LA CYBER SÉCURITÉ POUR TOUS

Le guide essentiel

AUX CITOYENS | AUX JOURNALISTES | AUX ASSOCIATIONS

CYBERFORGOOD.ORG

LA CYBER SÉCURITÉ POUR TOUS

ADVENS FOR PEOPLE AND PLANET

CYBERFORGOOD.ORG

↑ SOMMAIRE

EN CHIFFRES

6 MILLIARDS
d'internautes dans le monde en 2025

74 %
de la population en ligne

6H38 PAR JOUR
Le temps moyen qu'un internaute passe en ligne dans le monde

1H48 PAR JOUR
Le temps moyen quotidien passé sur les réseaux sociaux en France

90 %
des cyberattaques trouvent leur origine dans une erreur humaine

13 000
satellites tournent autour de la Terre (2025)

5 400 DATA CENTERS
aux États-Unis (2025)

750 INCIDENTS
déclarés en 2024 dans les établissements de santé français

40 %
des entreprises françaises ont subi au moins une cyberattaque significative en 2025

Comprendre et agir face à la menace cyber

de Grégoire Ducret et Giulio Zucchini

Le numérique a transformé profondément notre société. Travail, santé, information, administration, éducation, divertissement… Aucun domaine de notre vie publique ou privée n'a pu éviter cette révolution bâtie sur des nouvelles infrastructures, connaissances, outils, et usages. Nous avons gagné en efficacité. Nous n'avons jamais disposé d'autant de services et d'informations rien qu'à travers notre smartphone : services bancaires, administratifs, de consommation.

Désormais, le numérique fait partie intégrante de notre vie en tant que citoyen et travailleur ou retraité, client ou industriel, administré ou patient. Nos données personnelles voyagent d'un serveur à l'autre à travers des satellites ou via des câbles sous-marins, elles sont stockées dans des data centers à Aubervilliers, en Suède, en Chine ou aux États-Unis… Les données de nos entreprises, de nos associations, de nos hôpitaux et de nos médias sont quelque part dans le cloud, toujours accessibles et disponibles.

Les bénéfices sont immenses, mais cette transformation comporte aussi un risque majeur, celui de voir ces données accessibles à des acteurs malveillants. Si la révolution numérique s'est imposée au niveau global avec une rapidité inédite, elle n'a pas toujours été accompagnée par une culture, une compréhension et des pratiques nécessaires à la protection de nos données.

La cybersécurité est là pour anticiper ces risques. Elle permet de mieux protéger nos données. Si le mot « cyber » renvoie à des expertises techniques d'ingénieurs, hacker ou informaticien, une meilleure compréhension du fonctionnement d'Internet et des bonnes pratiques à mettre en place pourraient suffire pour mieux protéger nos données personnelles.

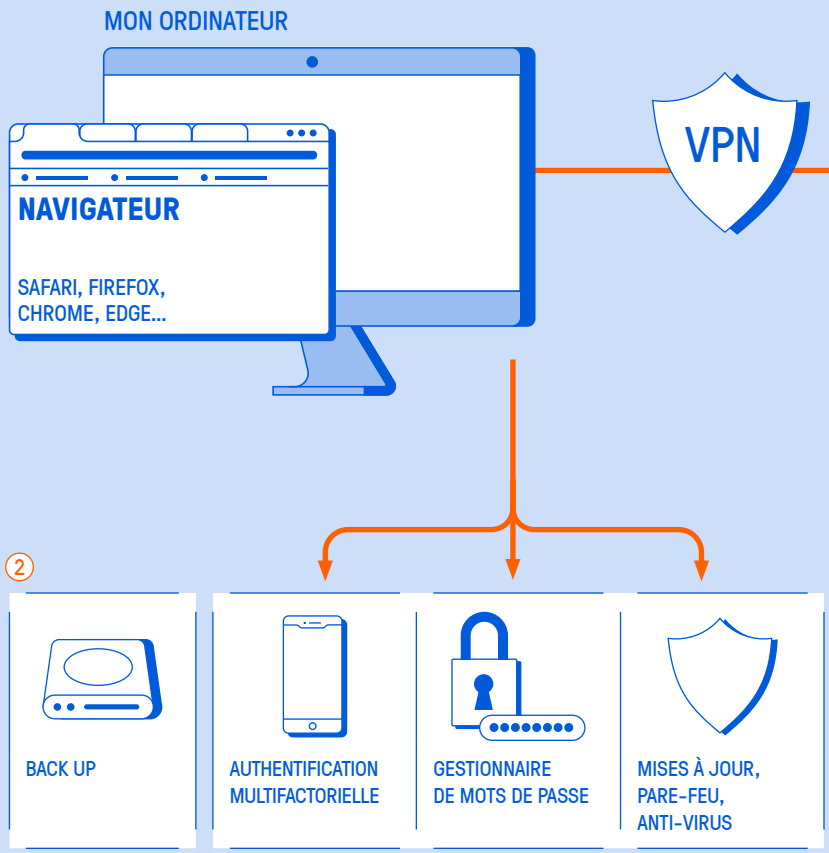
Nous avons rédigé ce guide pour cette raison. Il permet de mieux comprendre le fonctionnement d'Internet, de tirer profit du numérique en confiance, d'explorer les modes opératoires des attaques cyber et de mettre en place de bonnes pratiques afin de mieux se protéger. Conçu avec les experts cyber d'Advens dans le cadre du programme d'intérêt général *Cyber for Good*, ce guide transforme l'expertise cyber de pointe en repères concrets pour le quotidien et en bonnes pratiques accessibles à tous.

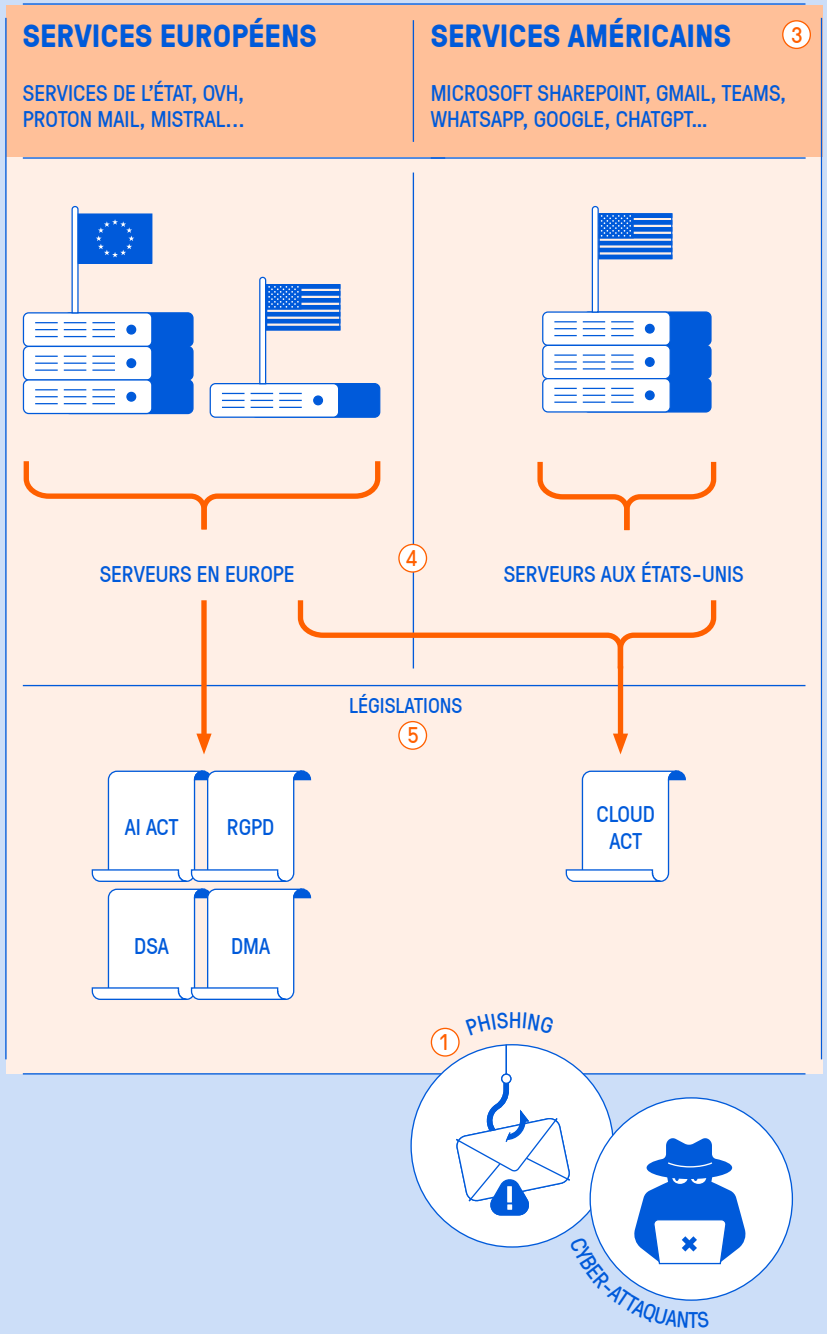
En 2026, nous croyons que la cybersécurité n'est plus uniquement un sujet technique pour les professionnels, mais une expertise nécessaire à tout citoyen, responsable associatif, journaliste, maire ou entrepreneur.

Bonne lecture !

↑ SOMMAIRE

La cyber, mode d'emploi pour le quotidien





↑ SOMMAIRE

① Se repérer dans l'univers cyber

② Les 10 bonnes pratiques

③ L'intelligence artificielle : alliée ou danger ?

④ Souveraineté numérique

⑤ RGPD : données et conformité

↑ SOMMAIRE

SE REPÉRER DANS L'UNIVERS CYBER

1

Ce module permet de comprendre
le fonctionnement des menaces numériques
et pourquoi personne n'est à l'abri.

Que vous soyez un entrepreneur,
un responsable associatif, un journaliste
ou un citoyen, vous apprendrez à reconnaître
les signaux d'une attaque, à identifier
les pratiques à risque dans le quotidien
et à adopter les bons réflexes pour réduire
votre exposition aux risques cyber.

1.1 Qu'est-ce que le cyberespace ?

Le cyberespace désigne l'espace virtuel créé par l'interconnexion des réseaux numériques au niveau mondial. Il ne s'agit pas d'un lieu physique, mais d'un environnement constitué d'ordinateurs, de serveurs, de câbles sous-marins, de satellites, de smartphones et de milliards de données en circulation. Dans cet environnement nous interagissons et échangeons des informations. Aujourd'hui, chaque mail envoyé, chaque paiement en ligne, chaque message sur un réseau social transite sur le cyberespace. Si nous utilisons quotidiennement ces réseaux, nous connaissons mal leur fonctionnement et les risques associés.

TOUS CONNECTÉS, TOUS MENACÉS

Qu'est-ce que le numérique représente dans le monde ? En 2023, plus de 5,3 milliards de personnes utilisaient Internet, soit environ 65 % de la population mondiale et 79 % des personnes âgées de 15 à 24 ans, selon l'Union internationale des télécommunications.

L'économie numérique représente plus de 15 % du PIB mondial d'après les estimations de la Banque mondiale. Le numérique est aujourd'hui le socle infrastructurel de notre vie privée et professionnelle. Or, à mesure que son utilisation et son périmètre s'étendent, les risques et les menaces augmentent également. En 2024, 348 000 atteintes numériques ont été enregistrées, soit une augmentation de + 74 % enregistrée en 5 ans : 65 % des attaques visent les biens, 29,7 % les personnes, 4,9 % les institutions et l'ordre public, selon le Commandement du ministère de l'Intérieur (COMCYBER-MI).

