournisseurs d'accès à Internet peuvent surveiller votre activité en ligne.

Le réseau Tor change cette dynamique fondamentalement. Au lieu d'envoyer vos données directement au serveur de destination, le protocole Tor les enroule dans plusieurs couches de chiffrement (d'où le nom « Onion » oignon).

Vos données sont alors envoyées par un chemin aléatoire à travers une série de serveurs appelés nœuds relais, distribués à travers le monde.

Voici comment cela fonctionne :

1. Votre ordinateur envoie les données chiffrées au premier nœud relais

2. Le premier nœud décrypte une couche de chiffrement, découvrant ainsi l'adresse du nœud suivant, mais pas celle de la destination finale

3. Le nœud suivant décrypte à son tour une couche, sans voir ni la source originale ni la destination finale

4. Ce processus se répète à travers plusieurs nœuds (généralement 3 à 5)

5. Le nœud de sortie envoie finalement les données décryptées au serveur de destination

Le résultat ?

Aucun nœud individuel ne possède l'information complète sur la source et la destination.

Même le serveur de destination ne sait pas d'où proviennent réellement les données. Seul le dernier nœud (le « nœud de sortie ») voit le trafic décrypté, et il n'a pas accès à l'identité de l'utilisateur original.

LES MARCHÉS DU DARKWEB

Une fois que vous avez accédé au darkweb via Tor, vous pouvez accéder aux marchés du darkweb, des places commerciales souterraines utilisant des domaines en .onion.

Ces marchés fonctionnent comme des sites e-commerce ordinaires : ils ont des vendeurs, des acheteurs, des évaluations, des messages privés et même des systèmes d'escrow pour protéger les transactions. Sauf que les produits vendus sur ces marchés sont illégaux. On peut y trouver des drogues, des armes, des faux documents, des services de piratage informatique, et bien sûr, des données personnelles volées.

La structure de ces marchés est généralement hiérarchisée. Il existe des petits marchés spécialisés et des grands marchés généralistes. Blacksprut, par exemple, est actuellement le plus grand marché du darkweb, contrôlant environ 28% de la part de marché.

Mais la scène du darkweb est hautement volatile. Les marchés apparaissent et disparaissent régulièrement, soit en raison de l'intervention des autorités, soit à cause de disputes internes ou de scissions.

Le 21 mars 2023, par exemple BreachForums a été fermé suite à l'arrestation de son propriétaire, Conor Brian Fitzpatrick .

Le forum a ensuite rouvert sous la direction du groupe de pirates ShinyHunters et de l'ancien administrateur de BreachForums, « Baphomet ».

Le site a de nouveau été fermé et le nom de domaine saisi le 15 mai 2024, mais ShinyHunters a réussi à le récupérer quelques heures plus tard.

COMMENT FONCTIONNE UN MARCHE DU DARKWEB ?

Inscription et Authentification

Pour accéder à un marché fermé, vous devez généralement vous créer un compte avec un nom d'utilisateur et un mot de passe.

Certains marchés requièrent des invitations ou des références de membres existants.

Navigation et Recherche

Une fois enregistré, vous pouvez parcourir les catégories de produits ou utiliser une barre de recherche pour trouver des données spécifiques .

Annonces de Vendeur

Les vendeurs publient des annonces décrivant les données qu'ils vendent. Une annonce type pourrait ressembler à ceci

"Dossiers médicaux vérifiés Patients USA, 2020-2024. 10 000 records pour 25 000$ Livraison instantanée."

Paiement

Vous payez généralement en cryptomonnaies (généralement versé en Bitcoin). Le paiement est souvent placé en escrow par l'acheteur, le tiers reçoit les fonds, mais ne les remet au vendeur que si l'acheteur confirme avoir reçu le produit satisfaisant.

Livraison

Le vendeur envoie généralement les données via un lien de téléchargement chiffré ou un fichier attaché à un message privé.

Révision

Après la transaction, les acheteurs peuvent laisser des avis sur la qualité des données, fiabilité du vendeur, etc... C'est ce qui construit la réputation.