1.2 L'augmentation des attaques cyber

En France, les incidents cyber ont augmenté de manière significative ces dernières années. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) traite chaque année des milliers de signalements d'attaques visant les entreprises, les collectivités et les particuliers. Le cyberespace est devenu un pilier de notre vie quotidienne : travail, santé, éducation, services publics, loisirs. Mais c'est aussi un espace d'opportunités pour la criminalité, l'espionnage ou la désinformation. Comme tout espace commun, il nécessite des règles, des compétences et une vigilance partagée.

LA CYBERSÉCURITÉ NOUS CONCERNE TOUS

Comprendre le cyberespace, c'est donc comprendre que derrière l'écran se trouvent des infrastructures réelles, des acteurs multiples – publics et privés, européens et internationaux – et des enjeux stratégiques majeurs. Qu'il s'agisse de nous en tant qu'individus ou des organisations dans lesquelles nous travaillons, nous sommes tous des cibles potentielles dans cet espace. La cybersécurité nous concerne tous aujourd'hui. Ce guide a pour objectif de rendre cet univers accessible à tous, afin que chacun puisse en profiter en confiance et en sécurité.

EN CHIFFRES | QUI UTILISE INTERNET ?

6 MILLIARDS
d'internautes dans le monde en 2025

74 %
de la population en ligne

94 %
de la population française

79 %
des personnes âgées de 15 à 24 ans

15 %
du PIB mondial provient de l'économie numérique

Source : Statistiques de l'Union internationale des télécommunications (UIT), 2024.

LES CYBERATTAQUES : TOUS CIBLÉS ?

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), une cyberattaque « consiste à porter atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants. » Dans le domaine cyber, le terme « malveillant » se réfère à tout acte intentionné visant à nuire à un système informatique ou corrompre des données par l'usage d'un logiciel. Elle répertorie quatre grandes finalités des cyberattaques (qui) sont : l'appât du gain, la déstabilisation, l'espionnage et le sabotage. Oui, mais qu'est-ce que cela veut dire pour vous ?

UN MATIN COMME TOUS LES AUTRES...

Vous êtes à votre bureau, avec votre ordinateur et tentez de vous rendre sur votre boîte mail. Or votre mot de passe ne fonctionne plus. Pourtant, vous savez que c'est le bon. La chaleur monte doucement, mais la confiance persiste. Après tout, pourquoi quelqu'un voudrait-il s'emparer de cette boîte mail ? Il n'y a rien d'intéressant à y voler. Par acquit de conscience, vous en parlez à votre collègue. Stupeur, tout fonctionne pour elle. Elle s'apprêtait d'ailleurs à répondre à votre mail envoyé la veille, une invitation à contribuer au pot de départ de Marc de la compta. Sueurs froides : ce message, vous ne l'avez jamais envoyé. Une certitude s'impose alors : votre boîte mail a été piratée.

L'ERREUR HUMAINE RESTE LE PREMIER FACTEUR DE RISQUE !

60 % DES VULNÉRABILITÉS NUMÉRIQUES IMPLIQUENT L'HUMAIN

Source : Verizon Data Breach Investigations Report (DBIR) 2025

1.3 Pourquoi moi ?

« Je n'ai rien à cacher, je ne suis personne ! » Cette phrase revient souvent, comme si l'anonymat protégeait des risques numériques. Elle fait écho à une autre idée reçue : pourquoi un pirate viserait-il une simple boîte mail ou la petite structure du coin plutôt qu'un grand groupe du CAC 40 ? En réalité, cette croyance est précisément ce qui fragilise. Pour comprendre cela, il faut adopter le point de vue de l'attaquant. Son objectif n'est pas toujours de frapper fort, mais de frapper facilement. Entre une organisation bien protégée et une autre qui repousse les mises à jour, utilise le même mot de passe partout ou ne forme pas ses équipes, le choix est vite fait.

ATTAQUER UNE PETITE STRUCTURE : QUEL INTÉRÊT ?

Peut-être, pensez-vous : « Les petites entreprises et les associations sont trop modestes pour intéresser les acteurs malveillants. » Mais c'est faux ! Elles détiennent des fichiers d'adhérents, des coordonnées bancaires, des données internes, parfois sensibles... Il y a un écart important en termes de préparation entre les grandes ONG et celles plus petites qui ont peu de moyens à allouer dans la cybersécurité. Pourtant, les cybercriminels s'attaquent à tous types de structures, indépendamment de leur taille ou de leur rôle dans la société.

L'enjeu n'est pas de devenir invincible mais d'élever son niveau de protection. Pour cela vous pouvez adopter des bonnes pratiques dès à présent : mettre à jour vos outils, utiliser des mots de passe robustes, activer la double authentification, sauvegarder régulièrement vos données. Ces gestes simples constituent les fondations solides nécessaires pour mieux vous protéger (cf : Chapitre 2 : les 10 bonnes pratiques). Ils ne garantissent pas le risque zéro, mais ils réduisent fortement l'impact d'un incident. Dans le domaine de la cyber, la vigilance ordinaire permet de réduire considérablement les risques.

↑ SOMMAIRE

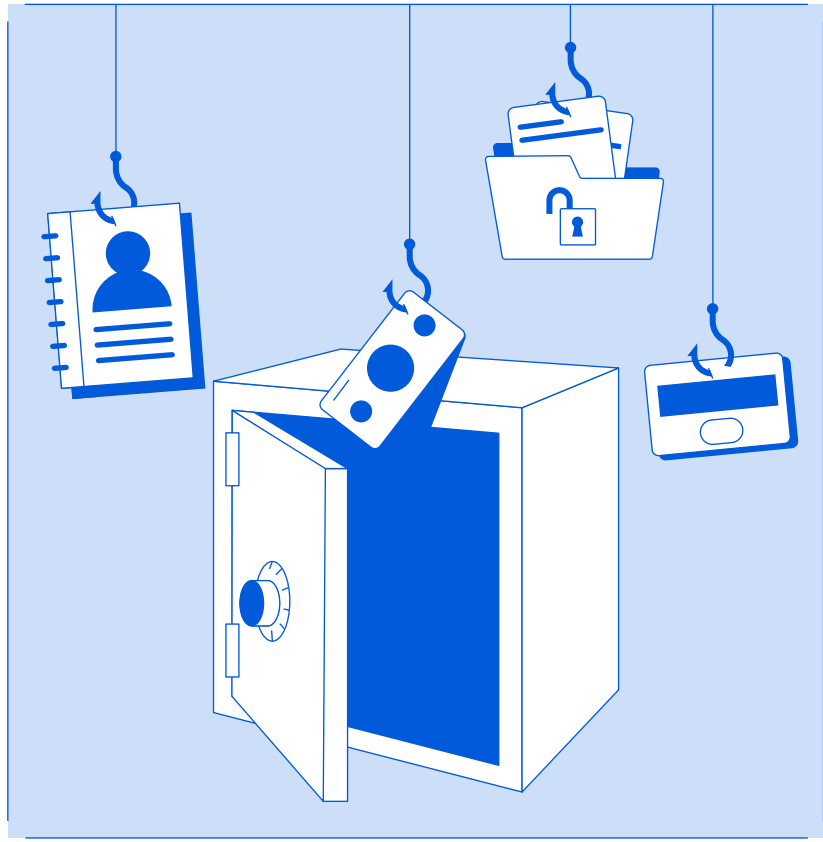
LES ONG ET LES ASSOCIATIONS : DES CIBLES CYBER

AMNESTY INTERNATIONAL ÉTÉ 2018	Tentative d'installation du logiciel espion Pegasus (NSO Group). Lien avec une campagne saoudienne pour surveiller des défenseurs des droits des femmes.
COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR) JANVIER 2022	Attaque APT ultra-ciblée. 515 000 dossiers de personnes vulnérables compromis via 60 Croix-Rouge nationales. Code malveillant conçu spécifiquement pour le CICR.
SAVE THE CHILDREN INTERNATIONAL SEPTEMBRE 2023	Ransomware BianLian : ~6,8 To de données exfiltrées. Données financières, médicales, personnelles. ONG présente dans 116 pays ciblé par extorsion.

Source : CICR, Amnesty International, Save the Children International.

1.4 Les typologies des attaques

Une boîte mail piratée n'est jamais un incident anodin. Derrière ce qui peut paraître un simple accès non autorisé se cache en réalité un effet domino aux conséquences multiples. Votre messagerie concentre des informations stratégiques : contacts, échanges internes, documents administratifs, factures, projets en cours. Elle constitue à la fois un carnet d'adresses, une mémoire d'activité et un sésame vers d'autres services en ligne. Dès lors, le cybercriminel y voit une mine d'or pour ses activités. Mais que compte-t-il faire de ces données ?



DANS LA TÊTE D'UN CYBERCRIMINEL

À partir d'un seul compte compromis, il devient possible d'orchestrer des arnaques crédibles, de diffuser des logiciels malveillants, de revendre des données ou d'usurper une identité. Chaque message, chaque pièce jointe, chaque information conservée peut être détournée de son usage initial. Les menaces qui en découlent sont variées : escroqueries ciblées, paralysie de l'activité par rançongiciel, revente de données personnelles, atteinte à la réputation ou sabotage des outils de communication. Comprendre ces risques, c'est mesurer qu'une messagerie professionnelle n'est pas qu'un outil pratique du quotidien : c'est un maillon central de la sécurité de toute une organisation.

PHISHING ET ARNAQUES CIBLÉES

risque 01

Des e-mails frauduleux peuvent être envoyés depuis votre compte aux membres de votre association, partenaires ou contacts, dans le but de soutirer des informations sensibles ou de l'argent. Ces messages usurpent votre identité pour se rendre crédibles : ils peuvent demander des paiements de factures fictives, solliciter des « dons » (comme dans l'exemple de la cagnotte pour Marc), ou proposer des liens vers de faux sites pour voler des identifiants ou des coordonnées bancaires. Cette technique exploite la confiance que vos contacts ont en vous.

Ces messages dits de « *phishing* » ou hameçonnage sont d'autant plus dangereux qu'ils peuvent gagner en crédibilité grâce aux autres informations glanées en consultant votre boîte de réception. En parcourant vos anciens échanges, les pirates collectent des éléments de contexte (le nom d'un collègue, un projet en cours, ou encore le départ prochain d'un collaborateur) pour construire un message convaincant et difficile à repérer avec son apparence d'authenticité.

LE PHISHING, LA PREMIÈRE MENACE

1,9 M
de consultations d'articles (+13 %) sur cybermalveillance.gouv.fr

64 000
recherches d'assistance (+22 %)

LE TOP 3 DES HAMEÇONNAGES LES PLUS FRÉQUENTS

234 356
infractions routières

156 984
infractions pédopornographiques

149 658
livraison de colis

RANSOMWARE

risque 02

Le pirate peut également utiliser l'accès à votre messagerie pour diffuser des liens de téléchargement vers un *ransomware* (ou rançongiciel). Concrètement, il s'agit d'un logiciel malveillant qui chiffre les fichiers ciblés et peut paralyser partiellement ou totalement l'activité de votre structure : documents internes, bases de données, informations stratégiques deviennent soudainement inaccessibles. Dans ce cas de figure, la motivation des hackers est avant tout financière. Certains attaquants menacent de publier ou de vendre les informations volées si la rançon n'est pas versée.

Quel est leur moyen de pression ? Ils détiennent la clé de chiffrement et exigent une rançon pour remettre l'infrastructure en état de fonctionnement. Pour provoquer une telle compromission des systèmes, les attaquants ont souvent besoin d'une seule chose : qu'un utilisateur télécharge le logiciel sur l'une des machines du réseau de l'association ou de l'entreprise. Pour ce faire, votre boîte mail est une mine d'or avec ses adresses, son historique et ses messages. En ouvrant une pièce jointe qui semble anodine (un tableau, une facture, une invitation), un employé ou un bénévole permet au rançongiciel de se déployer et compromettre la sécurité de toute la structure.