La Communauté du Darkweb

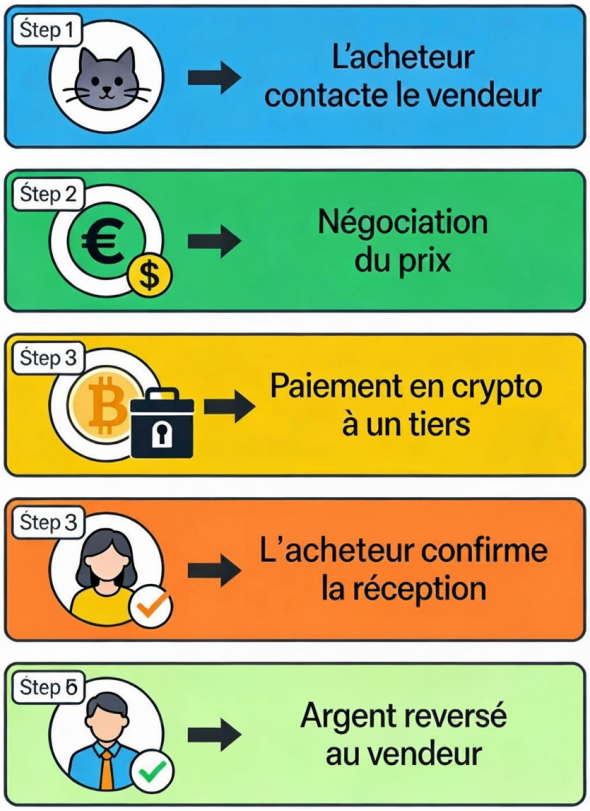
Les utilisateurs du darkweb forment une communauté avec ses propres forums, ses influenceurs, ses débats. Il y a des tutoriels pour les débutants, des discussions techniques, et même des conseils juridiques. C'est une communauté sans chef mais densément connectée.

Cette communauté comprend une variété de personnes. Il y a bien sûr, les criminels professionnels, les pirates qui volent les données, les arnaqueurs, les trafiquants de drogue.

Mais il y a aussi des activistes, des dissidents politiques, des journalistes travaillant sous des régimes autoritaires, des lanceurs d'alerte et des simples citoyens qui valorisent leur vie privée.

C'est ce mélange qui rend le darkweb particulièrement difficile à réguler. Interdire le darkweb serait persécuter les activistes politiques et les victimes de répression qui en ont besoin pour survivre.

D'un autre côté, le laisser sans surveillance serait permettre à la criminalité organisée de prospérer sans entraves.



LES TYPES DE DONNÉES VOLÉES ET LEURS PRIX

Sur le marché noir du darkweb, les données ne sont pas toutes égales. Leur valeur est déterminée par plusieurs facteurs : la complétude des informations la fraîcheur des données et surtout, l'utilité criminelle de l'information.

Les vendeurs de données sur le darkweb proposent généralement un catalogue de produits organisés par catégorie.

Au sommet de la hiérarchie se trouvent les packages de données complètes appelés "fullz".

Ces bundles contiennent essentiellement tous les éléments nécessaires à un criminel pour usurper complètement votre identité en ligne et hors ligne.

Le prix d'un fullz varie selon la qualité et la localisation de la victime.

Selon les données collectées par les chercheurs en cybersécurité en 2025 :

Fullz basiques (pays en développement) : 6$ à 12$

Fullz standard (pays développés) : 20$ à 100$

Fullz premium (avec score de crédit élevé) : 150$ à 250$

Le paradoxe est troublant : votre identité entière, le fruit d'années de construction de votre réputation, de crédit et de votre historique financier, peut être vendue pour le prix d'une pizza.

Les numéros de sécurité sociale américains, les numéros d'assurance maladie européens et d'autres identifiants gouvernementaux sont particulièrement recherchés.

Numéro de sécurité sociale simple : 1$ à 6$

Numéro de sécurité sociale avec validation : 8$ à 15$

Passeport ou permis de conduire : 500$ à 3 000$

Un numéro de sécurité sociale isolé est relativement facile à falsifier ou à deviner (il suit un format prédictible), tandis qu'un passeport ou un permis de conduire valide est beaucoup plus difficile à imiter et peut être utilisé pour des escroqueries de haut niveau comme l'ouverture de comptes bancaires ou l'accès à des services de prêt.

Informations Bancaires et Financières

Les informations bancaires volés sont au cœur du commerce de données sur le darkweb. Ils offrent un accès direct aux ressources financières de la victime.