LES RANÇONGICIELS EN CHIFFRES

7
cyberattaques sur 10 dans le monde en 2023

+ 300 millions
de tentatives enregistrées

PERTURBATIONS LES PLUS LOURDES :

1. Arrêts d'activité
2. Fuites de données
3. Chantage

Source : Statista et ANSSI (2024)

VENTE DE DONNÉES PERSONNELLES

risque 03

L'opportunité financière peut se présenter sans même recourir à un *ransomware* ou au vol des coordonnées bancaires d'un collaborateur. À vrai dire, pirater votre boîte mail représente déjà une petite victoire pour le hacker. Les informations récupérées – adresses, numéros de téléphone, échanges confidentiels, documents internes – ont une valeur marchande appréciable pour d'autres cybercriminels : elles sont revendues sur des places de marché du dark web où elles alimentent des attaques, vols d'identité ou campagnes de spam. Un dossier contenant des fichiers personnels ou professionnels peut se monnayer entre 100 et 1 000 €, selon la richesse des données et leur fraîcheur sur les forums cybercriminels.

LA VENTE DE DONNÉES PERSONNELLES

41 %
des Français déclarent avoir déjà été victimes d'une utilisation frauduleuse de leurs données personnelles

21 %
ont subi un préjudice financier direct

740 €
le préjudice financier moyen par victime

915 €
le préjudice financier moyen par victime, en cas d'usurpation d'identité

Sources : Cybercriminalité : risques et conséquences pour les données personnelles | CNIL

↑ SOMMAIRE

USURPATION D'IDENTITÉ
risque 04

L'usurpation d'identité n'a malheureusement rien d'une fiction. Elle surgit lorsque des copies de documents administratifs sensibles tels qu'une pièce d'identité, des justificatifs ou des factures se trouvent en pièces jointes dans votre messagerie. Une fois ces documents récupérés, le champ des possibles s'élargit : ouverture frauduleuse de comptes bancaires en ligne, souscription à des micro-crédits, création de comptes sur des plateformes de paiement (PayPal, crypto-monnaies, etc.) pour des opérations de blanchiment d'argent. Toutes ces démarches peuvent se faire à votre insu, en s'appuyant sur les preuves numériques récupérées dans votre boîte mail. Les conséquences ne s'effacent pas d'un simple clic : ce type de fraude débouche souvent sur des années de démarches pour rétablir la vérité et effacer des dettes.

DIFFAMATION ET SABOTAGE
risque 05

Pour votre association ou entreprise, le risque est aussi réputationnel. Le piratage d'une boîte mail peut offrir au hackeur une porte d'entrée vers d'autres plateformes de communication. En prétextant un simple oubli de mot de passe et en se connectant via un lien reçu sur la messagerie compromise, il peut se frayer un chemin jusqu'à votre site web, vos comptes professionnels ou vos réseaux sociaux. À partir de là, tout devient possible : publication de messages compromettants, diffusion de fausses informations ou même de contenu idéologique et politique, le tout, à votre insu.

L'objectif est clair : ternir votre image, celle de l'association, ou semer la confusion auprès de vos membres et partenaires. Et parce que la plupart des utilisateurs réutilisent leurs mots de passe sur plusieurs services, l'intrusion ailleurs devient d'autant plus facile. De plus, le risque est croissant si le mot de passe contient des données pouvant être retrouvées par le hacker en ligne. Cette habitude, pourtant anodine en apparence, est l'une des plus dangereuses dans la gestion des accès.

À SAVOIR | LE CAS DE LA CYBERATTAQUE CONTRE LE COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR).

Le 18 janvier 2022, une cyberattaque a exposé les données de plus de 515 000 personnes. Les données du CICR portaient sur des personnes affectées par des conflits, des catastrophes ou des migrations, cherchant des proches disparus ou à préserver la dignité de personnes décédées.

1.5 La menace informationnelle

Les atteintes à la cybersécurité ne se limitent plus aux systèmes techniques : elles fragilisent aussi l'espace informationnel, facilitant la désinformation et les stratégies d'ingérences numériques étrangères visant à déstabiliser les sociétés démocratiques. Un environnement social, économique et informationnel dégradé constitue un terreau fertile pour les manipulations de l'information. Dans un contexte de défiance envers les institutions et les médias « traditionnels », les journalistes représentent aujourd'hui une cible privilégiée pour les acteurs de la menace informationnelle. Afin de bien comprendre la crise de l'information que traversent actuellement les sociétés démocratiques, et comment celle-ci peut être instrumentalisée par les acteurs de la menace informationnelle, il convient d'abord de s'intéresser à ses causes structurelles.

Ce module a été rédigé par les équipes de VIGINUM, le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères.

UN ÉCOSYSTÈME INFORMATIONNEL DÉGRADÉ

Pour comprendre la dégradation de l'écosystème informationnel, trois causes structurelles méritent d'être soulignées :

1 La concentration des groupes de presse

Si l'on ne peut en tirer des conclusions définitives sur le pluralisme éditorial, la concentration de plusieurs groupes de presse dans les mains de quelques personnes favorise des stratégies de captation de l'attention fondées sur des logiques commerciales et d'influence, souvent au détriment de l'investigation journalistique, la neutralité et l'indépendance.

2 L'érosion des modèles économiques de la presse

Depuis des années, les modèles économiques de la presse traditionnelle sont fragilisés par les mutations technologiques (essor du numérique et des réseaux sociaux qui permettent un accès gratuit à l'information et une concurrence accrue etc...) et socioculturelles (transformation des modes de consommation et d'accès à l'information etc...).

Par ailleurs, les recettes publicitaires de la presse écrite ont chuté de 50 % en une décennie, sous l'effet de la captation croissante des revenus par les grandes plateformes numériques.

Enfin, la transition numérique de la presse traditionnelle peine à s'accompagner d'un modèle économique pérenne : par exemple, les taux de conversion des lecteurs gratuits en abonnés payants demeurent encore relativement faibles. Il en résulte une baisse des effectifs dans les rédactions, une surreprésentation des contenus à fort potentiel de viralité, souvent émotionnels et / ou polémiques, au détriment de formats longs et du journalisme d'investigation.

3 La fragmentation des audiences

Comme mentionné précédemment, de multiples sources d'informations se retrouvent aujourd'hui en concurrence dans l'espace informationnel. L'offre informationnelle est telle que les audiences se trouvent très fragmentées. Elles se structurent et se polarisent bien souvent en fonction des générations et des profils socioculturels. Faute de pouvoir maintenir un lien de confiance stable avec ces différents publics, les médias traditionnels cèdent du terrain à des « médias alternatifs » aux lignes éditoriales souvent plus polarisées, clivantes et idéologiques.

Par ailleurs, on ne peut comprendre la crise de l'information et les défis auxquels sont confrontés les médias traditionnels sans prendre en compte le rôle des réseaux sociaux dans la production et la diffusion de l'information, ainsi que leurs algorithmes de recommandation. Par exemple, il est utile de comprendre que ces algorithmes sont conçus pour maximiser l'engagement, et ainsi, les revenus des plateformes. Cela favorise systématiquement la viralité de contenus émotionnels, sensationnalistes et polarisants.

En outre, la diffusion de ces contenus est facilitée sur les réseaux sociaux. Par un simple clic, il est possible pour un contenu d'atteindre très rapidement des audiences massives et hétérogènes, bien au-delà de la communauté initiale. Les acteurs de la menace informationnelle tirent parti de cette situation dégradée pour mettre en place des modes opératoires informationnels qui ciblent les médias traditionnels et qui tentent de discréditer le travail des journalistes.

En ciblant ces médias, et de ce fait, l'importance de la place de ces derniers dans nos sociétés démocratiques, ces acteurs exacerbent la dégradation du champ informationnel. En brouillant les frontières entre le vrai et le faux, en incitant les internautes à se tourner vers des médias alternatifs, et en instaurant un scepticisme généralisé où le doute envers toute source d'information devient permanent, ces acteurs finissent par éroder la confiance des citoyens dans les processus démocratiques. VIGINUM a documenté plusieurs des techniques, tactiques et procédures (TTPs) employées par les acteurs de la menace informationnelle ciblant les médias.

L'USURPATION DE L'IMAGE DE MÉDIAS ET LE TYPOSQUATTING

Le typosquatting est une technique qui a souvent été documentée dans les investigations de VIGINUM. Il s'agit d'un procédé consistant à usurper l'identité de sites web connus en enregistrant un nom de domaine très proche du nom de domaine officiel. Cette technique sert à tromper les internautes peu avertis et s'accompagne souvent d'une usurpation de l'identité visuelle du site web concerné. Le typosquatting est souvent utilisé également dans les activités de *phishing*.

À SAVOIR | FRANCE DIPLOMATIE EN 2023

Le site France Diplomatie a été typosquatté en 2023 par des acteurs russes. Cela signifie simplement que le site de France Diplomatie a été copié afin de propager des fausses informations en usurpant l'identité du site officiel. Exemples de sites typosquattés :

DIPLOMATIEGOV.FR → DIPLOMATIE.GOUV.FR

LA-POSTE.FR → LAPOSTE.FR

FAACEBOOK.COM → FACEBOOK.COM

LA CRÉATION DE FAUX MÉDIAS, FAUX ARTICLES ET FAUX REPORTAGES

L'une des techniques fréquemment utilisées par les acteurs à l'origine des manipulations de l'information consiste à créer des faux sites d'information et autres médias « alternatifs ». Ces sites peuvent prendre l'apparence de sites de médias « légitimes » proposant une large gamme de contenus, dont des faux articles et faux reportages vidéo (parfois générés avec l'aide de l'IA) centrés sur des narratifs créés de toute pièce ou trompeurs ou encore des images et vidéos sorties de leur contexte etc... Le tout suivant une ligne éditoriale bien souvent clivante et polarisante, cherchant à exacerber les tensions déjà existantes au sein de nos sociétés. Dans le cadre de ses investigations, VIGINUM suit des modes opératoires informationnels (MOI) qui ont notamment recours à la création de faux sites d'informations et à la diffusion de faux articles et reportages.

À SAVOIR | STORM-1516, LA DÉSINFORMATION RUSSE S'INVITE DANS L'HEXAGONE

Storm-1516 est le nom d'un mode opératoire russe de désinformation, actif depuis 2023, qui vise à manipuler l'opinion publique dans plusieurs pays, dont la France. Ce mode opératoire ne consiste pas à pirater des systèmes, mais à fabriquer et diffuser de fausses informations de manière industrielle. On peut l'imaginer comme une « usine à fake news » coordonnée depuis la Russie, avec trois objectifs principaux :

1. ATTAQUER L'UKRAINE ET SES ALLIÉS
On peut prendre le cas d'une rumeur circulant sur les réseaux sociaux quant à une fuite de Zelensky, le 26 février 2022.

2. INFLUENCER LES DÉBATS POLITIQUES EN EUROPE
Durant les élections municipales française de 2026, de nombreux sites web identiques d'informations régionales ont été copiés afin de diffuser des fausses informations. On peut prendre le cas du flash-bourgognefranchecomte.fr qui expliquait le 10 octobre 2025 que « le Panthéon français s'apprête à glorifier un homme qui a trahi la justice ». Or les Français ont particulièrement confiance en la Presse Quotidienne Régionale (PQR). Dès lors, s'attaquer à ces médias revient à détruire un des piliers de la confiance démocratique à une échelle locale et donc influencer des élections.

3. FABRIQUER DES CONTENUS TRÈS CONVAINCANTS
La création d'un faux bandeau CNN « Poutine repousse l'invasion de l'Ukraine jusqu'à ce que Biden envoie des armes à l'Ukraine afin de les saisir » est superposée à une image réelle datant de 2017.