Un compte bancaire compromis n'est pas seulement une violation de la vie privée c'est un vol direct d'argent. Les prix varient beaucoup selon le type d'accès :

Accès à compte bancaire en ligne : 200$ à 1 000$

Numéro de carte de crédit simple : 5$ à 25$

Numéro de carte de crédit avec cryptogramme (code de sécurité) : 25$ à 120$

Dumps complets de cartes (numéro + crypto + informations du titulaire) : jusqu'à 500$ pour une carte haut de gamme

Les cartes de crédit américaines ont un prix plus élevé que les cartes d'autres nationalités.

Cela reflète simplement la puissance d'achat relative et le fait que les cartes américaines sont en général associées à des limites de crédit plus élevées.

Au-delà des informations financières brutes, les vendeurs proposent un accès direct aux comptes en ligne des victimes ce qu'on appelle des "comptes compromis" ou des "logins".

Les comptes de médias sociaux

Netflix : ~5$
Spotify : ~3$
Instagram premium : ~20$
Comptes email (Gmail, Yahoo, Outlook) : 10$ à 50$ selon l'ancienneté du compte

Comptes de cryptomonnaies et e-wallets

1 100$ à 2 000$ si le compte contient des actifs significatifs

Accès administrateur à un système entreprise

500$ à 100 000$ selon l'importance de l'entreprise

Quand un pirate vole les accès d'un administrateur informatique d'une grande entreprise, cette information est extrêmement précieuse. Elle peut être utilisée pour lancer des attaques de ransomware, voler les données de l'entreprise entière, ou la revendre à d'autres criminels.

Dossiers Médicaux

Parmi tous les types de données volées sur le darkweb, les dossiers médicaux complets sont les plus chers. Cela peut sembler contre-intuitif après tout, pourquoi un dossier médical serait-il plus précieux que l'accès direct à un compte bancaire ? La réponse réside dans la polyvalence criminelle de ces informations.

Un dossier médical complet permet aux criminels de commettre une fraude d'assurance maladie en prétendant être vous et en réclamant de faux traitements, acheter des médicaments sur ordonnance au nom de la victime.

Créer une identité médicale frauduleuse pour un marché noir de services médicaux, usurper votre assurance maladie et épuiser votre couverture. Mais aussi utiliser vos antécédents médicaux pour des applications de prêt ou d'assurance.

Selon les données de 2025, les prix pour les dossiers médicaux sont :

Informations médicales plutôt basiques : 50$ à 150$

Dossier médical avec historique complet d'assurance maladie : jusqu'à 500$ ou plus

Informations médicales très completes : 250$ à 1 000$

Données de Localisation et Métadonnées

La technologie moderne génère des quantités massives de métadonnées. Les données de localisation, en particulier, sont devenues une marchandise précieuse.

Quand vous utilisez une application, quand vous appelez quelqu'un, quand vous naviguez sur le web, votre localisation est enregistrée. Cumulée sur le temps, cette information crée un profil détaillé de votre vie quotidienne.

Selon une investigation menée par Datarade en 2025, les données de localisation de millions de personnes ont été vendues sur le darkweb, parfois de manière « légale » au sens où des data brokers les ont vendues à des acheteurs inconnus.

Le prix de ces données est généralement calculé comme suit :

Données de localisation brutes (point de données) : quelques centimes par enregistrement

Données de localisation agrégées (millions de points) : 10 000$ à 1 000 000$ selon la granularité et la couverture géographique

Données d'Enfants et de Mineurs

Une catégorie criminelle particulièrement sinistre existe sur le darkweb : les données d'enfants et de mineurs. Ces données sont recherchées pour l'abus sexuel d'enfants, le trafic d'enfants et la fraude contre les mineurs.

Nous ne détaillerons pas les prix de ces données par souci de décence, mais il faut noter que cette forme de crime est parmi les plus graves et les plus poursuivies par les autorités à travers le monde.

Source : deepstrike.io

Comment sont volées nos données ?

Avant que les données ne soient vendues sur le darkweb, elles doivent d'abord être volées. Comprendre les méthodes de vol de données est essentiel pour comprendre pourquoi ce phénomène s'est amplifié aussi rapidement.

Les données volées proviennent de nombreuses sources différentes, chacune représentant un vecteur d'attaque distinct.

Violations de Données à Grande Échelle (Data Breaches)

La source la plus spectaculaire de données volées est la violation de données à grande échelle. Quand un pirate pénètre dans les serveurs d'une grande entreprise ou d'un gouvernement et en extrait de vastes quantités de données personnelles, cela crée un afflux soudain de millions de records sur le marché du darkweb.

Les violations de données se produisent généralement par l'une de ces méthodes :

Exploitation de vulnérabilités logicielles

Un pirate découvre une faille dans le code d'une application web qui lui permet d'accéder à la base de données sous-jacente sans se faire identifier. Certaines de ces vulnérabilités peuvent persister pendant des années avant d'être découvertes.

Phishing et Ingénierie Sociale

Le pirate envoie un email prétendant provenir d'une source fiable (un service bancaire, une plateforme de médias sociaux) et demande aux employés de saisir leurs identifiants. Incroyablement, ces techniques rudimentaires restent parmi les plus efficaces. Un seul employé qui clic sur un lien malveillant peut donner aux pirates l'accès à l'ensemble du système.

Accès aux comptes Administrateurs

Les comptes d'administrateur offrent des droits d'accès élevés au système. Si un pirate peut voler ou deviner les codes d'accès d'un administrateur, il peut potentiellement accéder à toutes les données stockées sur ce système.

Cela peut se faire en devinant les mots de passe faibles, en exploitant des options de récupération de compte mal configurées, ou en manipulant un administrateur pour lui faire donner l'accès.

Malware et Rançongiciels

Un malware est un logiciel malveillant qui s'installe sur l'ordinateur d'une victime ou d'une entreprise. Une fois installé, il peut enregistrer les frappes au clavier, voler les fichiers, ou créer des backdoors. Souvent, avant de chiffrer, le pirate copie les données volées pour les revendre sur le darkweb, même si la rançon est payée.

Accès aux Sauvegardes Cloud

Les entreprises stockent souvent des sauvegardes de leurs données sur le cloud. Si ces sauvegardes ne sont pas correctement chiffrées ou sécurisées, un pirate peut y accéder directement.

Données Achetées auprès de Data Brokers

Il y a un aspect légal et semi-légal au commerce de données que nous avons explorer plus en détail dans un chapitre précedent. Mais il est important de noter que certaines données volées vendues sur le darkweb proviennent initialement de data brokers légitimes.

Parfois, ces données trouvent leur chemin jusqu'au darkweb quand les data brokers eux-mêmes sont piratés.

Données Accessibles Publiquement

Contrairement à ce que l'on pourrait supposer, beaucoup de données personnelles vendues sur le darkweb ne sont pas réellement "volées".

Elles sont simplement compilées à partir de sources d'information publiquement accessibles. Les noms, adresses, numéros de téléphone et professions de millions de gens sont disponibles publiquement via les répertoires en ligne, les registres fonciers, les pages jaunes numériques, et même les réseaux sociaux.

Un pirate peut écrire un simple script qui « scrape » ces sources publiques et compile les informations dans une base de données consolidée.

Employés Corrompus

Parfois, les données ne sont pas volées par un pirate externe, mais par un employé mécontent ou corrompu de l'entreprise qui a accès légitime aux données. Cet employé peut copier les données et les vendre sur le darkweb. Ils sont particulièrement dangereux parce qu'ils by-pass généralement tous les systèmes de sécurité externe. Ils savent où les données sensibles sont stockées, comment contourner les alarmes, et comment couvrir leurs traces.

Les Flux d'Argent

Comment l'argent circule-t-il dans l'économie du darkweb ?

C'est une question complexe qui implique plusieurs étapes :

Négociation et Vente
Les acheteurs potentiels contactent le vendeur, négocient le prix (surtout pour les gros volumes), et finalement achètent les données en cryptomonnaie.

Blanchiment de l'Argent
Les cryptomonnaie reçues du darkweb doivent être converties en argent réel utilisable.

a. Échange en Peer-to-Peer
La cryptomonnaie est échangée avec d'autres utilisateurs pour obtenir d'autres types de cryptos ou de l'argent fiat (c'est-à-dire régulier).

b. Mixing
Pour rendre le traçage des fonds plus difficile, la cryptomonnaie est envoyée à travers des "mixeurs", des services qui mélanges les transactions de nombreux utilisateurs, ce qui rend très difficile de suivre l'origine des fonds.

c. Conversion en argent réel
Finalement, les cryptomonnaies sont converties en devises fiduciaires auprès d'échangeurs crypto, souvent à travers une succession de transactions pour éviter les seuils de déclaration.