DES MONTAGES PHOTO ET VIDÉO

Ces opérations visent à contrefaire des logos de médias, des affiches de films, des registres publics, des documents gouvernementaux, des factures, des articles de presse ou encore des captures d'écran de réseaux sociaux, notamment pour tenter de « prouver » l'existence de dépenses et de transactions financières compromettantes. Par exemple, Storm-1516 a diffusé, en juillet 2024, une fausse facture visant à faire croire qu'Olena Zelenska (première dame d'Ukraine) avait profité d'une visite officielle de Volodymyr Zelensky en France pour acheter une voiture de la marque Bugatti, d'un montant de 4,5 millions d'euros. De nombreuses incohérences et imprécisions confirment que le document a été contrefait.

1 Des vidéos impliquant des acteurs amateurs

VIGINUM estime que, pour plus de la moitié des opérations imputées au mode opératoire informationnel Storm-1516, ses opérateurs ont recruté des individus pour enregistrer des voix off, jouer des rôles de lanceurs d'alerte, ou intervenir dans une mise en scène. Par exemple, VIGINUM a détecté une vidéo d'une femme se présentant comme une employée du magasin Cartier à New York, où Olena Zelenska aurait soi-disant dépensé plus d'un million de dollars à l'occasion d'une visite du président ukrainien.

2 Des vidéos et audios probablement générés via des outils d'intelligence artificielle générative

Ces outils d'IA permettent de mettre en scène des individus à visage découvert (et non plus des acteurs apparaissant face cachée) mais aussi d'usurper l'identité de personnalités publiques et d'internautes. Par exemple, VIGINUM a détecté une vidéo accusant la CIA de conduire une ferme à trolls pro-Biden à Kyiv qui incluait très probablement une voix « générée de manière synthétique ».
Dans de rares cas, le mode opératoire a également mis en ligne des deepfakes vocaux usurpant l'identité de personnalités politiques, par exemple celle de Barack Obama.

1.6 Le *legal checking*, ou le droit comme outil de protection pour les journalistes et pour les citoyens

Si nous avons des droits, nous avons tout autant de devoirs. Plus particulièrement en tant que journaliste ou communiquant face à la montée de la désinformation, la question du legal checking demeure essentielle. Ce module s'attache à fournir quelques bonnes pratiques à appliquer pour être conscient des enjeux juridiques dans votre travail journalistique et communicationnel.

Ce module a été rédigé par Les Surligneurs, un média indépendant qui lutte contre la désinformation politique. Dans un espace informationnel numérique peu propice à la véracité des faits et des affirmations, où la rapidité de diffusion l'emporte fréquemment sur leur fiabilité, Les Surligneurs utilisent un référentiel fiable : le droit. Cette méthode, pensée tout d'abord pour les journalistes, est une pratique que vous pouvez utiliser dans le quotidien de votre communication, ou en tant que citoyen éclairé. lessurligneurs.eu

QU'EST QU'UNE AFFIRMATION JURIDIQUEMENT VÉRIFIABLE ET EN QUOI CELA IMPORTE DANS VOTRE TRAVAIL ?

Dans un espace public saturé d'informations, le droit est régulièrement simplifié, déformé ou instrumentalisé. Une phrase coupée de son contexte, une interprétation approximative d'un texte de loi, une confusion entre le droit français et le droit européen… et une fausse évidence s'impose. Cette désinformation est particulièrement piégeuse. C'est ce qu'on appelle la désinformation juridique : une forme de fausse information qui ne repose pas sur des faits inventés, mais sur une mauvaise lecture du droit. Un sujet juridiquement vérifiable naît toujours d'une affirmation à portée juridique : une phrase, prononcée dans le débat public, qui prétend décrire ce que dit le droit.

UN CAS PRATIQUE POUR TOUT COMPRENDRE : « L'UNION EUROPÉENNE A-T-ELLE AUTORISÉ LES PAYS MEMBRES À ARRÊTER DES JOURNALISTES COMME L'AFFIRMENT CERTAINS INTERNAUTES ? »

CONTEXTE :
L'UE a adopté de nouveaux textes qui visent à encadrer et renforcer les garanties pour les journalistes. Certains internautes, souvent anti-UE, clament que ce texte permet d'arrêter des journalistes.

POURQUOI VÉRIFIER ?
Comme souvent, l'affirmation touche à la fois à un enjeu juridique (ce que le droit européen permet ou interdit en matière d'arrestation de journalistes) et à un contexte politique sensible, où des internautes ou partis politiques exploitent la peur d'une dérive autoritaire.

RÉSULTAT :
Plus compliqué. Si le texte encadre l'arrestation de journalistes dans certaines procédures, il ne crée pas cette possibilité, qui existe déjà dans le droit français.

COMMENT RÉDIGER UN ARTICLE UTILISANT LE LEGAL CHECKING ?

Vérifier une affirmation juridique n'est que la première étape du travail : encore faut-il savoir comment la raconter. Une fois la règle de droit identifiée et l'analyse établie, le défi du journaliste consiste à transformer cette matière – souvent technique – en un article clair, lisible et fidèle au droit positif.

1 Fondez-vous sur le droit positif et la hiérarchie des normes

Le droit positif ne pose pas de jugement mais renvoie aux lois en vigueur existant à l'état. À l'image du *fact-checking* qui repose sur des faits établis, le *legal checking* repose sur les sources officielles du droit :

- les textes (lois, codes, règlements, traités),
- la jurisprudence (décisions de justice qui interprètent ces textes),
- la doctrine majoritaire, c'est-à-dire la lecture la plus communément admise par les juristes.

Il faut également préciser le niveau de norme mobilisé en se fondant sur la hiérarchie des normes : droit national, droit européen, droit international. En effet, il est possible qu'une affirmation soit correcte selon un texte, mais contredite par une norme supérieure (Constitution, droit européen, droit international).

2 Fondez-vous sur le droit positif et la hiérarchie des normes

Les principaux angles possibles sont :

- **Explicatif :** rendre compréhensible une règle de droit souvent mal connue. Clarifier ce que dit réellement la loi sur un sujet polémique.
- **Rectificatif :** corriger une erreur ou une interprétation abusive. Idéal lorsque l'affirmation fausse circule largement ou influence le débat public.
- **Contradictoire :** présenter une situation où plusieurs lectures juridiques coexistent. Utile lorsque la jurisprudence n'est pas totalement stabilisée ou que les interprétations divergent.

Choisir un angle, c'est décider à quelle question principale votre article répondra.

3 Établissez un plan clair et lisible

Un article de *legal checking* doit suivre une structure rigoureuse pour ne pas perdre le lecteur. Un plan simple et efficace consiste à organiser le texte en trois temps :

- 1. Affirmation à vérifier (claim) et vérification
- 2. Contexte
- 3. Ce que dit le droit

4 Citez vos sources

Pour garantir la transparence et la rigueur, toute affirmation juridique doit renvoyer à la source exacte :

- Jugement d'une affaire
- Article de loi
- Disposition d'un code
- Décision du Conseil d'État
- Arrêt de la Cour de justice de l'UE
- Traité international

LEGAL CHECKING | COMMENT S'ASSURER QUE TOUT EST EN RÈGLE

- Confondre un discours politique avec une règle de droit
- Utiliser des termes juridiques sans les expliquer
- Parler de « loi » à propos d'un texte qui ne l'est pas
- Oublier la hiérarchie des normes
- Négliger le contexte dans lequel le droit s'applique

1.7 Rapport sur l'état de la menace

Dans un contexte de guerres hybrides et de révolutions technologiques, les cyberattaques se sont massifiées et industrialisées. Pour ces raisons, elles sont susceptibles de toucher des organisations de toutes tailles et de tout secteur, dont la vôtre. Aujourd'hui, les vulnérabilités numériques de votre infrastructure importent davantage que la mission de votre organisation.

Ce module n'est pas un document technique, mais une synthèse accessible au grand public du Rapport sur l'état de la menace 2025-2026 publié par Advens, un rapport annuel destiné aux responsables de la sécurité des systèmes d'information (RSSI) et à tous ceux qui veulent protéger leurs organisations contre des menaces en constante évolution.

UN MONDE CYBER EN PLEINE MUTATION : LA « MASSIFICATION » DES ATTAQUES

Massification, voici le mot qui résume le mieux l'année 2025 en cybersécurité, selon le rapport sur l'état de la menace d'Advens. Ce terme décrit un basculement profond : les attaques informatiques ne sont plus des initiatives isolées menées par un hacker solitaire. Elles sont devenues industrielles, organisées comme de véritables entreprises criminelles, avec des équipes spécialisées, des outils standardisés et une capacité à viser simultanément des milliers de cibles potentielles. Cette massification touche trois domaines en particulier, identifiés par Advens comme les plus marquants de 2025.

1 Les vols de données

En France seule, 40,3 millions de comptes ont été compromis sur l'année. Adresses e-mail, mots de passe, numéros de téléphone, coordonnées bancaires : ces données finissent sur des marchés illégaux du dark web, la partie d'Internet inaccessible aux navigateurs classiques, où se tiennent les transactions criminelles, puis sont réutilisées pour des arnaques ciblées ou des intrusions plus profondes.

2 Les attaques via la chaîne de sous-traitance

Les attaquants ne frappent plus nécessairement directement leur cible finale. Ils visent d'abord un prestataire informatique, un fournisseur de logiciels, un partenaire moins bien protégé, puis rebondissent vers l'objectif principal. Pensez-y comme à un cambrioleur qui entrerait chez le serrurier pour voler les clés d'une banque, plutôt que d'attaquer la banque elle-même.

3 L'intelligence artificielle au service des attaquants

L'IA générative amplifie les attaques en les rendant plus convaincantes et en accélérant leur déploiement.

4 Des e-mails d'arnaque presque indétectables

Il fut un temps où repérer un e-mail frauduleux relevait presque du réflexe : fautes d'orthographe flagrantes, tournures maladroites, adresses suspectes… Cette époque est désormais révolue.
Les cybercriminels peuvent à présent produire en quelques heures des milliers d'e-mails parfaitement rédigés, personnalisés au nom du destinataire, adaptés à son secteur d'activité et capables d'imiter avec un réalisme troublant le ton d'une institution officielle ou même d'un collègue.

5 Le vishing : quand l'arnaque passe par appel vidéo

Le *vishing* (contraction de *voice* et *phishing*) est un hameçonnage par la voix. L'attaquant se fait passer pour un technicien informatique, un responsable ou un prestataire et invente une urgence technique pour obtenir l'accès à distance à l'ordinateur de sa cible. Une fois la confiance établie, il installe discrètement un logiciel malveillant.
Ce scénario a notamment été observé dans le cas du groupe Black Basta, qui contactait des employés via Microsoft Teams à partir de comptes externes à leur organisation.

6 Des malwares qui s'adaptent à la volée

Un autre champ de développement de l'intelligence artificielle dans l'arsenal des cybercriminels concerne la création de *malwares* modulaires, ces logiciels malveillants capables de modifier leur comportement en temps réel pour passer entre les mailles des antivirus et des systèmes de détection.

En bref, ces programmes ne se contentent plus d'exécuter un code figé : ils observent leur environnement, s'adaptent aux défenses qu'ils rencontrent et changent de technique ou de signature pour rester invisibles.

LES MENACES QUI ONT MARQUÉ 2025

Ces avancées technologiques, combinées à une exécution sans faille, ont fait de 2025 une année record pour les cyberattaques. Le rapport sur l'état de la menace d'Advens dresse un bilan alarmant, dominé par trois types de menaces qui ont marqué l'année.