Utilisation Finale
L'argent blanchis est ensuite utilisé pour acheter des biens, financer d'autres opérations criminelles, ou simplement être investi.

LES CONSÉQUENCES POUR LES VICTIMES

Le vol de données personnelles porte atteinte au droit fondamental du respect de la vie privée. Mais pas seulement ...

Dégâts Financiers

Perte directe d'argent : La conséquence la plus directe est souvent la perte d'argent. Un criminel avec accès à votre compte bancaire peut simplement drainer le compte. Un criminel avec vos informations de carte de crédit peut effectuer des achats frauduleux jusqu'à atteindre votre limite de crédit.

Le FBI a estimé que les pertes directes de fraude en ligne aux États-Unis s'élèvent à 12,5 milliards de dollars en 2023 (880 418 plaintes), soit une augmentation de 22% par rapport à 2022.

Ouverture de Comptes au Nom de la Victime

Un risque plus insidieux est quand un criminel ouvre des nouveaux comptes bancaires, des cartes de crédit, ou même des prêts au nom de la victime. Vous ne découvrez souvent le problème que des mois plus tard quand vous recevez une lettre de la banque demandant le paiement d'un compte que vous n'avez jamais ouvert.

Perturbation Fiscale

Un voleur d'identité peut utiliser vos documents d'impôt pour déposer une fausse déclaration de revenus et réclamer un remboursement d'impôt en vôtre nom propre.

Abus de Crédit

Les criminels peuvent prendre des prêts au nom de la victime et simplement ne pas les rembourser. Pendant ce temps, le taux de crédit du vrai propriétaire du nom aumgente. Cela peut nuire à votre capacité d'obtenir des prêts pour une voiture, une maison.

Fraude médicale

Si les dossiers médicaux de la victime sont volés, un criminel peut utiliser la couverture d'assurance de la victime pour obtenir des traitements médicaux coûteux.

La victime découvre seulement le problème plus tard quand elle reçoit une facture pour des services qu'elle n'a jamais utilisés, ou quand sa couverture d'assurance est complètement épuisée par de fausses réclamations.

Perte de Couverture d'Assurance

Si vous avez une assurance maladie et qu'un criminel vous vole votre couverture pour des traitements coûteux, votre compagnie d'assurance pourrait résilier votre contrat. À aucun moment cela est de votre faute, vous êtes la victime mais vous vous retrouvez sans assurance maladie.

Ordonnances Frauduleuses

Les criminels peuvent utiliser votre identité pour obtenir des médicaments sur ordonnance, notamment des opioïdes et d'autres substances contrôlées. Non seulement cela ajoute de faux frais médicaux, mais cela crée aussi un enregistrement ou vous avez obtenu des drogues que vous n'avez jamais cherchées, ce qui peut causer des problèmes avec la justice.

Conséquences Professionnelles et Criminelles

Les victimes de fraude d'identité doivent souvent elles-mêmes initier le processus de réclamation.

Elles doivent prouver qu'elles ne sont pas responsables de la fraude et le fardeau de la preuve repose souvent sur la victime, pas sur le criminel ou l'institution financière qui a échoué à prévenir la fraude

Antécédents Judiciaires Frauduleux

Dans les cas extrêmes, un criminel peut commettre des crimes au nom de la victime. Cela signifie que votre nom et votre dossier judiciaire numérique deviennent associés à des infractions criminelles que vous n'avez jamais commises.

Emploi

Les employeurs vérifient régulièrement les antécédents criminels des candidats à l'emploi. Un dossier entaché par la fraude d'identité peut disqualifier le candidat de nombreuses positions, en particulier celles impliquant la confiance ou l'accès à des informations sensibles.

Casier Judiciaire Permanent

Même si vous réussissez à prouver que vous n'avez pas commis les crimes imputés à votre nom, le casier judiciaire reste souvent sur les registres publics. Les futurs employeurs et partenaires verront qu'il y a un enregistrement criminel.

Impact Psychologique et Émotionnel

Combien de temps faut-il pour se rétablir complètement d'une usurpation d'identité ?