1 Les rançongiciels : la prise d'otage numérique

En 2025, cette menace n'a rien perdu de sa vigueur. Le rapport d'Advens recense plus de 8 150 victimes revendiquées dans le monde, soit une hausse de 33 % par rapport à 2024, avec un pic de plus de 1 000 incidents sur le seul mois de février. En France, 180 attaques ont été officiellement revendiquées.

SIX SEMAINES À L'ARRÊT POUR UN MOT DE PASSE OUBLIÉ

L'exemple de Jaguar Land Rover illustre l'ampleur possible des dégâts. En août 2025, le constructeur a été paralysé pendant plus de six semaines par une attaque exploitant des identifiants volés datant de 2021 et jamais changés depuis.

39 000
salariés en chômage technique

2,19 MILLIARDS
d'euros de perte pour l'économie britannique

Tout ça parce qu'une faille de sécurité basique avait été laissée sans correction pendant quatre ans.

2 Les infostealers : des espions invisibles

Un *infostealer*, littéralement « voleur d'informations », est un logiciel malveillant conçu pour récupérer discrètement tous les mots de passe, identifiants de connexion et données sensibles stockés dans les navigateurs ou applications d'un ordinateur, puis les transmettre aux attaquants sans que la victime s'en aperçoive. Ces programmes sont diffusés via des logiciels piratés téléchargés sur des sites non officiels, de faux jeux vidéo, ou des pièces jointes piégées. Ils opèrent

en silence. En 2025, ils ont infecté 27 millions d'ordinateurs dans le monde. En France, 80 millions d'adresses postales ont fini sur le dark web à la suite de ce type de vols.

3 Les fédérations sportives dans le viseur

Le rapport d'Advens cite un cas parlant pour le monde associatif. En 2025, la Fédération Française de Tir (FFTir) a subi une fuite massive : les données de 250 000 tireurs actifs et 750 000 anciens licenciés, état civil, adresses personnelles, numéros de téléphone, se sont retrouvées sur le dark web. La particularité de cette fuite est qu'elle ne touche pas que des noms et des adresses : une grande partie de ces personnes détiennent légalement des armes à domicile. Leur adresse devient alors une information d'une tout autre valeur pour des réseaux criminels. La Fédération Française de Cyclisme a déclaré une fuite similaire en fin d'année.

Ces cas révèlent un angle mort fréquent : les associations et fédérations détiennent souvent des données bien plus sensibles qu'elles ne le réalisent, sans protection adaptée à leur criticité.

QUI ATTAQUE, ET POURQUOI ?

Vous devez certainement vous demander : qui sont les personnes menant des cyberattaques ? On vous en parle juste ici et on déconstruit le stéréotype autour du hacker.

1 Des groupes organisés comme des entreprises

Oubliez l'image du hacker isolé. Les groupes qui mènent les attaques les plus importantes en 2025 fonctionnent comme des entreprises, avec des spécialisations, des partenariats et des modèles économiques élaborés.

Le groupe DragonForce s'est officiellement structuré comme tel, permettant à plusieurs organisations criminelles d'opérer sous leur propre nom en s'appuyant sur une infrastructure mutualisée : plus résilients face aux démantèlements, moins dépendants d'un seul vecteur d'attaque.

2 La géopolitique s'invite dans la cyber

L'une des évolutions les plus marquantes de 2025 : les États utilisent désormais le cyberespace comme un terrain d'affrontement à part entière. Le conflit russo-ukrainien a généré un flux continu d'attaques

contre des infrastructures énergétiques, des médias et des institutions financières en Europe. Des groupes de hacktivistes, des militants qui utilisent le piratage comme forme d'action politique, liés à la Russie ont ciblé des organisations européennes soutenant l'Ukraine, dont des structures françaises, espagnoles, italiennes et britanniques.

3 Comment les attaquants entrent-ils ? Les portes d'entrée les plus courantes

Les équipes d'Advens sont intervenues sur plus d'une vingtaine d'incidents majeurs en 2025. Dans 80 % des cas, l'accès initial avait été obtenu grâce à des identifiants volés (nom d'utilisateur et mot de passe compromis), parfois depuis des années.

À RETENIR | L'ÉTAT DE LA MENACE CYBER 2025

L'HAMEÇONNAGE RESTE LA MÉTHODE D'ENTRÉE LA PLUS FRÉQUENTE.
Un e-mail, un SMS, un appel vidéo imitant une personne ou un organisme et la victime clique sur un lien, ouvre une pièce jointe ou communique ses codes d'accès.

LES MOTS DE PASSE RÉUTILISÉS SONT UNE FAILLE SYSTÉMIQUE.
Si vous utilisez le même mot de passe sur plusieurs services, et que l'un d'eux est compromis, tous vos comptes utilisant ce mot de passe sont exposés.

LES LOGICIELS NON MIS À JOUR LAISSENT DES PORTES OUVERTES CONNUES DES ATTAQUANTS.
En 2025, plus de 48 000 vulnérabilités informatiques ont été officiellement répertoriées – soit une moyenne de 130 nouvelles failles par jour.

LES ACCÈS PRESTATAIRES MAL ENCADRÉS CRÉENT DES RISQUES INVISIBLES.
Si un fournisseur informatique dispose d'un accès permanent et non surveillé à vos systèmes et qu'il est lui-même compromis, vous l'êtes aussi.

Dès lors, une personne ou une organisation avec un système informatique peu sécurisé peut être une porte d'entrée vers des partenaires plus importants, ou simplement une cible rentable pour un *ransomware* réclamant quelques centaines d'euros.

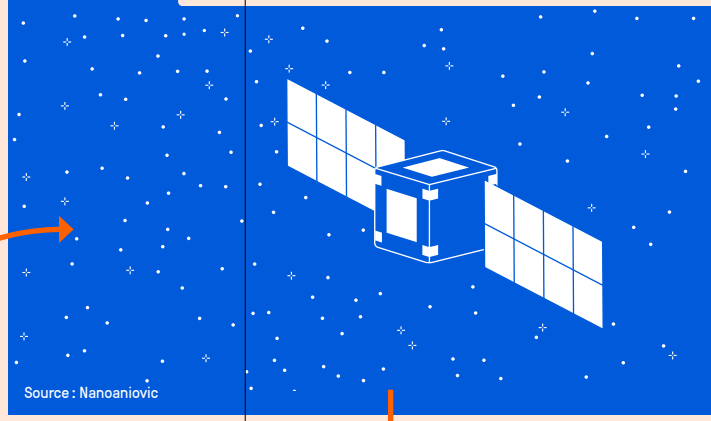
Les infrastructures numériques

Comprendre les réseaux des télécommunications

ORDINATEUR, TÉLÉPHONE

FIBRE OPTIQUE, BOX WIFI, BORNE 5G

DANS L'ESPACE



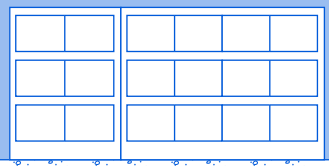
Source : Nanoaniovic

L'EXPLOSION DES SATELLITES AMÉRICAINS

12 952 satellites tournaient en orbite autour de la terre en 2025

9 000	USA
1500	Russie
800	Chine
700	Royaume-Uni
200	Japon
100	France

SUR TERRE



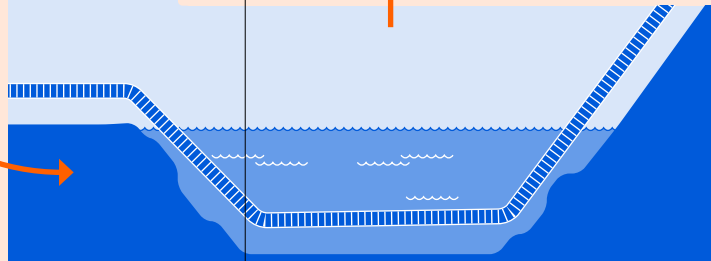
Source : Cloudscene, 2025

NOS DONNÉES DANS LES DATA-CENTERS

Nombre de data-centers par pays

5 427	USA
529	Allemagne
523	Chine
499	Royaume-Uni
337	Japon
322	France

SOUS L'EAU



LA VIE SECRÈTE DES CABLES SOUS-MARINS

99% du trafic Internet international transite par des câbles

Plus de 500 systèmes de cables actifs dans le monde

1,7 million de kilomètres de longueur totale

Source : Agence des Nations Unies pour les technologies numériques

↑ SOMMAIRE

À retenir
Se repérer dans l'univers cyber

En chiffres

6 MILLIARDS
d'internautes dans le monde en 2025, c'est-à-dire 74 % de la population mondiale et 94 % de la population française

15 %
du PIB mondial d'après la Banque mondiale provient de l'économie numérique

46 %
des cyberattaques exploitent des erreurs humaines

750
incidents déclarés en 2024 dans les seuls établissements de santé français

67 %
des entreprises françaises victimes d'au moins une cyberattaque en 2024

En France, sur l'année 2023, les piratages de comptes ont augmenté de 26 %, les hameçonnages de 21 %, les rançongiciels de 17 % et les virements frauduleux de 63 % selon le site de cybermalveillance.gouv.fr.

1
Le cyberespace est aujourd'hui le socle infrastructurel de notre vie privée et professionnelle et connaît une augmentation de la criminalité.

2
Les cyberattaques peuvent tous nous toucher. Du point de vue de l'attaquant, l'objectif n'est pas toujours de frapper fort mais facilement afin d'accéder rapidement aux données personnelles, aux coordonnées bancaires et aux fichiers internes.

3
Les principaux types de cyberattaques sont : le phishing, le rançongiciel (ransomware), la vente de données personnelles, l'usurpation d'identité et la diffamation et le sabotage.

4
La menace informationnelle fait partie du cyberespace. Elle repose sur des causes structurelles économiques menant à l'érosion de la confiance des citoyens envers les médias traditionnels. Des acteurs malveillants s'appuient sur ces fragilités afin de manipuler l'information notamment via l'usurpation et mettre à mal la confiance des citoyens envers les institutions.

LES 10 BONNES PRATIQUES

2

Ce module permet de connaître les bonnes pratiques et des méthodes simples et accessibles pour renforcer la sécurité de votre structure, protéger vos données et réagir efficacement en cas d'incident. Vous découvrirez comment éviter les pratiques à risque dans votre quotidien et adopter les bons réflexes pour réduire votre exposition.

2.1 Choisir des mots de passe solides

Un mot de passe, c'est souvent la première barrière entre un pirate et vos données. Mais beaucoup d'erreurs persistent : l'écrire sur un post-it, le sauvegarder dans le navigateur, ou encore utiliser partout le même. Alors, comment choisir un bon mot de passe ?

1 Utilisez au moins 12 caractères

Pourquoi ? En raison des « attaques par force brute. » Cette technique permet au hacker d'essayer toutes les combinaisons possibles des caractères. Chaque symbole ajouté, qu'il s'agisse d'une lettre, d'une ponctuation ou d'un chiffre, multiplie le temps nécessaire pour percer la défense. D'où l'importance d'un mot de passe long.

2 Utilisez des majuscules, minuscules, chiffres et caractères spéciaux

L'usage de symboles complique le hacking. C'est le cas pour l'« attaque par dictionnaire » il teste automatiquement des millions de combinaisons à partir de mots existants dans la langue française. Si votre mot de passe contient un mot commun ou un prénom, il sera trouvé en un instant.

3 Évitez les informations personnelles et professionnelles évidentes

Par « information évidente », on entend : noms de l'entreprise, dates de naissance, informations accessibles en ligne… Dans la méthode de devination basée sur vos infos personnelles ou le bourrage d'identifiants – réutiliser un de vos mots de passe volés – celles-ci facilitent son travail.

4 Évitez les informations personnelles et professionnelles évidentes

Par « information évidente », on entend : noms de l'entreprise, dates de naissance, informations accessibles en ligne… Dans la méthode de devination basée sur vos infos personnelles ou le bourrage d'identifiants – réutiliser un de vos mots de passe volés – celles-ci facilitent son travail.

5 Utilisez une phrase entière comme mot de passe

Une phrase est un compromis entre la mémorisation du secret et sa robustesse. Par exemple, « Les3coucousqui_mangent » est considéré comme un mot de passe faible mais relativement facile à retenir, là où « 3nIo_BNaJj4H_7iKlaE!6t » est considéré comme très fort mais difficile à mémoriser.

6 Utilisez des mots de passe distincts pour vos comptes personnels et professionnels

Pourquoi, vous demandez-vous certainement ? Mettez-vous à la place d'un cybercriminel. En passant par votre espace personnel il peut s'infiltrer d'autant plus facilement dans votre espace professionnel.

À RETENIR | Un mot de passe doit comporter au moins douze caractères, mêlant majuscules, minuscules, chiffres et symboles, sans lien évident avec votre vie personnelle ou professionnelle. Vous pouvez tester la qualité de votre mot de passe sur bitwarden.com/password-strength.

2.2 Gérer les accès

Laisser l'accès à un drive ou à un outil partagé à des membres qui ont quitté votre organisation, c'est comme laisser la clé sous le paillasson. À terme, cela expose vos données à des suppressions accidentelles ou à des fuites. Pour éviter cela, appliquez plusieurs gestes préventifs.

1 Supprimez systématiquement les comptes des personnes qui partent

Pour ce faire, pensez de temps à autre à effectuer une revue complète des accès : qui a encore les clés, et qui ne devrait plus les avoir ? De cette façon, vous limitez le risque qu'un hacker rentre dans votre système via une attaque de *phishing* d'une personne ayant quitté votre organisation.

2 N'invitez pas des personnes extérieures sur votre drive

S'il ne s'agit que d'un échange ponctuel, privilégiez plutôt l'envoi direct du document par mail.
Si travailler de manière collaborative est indispensable, il est préférable de ne partager que l'accès au document de travail et pas l'ensemble du drive.

3 Ne partagez jamais vos identifiants et mots de passe

Même s'il s'agit d'identifiants professionnels et que vous les transmettez à l'un de vos collègues, vous vous exposez à un risque. Si vous n'avez pas le choix, pensez à changer le mot de passe dès que possible.

À RETENIR | Ne laissez pas l'accès à votre drive à des personnes extérieures à votre organisation. Faites attention au nombre de personnes ayant fait partie de votre organisation qui ont toujours accès à votre drive. Considérez chaque partage comme une porte ouverte. Demandez-vous toujours : « Est-ce indispensable ? Est-ce que cette personne a besoin des clés pour entrer et accéder aux informations de votre entreprise ? »

2.3 Utiliser un gestionnaire de mot de passe

Un gestionnaire de mots de passe fonctionne comme un coffre-fort numérique : tous vos identifiants y sont enregistrés dans une base de données chiffrée, c'est-à-dire illisible sans une clé. Cette clé devient votre mot de passe maître, le seul que vous devez retenir.

1 Comment ça marche ?

Dès que vous entrez le mot de passe, le gestionnaire déverrouille votre coffre et remplit automatiquement vos identifiants sur les sites ou applications que vous utilisez. Cela permet d'avoir des mots de passe longs, uniques et complexes pour chaque compte, sans jamais les mémoriser.

2 Les gestionnaires de mot de passe en ligne

Les outils comme Proton, Bitwarden, Dashlane ou 1Password stockent vos données chiffrées dans un cloud sécurisé. Ils permettent d'y accéder depuis plusieurs appareils (ordinateur, smartphone, tablette) et de synchroniser vos mots de passe en temps réel.
Le chiffrement s'effectue localement, avant l'envoi.

3 Les gestionnaires de mot de passe hors ligne

À l'inverse, un outil comme KeePassXC fonctionne hors ligne. La base de mots de passe est conservée uniquement sur votre machine, dans un fichier chiffré que vous gérez vous-même. C'est une option appréciée par ceux qui veulent garder un contrôle total et ne pas confier leurs données à un service en ligne, mais cela demande plus de vigilance pour les sauvegardes.

4 Luttez contre l'oubli et restez vigilant

Dans tous les cas, ces gestionnaires réduisent considérablement le risque d'oubli, de réutilisation de mots de passe ou d'erreurs humaines.
En bref, ils apportent à la cybersécurité un peu de simplicité sans compromis sur la protection.

À RETENIR | Adoptez un gestionnaire de mot de passe.

2.4 Activer l'authentification multifacteur (le MFA)

Imaginez maintenant qu'un pirate parvienne à trouver votre mot de passe. Sans la double authentification, il aurait accès à tout. Avec elle, il se heurte à une seconde barrière. L'authentification multifacteur ou MFA est une clé temporaire, générée à chaque connexion, souvent sous forme de code envoyé par SMS ou via une application dédiée, qui vient compléter le mot de passe. Même si vos identifiants sont compromis, l'attaquant resterait bloqué. C'est une mesure simple à mettre en place et pourtant, très efficace.

À RETENIR | Activez l'authentification à deux facteurs dans vos applications dès qu'elle est disponible. Si besoin, installez l'application dédiée requise par le site que vous utilisez.

2.5 Penser à la sécurité physique

La cybersécurité ne se limite pas aux attaques en ligne : elle commence aussi dans le monde réel. Un ordinateur volé ou simplement laissé sans surveillance peut livrer, en quelques secondes, un trésor d'informations personnelles ou professionnelles. Veillez donc à verrouiller votre écran dès que vous quittez votre poste, même pour aller prendre un café.

De manière générale, ne laissez pas votre ordinateur ou votre smartphone sans surveillance.

1 Utilisez un filtre de confidentialité pour votre écran lors de vos déplacements

Dans les lieux publics tels que les transports (métros, trains etc), les cafés ou encore les espaces de coworking, pensez à disposer un filtre de confidentialité sur votre écran. Il s'agit d'un film qui réduit l'angle de vision : seules les personnes en face de l'appareil peuvent lire l'affichage. Votre voisin de siège ne verra ainsi qu'un écran noir, garantissant la confidentialité du document que vous consultez. Les filtres de confidentialité existent désormais pour tout type d'appareils, ordinateurs, tablettes, smartphones...

2 À l'étranger : attention à votre hygiène numérique !

Avant tout déplacement à l'étranger, sauvegardez vos données, puis nettoyez vos appareils. Moins ils contiennent d'informations sensibles, moins les risques sont grands en cas de perte ou de vol. Et pour les échanges confidentiels, ayez le réflexe de vous isoler. Évitez les accès aux réseaux wifi que vous ne connaissez pas et utilisez plutôt un partage de connexion avec votre téléphone portable.

À RETENIR | Ne laissez pas vos appareils numériques ouverts sans surveillance et évitez les réseaux wifi publics.

2.6 Effectuer les mises à jour

Encore une fois, c'est une petite musique que l'on croit connaître, mais que beaucoup préfèrent encore ignorer. Lorsqu'on vous rappelle de faire vos mises à jour, ce n'est pas pour vous imposer un nouveau design ou une fonctionnalité gadget. Dans la grande majorité des cas, ces mises à jour servent surtout à corriger des failles de sécurité fraîchement découvertes. Et il faut le savoir : les hackers, eux, scrutent attentivement ces correctifs dès leur publication pour exploiter les appareils qui ne sont pas encore à jour. Chaque jour gagné pour eux, c'est une porte ouverte pour attaquer.

1 Ne téléchargez jamais vos mises à jour ailleurs que sur les sites officiels

Assurez-vous de toujours vous rendre sur le site officiel du logiciel avant de télécharger une mise à jour, activez l'installation automatique quand c'est possible, et si votre appareil est trop vieux pour en bénéficier, il est temps d'envisager un remplacement.

2 Mieux vaut investir un peu que risquer de tout perdre

Oubliez les systèmes d'exploitation ou logiciels « craqués. » Ils peuvent sembler économiques sur le moment, mais ils bloquent l'accès à ces correctifs vitaux et laissent votre appareil exposé à la moindre faille connue.

À RETENIR | Réalisez les mises à jour nécessaires en temps et en heure ou activez l'installation automatique.

2.7 Sauvegarder les données

Une panne, un vol, un incendie ou une attaque par ransomware peut tout effacer. Sans sauvegarde, il ne reste plus qu'à constater les dégâts.

1 Identifiez ce qui compte le plus

Identifiez les dossiers les plus importants : comptabilité, fichiers d'adhérents, documents administratifs, données sensibles. Sauvegardez-les régulièrement, sur un disque externe ou dans un service cloud différent.

2 Disposez d'une copie hors ligne

Idéalement, gardez aussi une copie « hors ligne » et chiffrée de vos données, même si vous les sauvegardez régulièrement. En cas de blocage, vous pourrez tout restaurer simplement en quelques clics.

À RETENIR | Faites régulièrement une sauvegarde hors ligne de vos données.

2.8 Chiffrer les données

Le chiffrement signifie transformer vos fichiers en code illisible sans mot de passe. Utile si un ordinateur ou une clé USB est perdue ou volée. Des logiciels comme VeraCrypt permettent de créer un « coffre-fort » numérique : un simple dossier qui renferme vos documents, accessible uniquement avec votre mot de passe. Pour transmettre ce mot de passe, faites-le toujours par un autre canal, de préférence de vive voix.

1 Utilisez WhatsApp mais en conscience

En ce qui concerne les messageries, WhatsApp utilise le chiffrement. Néanmoins, il conserve des métadonnées telles que l'identité de vos correspondants, la fréquence et les horaires de vos échanges, le type d'appareil ou votre adresse IP. Pour limiter ces risques, activez l'option de « sauvegarde chiffrée de bout en bout ».

2 Transitez vers Signal

Contrairement à WhatsApp qui utilise le chiffrement mais collecte vos métadonnées, Signal minimise les informations qu'il détient sur vous. L'application ne connaît pas vos contacts ni avec qui vous communiquez. Elle ne conserve que votre numéro de téléphone et la date de dernière connexion.

À RETENIR | Adoptez des logiciels et outils de messagerie employant le chiffrement de bout à bout en conscience.

2.9 Séparer la vie pro et perso

Le mélange de genres est une porte ouverte aux fuites. Utiliser votre adresse personnelle pour des activités de l'association, ou inversement, c'est risquer une confusion dangereuse.

1 Gardez vos comptes distincts

Idéalement, n'utilisez pas vos identifiants personnels dans le cadre d'un usage professionnel. Des équipements distincts évite que le hacker s'appuie sur votre compte personnel pour s'immiscer dans le professionnel. En cas de doute sur une fuite, le site haveibeenpwned.com permet de vérifier si votre adresse mail ou votre numéro ont été compromis.

À RETENIR | Séparez vos comptes professionnels et personnels.

2.10 Se protéger du *phishing*

Le phishing, ou hameçonnage, c'est l'art de la tromperie à l'ère numérique. Un mail qui paraît sérieux, un logo bien imité, un lien apparemment légitime… et le piège se referme. Certains messages sont grossiers et faciles à repérer, d'autres, bien plus ciblés (on parle alors de spear-phishing), s'appuient sur vos habitudes ou votre entourage.

1 Restez vigilant face à une menace augmentée par l'IA

Avec l'IA, ces attaques sont plus sophistiquées. Les *deepfakes* peuvent reproduire des voix et des visages à s'y méprendre et les chatbots malveillants arrivent à simuler une conversation crédible. Certains cybercriminels mènent des appels ou visio piégés pour soutirer des informations sensibles.

2 Vérifiez l'adresse mail de l'expéditeur

Le premier réflexe consiste évidemment à vérifier attentivement l'adresse mail de l'expéditeur. Certains usurpateurs tenteront de tromper votre vigilance en utilisant des adresses très proches de celles d'expéditeurs légitimes (*typosquatting*).