Malheureusement, il n'y a pas de réponse simple. Cela dépend de l'ampleur de la fraude. Pour les cas simples (un compte ouvert frauduleusement), vous pouvez résoudre le problème en quelques semaines. Pour les cas complexes le processus peut prendre des années.

Traumatisme Psychologique

Les victimes d'usurpation d'identité signalent régulièrement un traumatisme psychologique important. La violation de découvrir que quelqu'un a utilisé votre identité, s'est présenté comme vous, a interagi avec vos créditeurs et agences gouvernementales en votre nom, peut être très perturbant.

Stress Chronique

Le processus de récupération d'une usurpation d'identité est long cela peut prendre des mois ou des années. Pendant tout ce temps, la victime est en attente, anticipant les prochaines conséquences découvertes, les prochains appels de créanciers, les prochaines lettres de la banque.

Isolement Social

Certaines victimes de fraude d'identité signalent une honte et un embarrassement qui les conduisent à s'isoler socialement. Elles peuvent se sentir responsables, même si la responsabilité réside entièrement chez le criminel et/ou l'entreprise qui a échoué à sécuriser les données.

Rencontre avec l'unité nationale cyber

Hervé Petry
Commandant
unité nationale cyber

Pouvez-vous nous présenter l'unité Nationale cyber ?

L'Unité Nationale cyber (UNCyber) est au sein de l'Unité Nationale de Police Judiciaire (UNPJ), le bras armé opérationnel de la Gendarmerie Nationale dans le cyberespace. Unité de police judiciaire à compétence nationale, basée à Pontoise (95), l'UNCyber conduit les enquêtes de haut spectre en matière de cybercriminalité.

Ses trois missions principales sont :

le renseignement , l'investigation et l'appui technique

Elle coordonne l'action des 26 antennes UNCyber et des 10 000 gendarmes qui composent le dispositif Cybergend, constituant ainsi son allonge dans les territoires métropolitains mais aussi ultra-marins.

Composée de pas moins de 120 personnels, l'UNCyber comporte trois divisions

La Division de l'Animation Renseignement Coordination (DARC), qui fournit des appuis spécifiques comme le renseignement humain, renseignement technique, CERT-GN, coordination nationale et internationale

La Division des Opérations (DO), qui est en charge des enquêtes sur la cybercriminalité organisée de niveau national et international (pédocriminalité, rançongiciels, fraudes en ligne, trafics en ligne…)

La Division Technique (DT) qui assure l'appui technique et criminalistique, par ses capacités projetables au profit de l'échelon local et ses outils d'analyse de la donnée.

L'UNCyber est commandée depuis le 1er février 2024 par **le général Hervé Petry.**

Quel est le rôle de l'UNCyber face aux vols de données ?

L'UNCyber dispose au sein de sa division des opérations et du département criminalité organisée, d'un groupe des atteintes STAD (système de traitement automatisé de données).

Ce dernier a été mis en place pour apporter une réponse opérationnelle face au constat que les PME, collectivités territoriales souvent plus vulnérables, sont de plus en plus régulièrement victimes de cyberattaques par rançongiciels. Toutefois, les grands groupes et grandes entreprises ne sont pas épargnés.

Cela se traduit par des exfiltrations de données et des demandes de rançons pouvant conduire à une désorganisation des infrastructures avec des répercussions économiques conséquentes lorsque les systèmes informatiques sont volontairement bloqués et pris en otage.

Extorquer de l'argent aux victimes, en échange de la promesse de leur restituer l'accès aux équipements ou aux données chiffrées et/ou de la non-divulgation de leurs données dérobées, reste la motivation principale de cette nouvelle forme de délinquance. Ces attaques ont aussi un impact direct sur les concitoyens. Les cyber-enquêteurs du groupe STAD sont ainsi spécialisés dans les vols de données, délinquance cyber moderne pouvant être parfois liée à la criminalité organisée.

La cybercriminalité est un sujet extrêmement important, pour ne pas dire grave eu égard au contexte géopolitique, qui

connaît une constante évolution. C'est une menace qui s'adapte et qui frappe tous les pans de notre société. Les cyberattaques causent en effet des dégâts considérables.

Elles portent atteinte autant à la population qu'à notre tissu économique.

Disposez-vous de chiffres récents illustrant cette menace ?