3 Méfiez-vous des demandes urgentes

La notion d'urgence est une caractéristique des tentatives de *phishing*, n'entamez aucune procédure dans la précipitation. Ne cliquez jamais sur un lien douteux : recherchez plutôt le site officiel via un moteur de recherche.

4 Vérifiez l'adresse réelle d'un lien et soyez attentifs aux fautes

Si vous devez cliquer, survolez le lien avec votre souris : l'adresse réelle s'affiche en bas à gauche du navigateur. Si elle correspond bien à ce qu'elle prétend être, vous pouvez cliquer. Si ce n'est pas le cas, abstenez-vous. Soyez attentif aux fautes, aux tournures maladroites, et en cas de doute, contactez directement l'expéditeur officiel.

5 Signalez les campagnes de phishing

Si vous repérez une campagne de *phishing*, signalez-la sans y répondre : même un message moqueur permet de mettre à jour les bases de données des cybercriminels.

Vous pouvez les signaler via la plateforme française signal-spam.fr .

À RETENIR | Avant de cliquer sur un lien, vérifiez attentivement l'adresse de l'expéditeur et l'URL.

Je suis victime d'une cyberattaque : que faire ?

1 Je garde mon calme

Ne cédez surtout pas à la pression qui monte et au sentiment d'urgence ! C'est justement ce que cherche à provoquer les cyberattaquants. Pas de clic fébrile et précipité sur un lien étrange, un message d'alerte, ou encore une demande de rançon en échange de vos données personnelles : restez calme, la panique ne fera qu'empirer les choses.

2 J'identifie la nature de l'attaque

Après avoir soufflé un bon coup, prenez du recul : de quoi êtes-vous victime ? Pour le savoir on suit les 3C :

- **Comment ?** Quel est le type de cyberattaque ? Est-ce un rançongiciel, un hameçonnage, un piratage de messagerie ? Pour identifier l'attaque dont vous avez été victime, vous pouvez remplir un formulaire en ligne : cybermalveillance.gouv.fr/diagnostic
- **Combien ?** Êtes-vous le seul à avoir été touché par l'attaque ou vos collègues également ? Quelle proportion de votre organisation a été touchée ?
- **C'est grave ?** Quel est le niveau de risque associé à l'utilisation de ces données ? Quel est le niveau de dégâts que peut causer cette faille dans la cybersécurité ?

Même si la situation semble urgente, prenez quelques minutes pour vous poser ces questions et y répondre, afin d'adopter les gestes adaptés et contacter les personnes adéquates.

3 Je réalise les gestes de premier secours numériques appropriés

Maintenant que vous comprenez mieux la situation à laquelle vous êtes confronté, adoptez les bons gestes. Quand vous êtes secouriste, vous ne faites pas un massage cardiaque à quelqu'un qui respire normalement. La cybersécurité c'est presque pareil ! Il faut faire les bons gestes et garder son calme. C'est pour ça que les 2 premières étapes sont essentielles. Alors concrètement, que faire en cas de problème ?

4 Je demande de l'aide

N'hésitez pas à contacter le service 17Cyber du gouvernement ! Ce service public d'assistance en ligne gratuit vous aidera à déterminer la situation exacte et à trouver des solutions pour y faire face.

En fonction de votre statut ainsi que du type et de l'étendue de l'attaque, ces services pourront vous renseigner de façon appropriée : cybermalveillance.gouv.fr/menaces/recommandations
Si l'aide publique ne suffit pas, vous pouvez aussi faire appel à un prestataire privé en remplissant ce formulaire en ligne : cybermalveillance.gouv.fr.

5 Je signale l'attaque aux personnes concernées

Ensuite, vous devez rapidement déposer une déclaration initiale à la CNIL (Commission Nationale de l'Informatique et des Libertés) si les cybercriminels ont pu accéder à vos données personnelles. Le délai imparti est de 72h maximum, sous peine de sanction, conformément à l'article 33 du RGPD.

Vous pouvez le faire via ce lien : cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles

Ensuite, sans susciter de panique, vous pouvez prévenir les personnes concernées par l'attaque si le risque est élevé. Ne restez pas seul : parlez-en autour de vous, sans honte, et contactez sans attendre les CSIRT régionaux (les centres de réponse aux incidents cyber sur les territoires) présents sur les territoires et chargés d'accompagner les victimes et d'analyser les incidents.

Pour plus d'informations : cert.ssi.gouv.fr/csirt/csirt-territoriaux cybermalveillance.gouv.fr

Déclarez le sinistre auprès de votre assureur qui peut vous dédommager, voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.

Enfin, à des fins d'utilité publique, si vous repérez une campagne de *phishing*, signalez-la sans y répondre : même un message moqueur permet de mettre à jour les bases de données des cybercriminels. Vous pouvez la signaler ici : signal-spam.fr.

6 Je porte plainte

Vous souhaitez déposer plainte à la suite d'une cybermalveillance ? Rendez-vous au commissariat de police ou à la brigade de gendarmerie dont vous dépendez, ou adressez votre plainte par écrit au procureur de la République du tribunal judiciaire de votre domicile.

Si vous êtes un particulier victime d'une cybermalveillance à caractère financier (chantage, sextorsion, escroquerie commerciale ou sentimentale, piratage de messagerie ou réseaux sociaux…), vous pouvez déposer plainte en ligne sur la plateforme THESEE du ministère de l'Intérieur.

Si vous êtes un particulier, vous pouvez être accompagné gratuitement dans votre dépôt de plainte par l'association France Victimes qui opère le numéro d'aide aux victimes du ministère de la Justice : 116 006 (appel et service gratuits, ouvert 7 jours sur 7 de 9h à 19h).

↑ SOMMAIRE

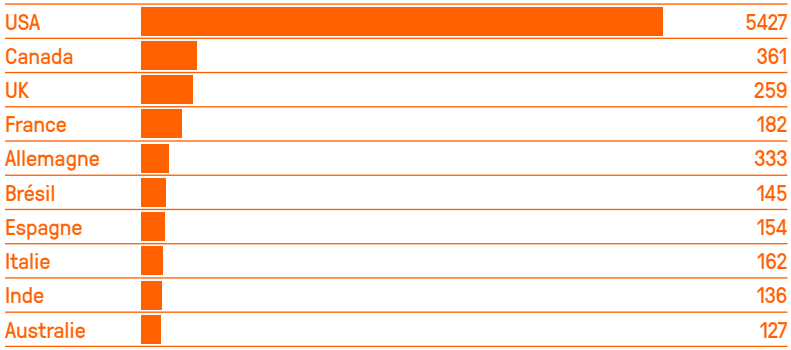
Les rançongiciels : qui sont les victimes ?

Le rançongiciel (ou ransomware) est un logiciel malveillant qui chiffre les fichiers ciblés et peut paralyser partiellement ou totalement l'activité de votre structure : documents internes, bases de données, informations stratégiques deviennent soudainement inaccessibles.

7 CYBERATTAQUES SUR 10
dans le monde sont des rançongiciels

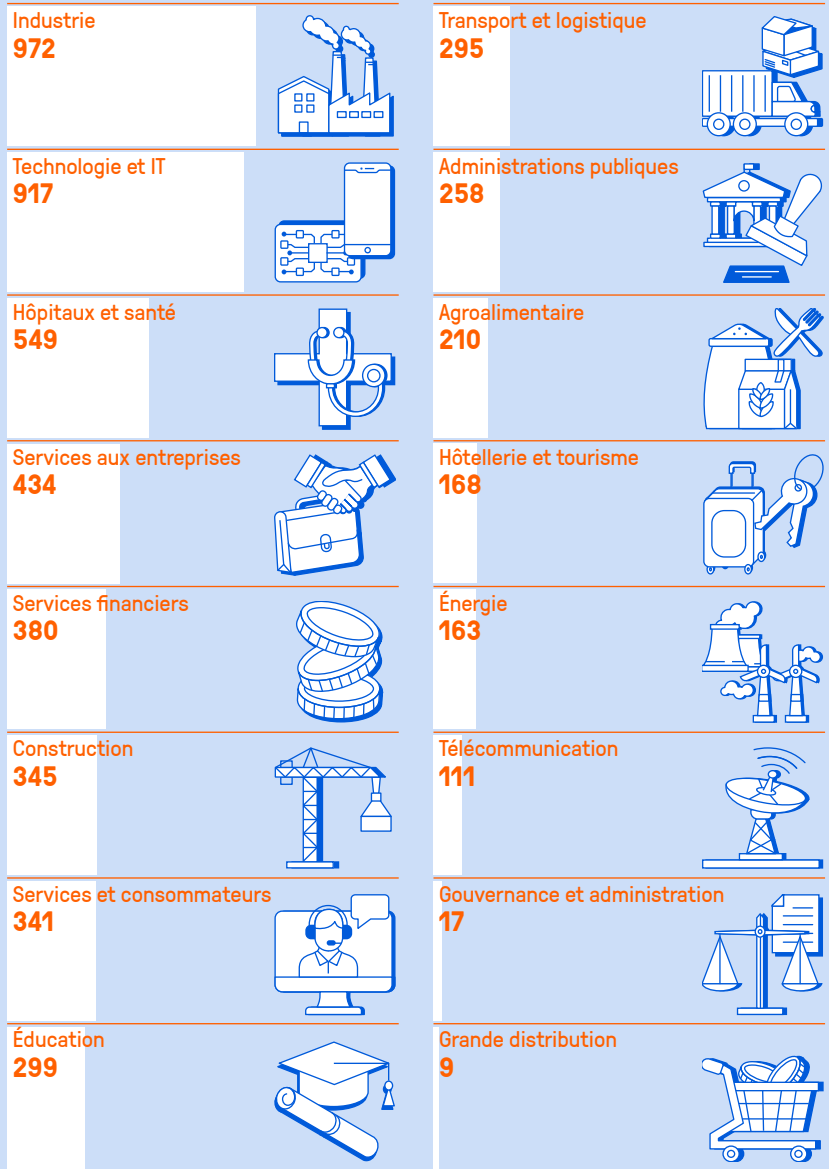
PLUS DE 317 MILLIONS
de tentatives enregistrées à travers le monde

PAYS CIBLÉS
(NOMBRE DE VICTIMES)



Source : Statista, 2023.

SECTEURS D'ACTIVITÉS CIBLÉS DANS LE MONDE EN 2025
(NOMBRE DE VICTIMES)



Source : Rapport état de la menace d'Advens (2026) p.21

LES 10 BONNES PRATIQUES
↑ SOMMAIRE

À retenir
Les 10 réflexes clés pour une bonne hygiène numérique !

Je suis victime d'une cyberattaque, les 6 étapes à suivre :

- Je garde mon calme.
- Je réalise les gestes de premier secours numériques appropriés.
- Je signale l'attaque aux acteurs concernés.
- J'identifie la nature de l'attaque.
- Je demande de l'aide à 17Cyber ou à un prestataire privé.
- Je porte plainte.

1
Je ne laisse pas l'accès à mon drive aux personnes ayant quitté mon organisation.

2
Un mot de passe doit comporter au moins douze caractères, mêlant majuscules, minuscules, chiffres et symboles, sans lien évident avec votre vie personnelle.

3
J'utilise un gestionnaire de mots de passe.

4
J'utilise une authentification multifacteur.

5
Je ne laisse pas mes appareils numériques ouverts sans surveillance.

6
Je réalise les mises à jour dès qu'elles sont disponibles.

7
Je fais régulièrement une sauvegarde hors ligne de mes données.

8
Je privilégie les outils chiffrés.

9
Je sépare ma vie professionnelle de ma vie personnelle.

10
Avant de cliquer sur un lien, je vérifie attentivement l'adresse de l'expéditeur et l'URL.

↑ SOMMAIRE

L'INTELLIGENCE ARTIFICIELLE ALLIÉE OU DANGER ?