Les chiffres clés de 2024 confirment cette tendance :

348 000 atteintes numériques enregistrées

soit + 74 % d'atteintes numériques en 5 ans

65 % d'atteintes aux biens,

29,7 % d'atteintes aux personnes,

4,9 % d'atteintes aux institutions et à l'ordre public

17 100 atteintes aux systèmes d'information

Quel type de données les malfaiteurs recherchent-ils et dans quels buts ?

Tout type de données car tout est monnayable : éléments relatifs à l'identité, date de naissance, adresse postale, adresse courriel, numéro de téléphone, numéro d'assuré social, compte bancaire. Cela peut être revendu ou utilisé pour faire des escroqueries, de l'usurpation d'identité, monter des dossiers de financement, d'obtention frauduleuse d'aides.

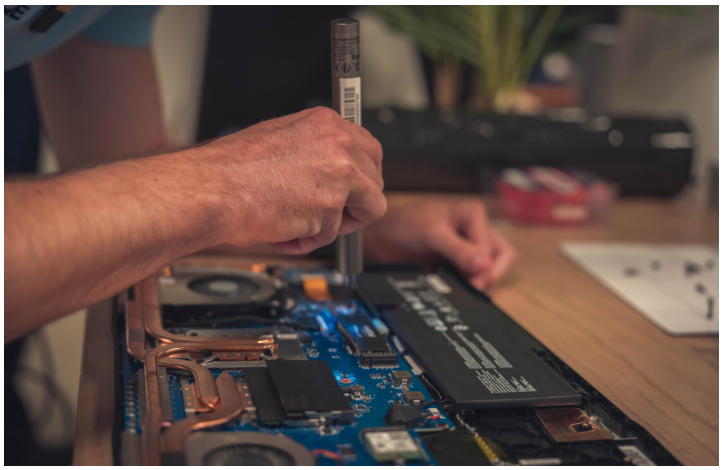
Comment se déroule une journée type de recherche de données sur le Clear Web et le Dark Web ?

Nous ne pouvons parler de journée type pour nos enquêteurs, chaque journée et dossiers traités étant différents.

Il convient de suivre l'actualité, les fils de discussions sur les sites informés, les forums de pirates, de ventes de données, et tous sites pouvant vendre ou proposer de telles informations

La cyber est un marathon pas un sprint !

Credit : Unité Nationale Cyber



Pouvez-vous nous décrire certaines actions entreprises lors de vos missions ?

Dès la découverte d'une fuite de données, il convient de déterminer la "fraîcheur" de celle-ci. Sommes-nous en effet en présence d'une fuite recyclée ou récente ?

Pour cela il faut dans la mesure du possible la télécharger en évitant de se faire contaminer. Il est possible que le ou les fichiers soient piégés.

Si l'origine de la fuite est déterminée (victime), les cyber-enquêteurs contactent cette dernière afin de l'informer et de recueillir sa plainte, ainsi que tous éléments techniques utiles pour l'orientation de l'enquête.

Le cyber-enquêteur va travailler sur le vendeur à la recherche des preuves permettant de matérialiser les faits et son implication. L'objectif recherché est de faire cesser la fuite et accompagner la victime dans les démarches (déclaration CNIL, ANSSI le cas échéant), faire identifier l'origine de la compromission afin d'éviter tout retour des attaquants . Également, identifier et interpeller l'auteur afin de le traduire devant une juridiction de jugement.

Quels dispositifs et conseils de prévention recommandez-vous ?

Plusieurs dispositifs existent pour accompagner les victimes et renforcer la prévention face aux cybermenaces. Les professionnels, notamment les TPE et PME, peuvent s'appuyer sur **17Cyber** en cas d'attaque, ainsi que sur **MonAideCyber,** les référents sûreté et les audits dédiés.

Les particuliers disposent quant à eux de différents outils et plateformes, comme l'application mobile **MaSécurité**, le site **Cybermalveillance.gouv.fr**, ainsi que les services **Pharos, Perceval, Thésée et la brigade numérique.**

En complément, certaines bonnes pratiques restent essentielles pour réduire les risques : activer l'authentification à deux facteurs, maintenir en permanence à jour les systèmes et applications, se former à la sécurité des systèmes d'information, limiter son empreinte numérique, ne jamais réutiliser un mot de passe et recourir à des gestionnaires de mots de passe.

Il est également recommandé de s'appuyer sur le guide de cybersécurité de l'ANSSI, qui constitue une référence en la matière.

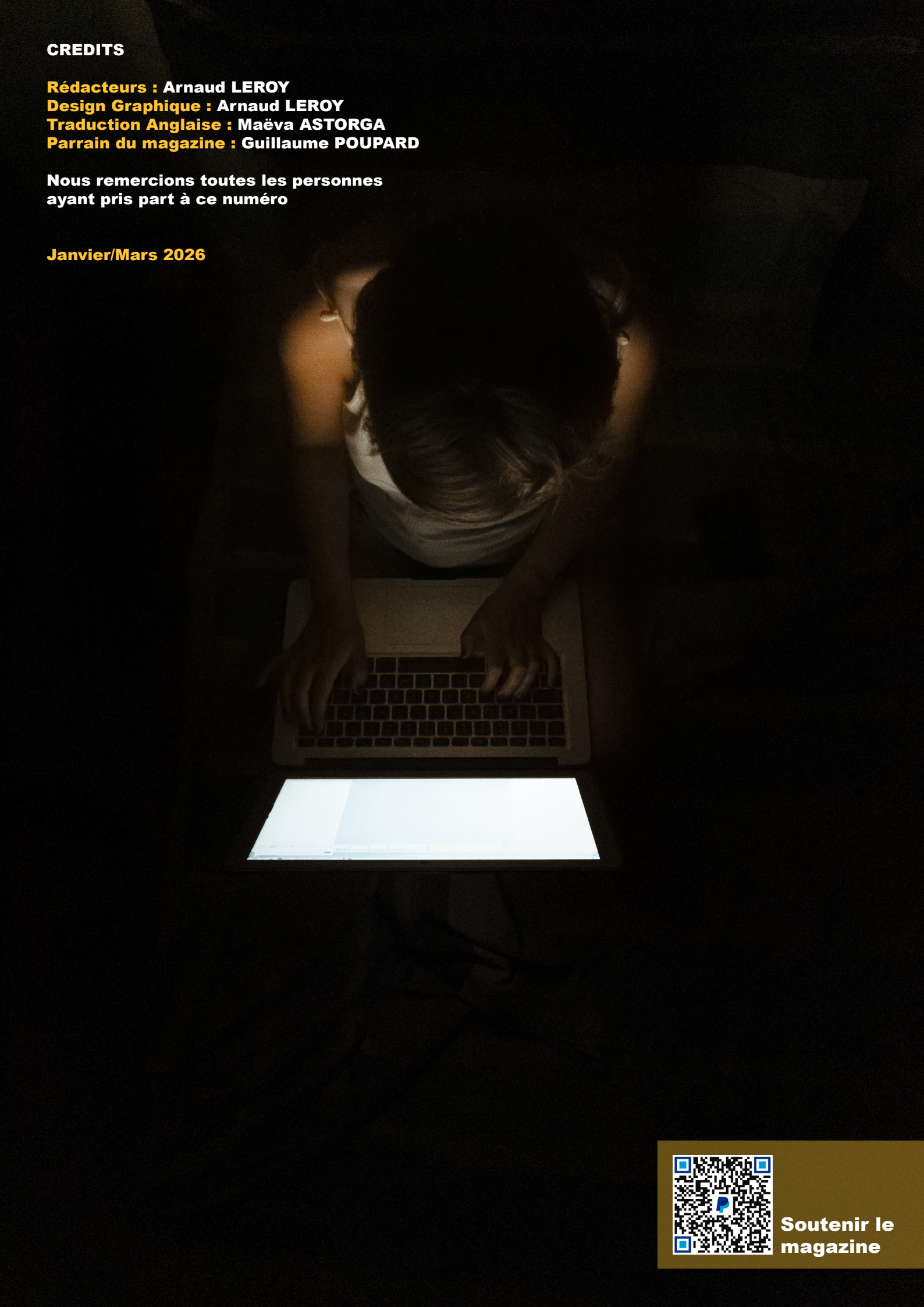
Credit photos : Unité Nationale Cyber

CREDITS

Rédacteurs : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume POUPARD

Nous remercions toutes les personnes ayant pris part à ce numéro

Janvier/Mars 2026



Soutenir le magazine