3

En suivant ce parcours, vous découvrirez comment fonctionne l'IA générative, quels sont ses principaux enjeux et comment l'utiliser de manière sécurisée et éthique. L'objectif n'est pas seulement d'apprendre à exploiter ces outils, mais aussi de développer un esprit critique pour anticiper leurs impacts sur la société et sur vos vies.

Ce chapitre a pour objectif de vous aider à comprendre les fondamentaux de l'IA générative, ses opportunités et ses risques, afin d'adopter des pratiques sûres et responsables. Cependant, il est important de garder à l'esprit que l'IA évolue extrêmement vite : les repères d'aujourd'hui seront peut-être dépassés demain.

3.1 L'IA, la définir pour l'anticiper

Le 30 novembre 2022, OpenAI met en ligne ChatGPT, un agent conversationnel d'IA générative capable de répondre à des questions et de générer du texte en retour. En quelques jours, il dépasse le million d'inscrits dans le monde. Un an plus tard, ChatGPT avait déjà été utilisé par 40 % de la population française. L'intelligence artificielle fait désormais partie de notre quotidien au travail et en famille, dans nos écoles et nos associations. Mais comment cela fonctionne ? Et comment anticiper les risques de cet outil ?

QU'EST-CE QUE L'IA ?

Selon la Commission Nationale de l'informatique et des libertés (CNIL), l'intelligence artificielle est un « procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies ». L'intelligence artificielle désigne des systèmes automatisés fondés sur des algorithmes capables de traiter des données afin d'assister, d'orienter ou d'automatiser certaines décisions ou actions. Selon les définitions institutionnelles, ces systèmes peuvent produire des recommandations, des contenus ou des décisions et influencer directement la vie personnelle ou professionnelle des personnes. Pour cette raison, l'usage de l'IA engage une responsabilité particulière : garantir que ces outils servent l'intérêt général, respectent la dignité humaine, protègent les données des publics accompagnés et renforcent sans fragiliser la mission sociale, solidaire et démocratique des organisations.

Concrètement, l'IA donne l'impression de « penser », dans le sens où elle ne se contente pas d'exécuter des ordres simples mais de planifier et résoudre des problèmes ou des tâches en faisant parfois preuve de « créativité » ou devrons-nous plutôt dire de « flexibilité » car l'IA ne repose que sur des règles logiques et fonctionne uniquement grâce aux programmes informatiques sur lesquels elle est basée. Il faut alors éplucher l'IA, tel un oignon, pour comprendre les différents mécanismes qui la composent. Débutons par la première couche : le machine learning.

QU'EST-CE QUE LE MACHINE LEARNING ?

Le machine learning, ou apprentissage automatique en français, constitue la première strate technologique de l'intelligence artificielle. Concrètement, il s'agit d'une méthode qui permet aux machines d'apprendre par elles-mêmes à partir de données, sans qu'un développeur ait besoin de programmer manuellement chaque règle ou chaque scénario possible.

Pour bien saisir cette nuance, prenons un exemple simple.
Dans la programmation classique, un développeur devrait explicitement écrire : « Si l'e-mail contient le mot « loterie » et provient d'une adresse inconnue, alors c'est un spam ». Avec le machine learning, on montre au système des milliers d'e-mails préalablement identifiés comme spams ou non-spams, et l'algorithme découvre lui-même les patterns récurrents qui caractérisent un message indésirable. Cette capacité d'auto-apprentissage change radicalement la donne.

Le fonctionnement repose sur trois phases distinctes. D'abord, la collecte de données : des centaines, des milliers, parfois des millions d'exemples sont rassemblés. Ensuite vient l'entraînement : l'algorithme passe au crible ces données pour y détecter des motifs, des corrélations, des tendances. Enfin, la prédiction : une fois rodé, le système peut analyser de nouvelles données qu'il n'a jamais vues et prendre des décisions cohérentes.

Au-delà de la détection de spam, cette technologie infiltre désormais notre quotidien bien plus qu'on ne l'imagine. Lorsque Netflix vous suggère une série qui semble taillée sur mesure pour vos goûts, c'est du machine learning à l'œuvre. Des technologies comme Google Maps, Waze ou CityMapper s'appuient également sur cette technologie pour prédire vos temps de trajet. Ces exemples permettent de mieux visualiser ce qu'est le machine learning, qui demeure l'une des couches les plus concrètes de l'intelligence artificielle. Pour établir de telles connexions, cette approche s'appuie sur une architecture particulière : les réseaux de neurones artificiels.

LES RÉSEAUX DE NEURONES ARTIFICIELS, QU'EST-CE QUE C'EST ?

Les réseaux de neurones artificiels s'inspirent du fonctionnement biologique du cerveau humain, bien qu'ils en constituent une version considérablement simplifiée. Concrètement, un réseau de neurones se compose de plusieurs couches de « neurones » interconnectés. Chacun d'eux reçoit des informations, les traite, puis transmet le résultat aux neurones de la couche suivante. Cette organisation en strates permet de décomposer un problème complexe en une succession d'étapes de traitement de plus en plus abstraite. Le principe reste relativement simple à visualiser, il suffit d'imaginer une chaîne de production où chaque ouvrier effectue une tâche précise avant de passer au produit suivant.

Cette architecture se révèle particulièrement efficace pour des tâches que les humains réalisent instinctivement mais qu'il serait quasiment impossible de programmer manuellement. Reconnaître un visage dans une foule, comprendre une phrase ambiguë... Autant de défis qui requièrent de saisir des nuances subtiles plutôt que d'appliquer des règles rigides.

LA RECONNAISSANCE FACIALE

Un exemple concret d'IA dans notre quotidien est la reconnaissance faciale, omniprésente sur nos smartphones, qui repose sur cette technologie. Lorsque vous déverrouillez votre téléphone d'un simple regard, un réseau de neurones compare instantanément les caractéristiques de votre visage, telles que la distance entre les yeux, la forme du nez et le contour des lèvres, à un modèle préalablement enregistré. Le système tolère les variations de luminosité, d'angle, ainsi que de légères modifications de votre apparence, comme le port de lunettes ou une barbe naissante.

Malheureusement, cette puissance a un coût. Les réseaux de neurones nécessitent des quantités massives de données d'entraînement et une puissance de calcul considérable. Là où un algorithme classique peut tourner sur un ordinateur portable, certains réseaux sophistiqués requièrent des fermes de serveurs équipés de processeurs spécialisés pendant des jours, voire des semaines. Mais c'est une problématique que nous aurons l'occasion de développer plus tard dans ce module notamment sur les risques environnementaux liés à son fonctionnement.

LE DEEP LEARNING, QU'EST-CE QUE C'EST ?

Si les réseaux de neurones constituent l'architecture de base, le *deep learning* (ou apprentissage profond en français) pousse cette logique à son paroxysme. Cette technique ne diffère pas fondamentalement des réseaux de neurones classiques, mais elle repose sur des architectures bien plus complexes, comportant des dizaines, voire des centaines de couches de neurones superposées. Voyez donc le *deep learning* comme une sous-catégorie du *machine learning* dotée d'une profondeur qui lui confère des capacités inédites.

Cette approche multicouche permet à la machine d'apprendre automatiquement les bonnes caractéristiques à extraire des données, sans intervention humaine. Dans le *machine learning* classique, un ingénieur doit identifier manuellement les paramètres pertinents comme la forme d'une oreille pour distinguer un chat d'un chien, la fréquence de certains mots pour détecter un spam. Avec le deep learning, le système découvre lui-même ces critères distinctifs. On lui montre des milliers d'images étiquetées « chat » et « chien », et il détermine quels indices visuels sont les plus discriminants.

Pour comprendre vos questions et y répondre de manière cohérente, ces modèles ont ingéré des quantités astronomiques de texte provenant d'Internet, de livres et d'articles scientifiques. Les chatbots conversationnels les plus avancés comme ChatGPT, Claude ou Gemini constituent probablement l'application la plus emblématique du *deep learning*.

3.2 Comprendre l'IA générative

Il existe plusieurs façons de distinguer les différentes catégories d'IA. On peut notamment les classer selon les techniques utilisées (comme nous venons de le faire avec le machine learning et le deep learning), leurs domaines d'application (traitement du langage, vision par ordinateur, etc.), ou encore leurs usages, c'est-à-dire les tâches qu'elles permettent de réaliser. Dans cette dernière classification, une catégorie attire particulièrement l'attention du grand public : l'IA générative, car elle est directement mise entre nos mains et nous permet d'interagir avec elle, de la tester, voire de la manipuler.

QUELS SONT LES DIFFÉRENTS OUTILS DE L'IA GÉNÉRATIVE ?

En quelques années, le monde de l'IA générative a explosé, proposant différents outils sur le marché pour répondre aux besoins des utilisateurs. Voici une liste non exhaustive des principaux des principales solutions disponibles :

GÉNÉRER DU TEXTE	GÉNÉRER DES IMAGES	GÉNÉRER DE L'AUDIO	GÉNÉRER DES VIDÉOS
ChatGPT	Dall-E	Mubert	Sora
Copilot	Midjourney	Suno	Heygen
MistralAI	Ideogram	ElevenLabs	KlingAI
Gemini	Stable Diffusion	Synthesia	Stable Diffusion
Claude	OpenArt	Heygen	OpenArt

Nous parlions, en introduction, du 30 novembre 2022, jour de la sortie de ChatGPT. Ce qui a marqué les premiers utilisateurs, c'est la capacité du grand modèle de langage (LLM) à répondre « comme un humain », poussant même certains utilisateurs à se confier ou à transmettre des informations personnelles à ce nouvel assistant virtuel.

DÉMYSTIFIER L'IA GÉNÉRATIVE

Pour démystifier cette révolution technologique, il semble important de rappeler que le LLM est un type de modèle d'intelligence artificielle entraîné sur d'énormes quantités de texte pour comprendre et générer du langage humain. L'objectif même de l'outil est de mimer le langage humain. Rien de plus. ChatGPT ne vous comprend pas, ne vous apprécie pas, ne vous juge pas. C'est un outil entraîné sur une quantité astronomique de données, qui a appris à prédire le mot le plus probable qui suit une suite de mots. L'outil, qu'il convient de ne pas humaniser, anticipe statistiquement ce qui vient ensuite. Mais voilà, qui dit statistiques et probabilités dit parfois erreur.

Il existe ainsi plusieurs manières de distinguer les différentes catégories d'IA. On peut notamment les classer selon les techniques utilisées (comme nous venons de le faire avec le machine learning et le *deep learning*), leurs domaines d'application (traitement du langage, vision par ordinateur, etc.), ou encore leurs usages, c'est-à-dire les tâches qu'elles permettent de réaliser.

Et maintenant que nous avons une vision plus claire de comment fonctionne l'IA, de ce qu'elle est et ce qu'elle n'est pas, nous tâcherons de décortiquer les risques que présente cette technologie.

3.3 Les risques liés à l'utilisation de l'IA

L'IA est un outil technologique remarquable à bien des égards, et ne pas l'utiliser, la rejeter de but en blanc ou ignorer son existence constituerait une erreur stratégique dans de nombreux domaines, parmi lesquels la cybersécurité. En effet, utiliser l'IA, en connaître les capacités comme les limites, permet de mieux en évaluer les risques. L'IA générative demeure une technologie jeune, aussi bien dans son développement que dans ses usages, et l'objectif de ce module est de l'intégrer avec le plus de sécurité possible, sans non plus tomber dans un enthousiasme aveugle.

LES RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE

1 La fuite ou le vol d'informations

Premier risque majeur et souvent sous-estimé : il ne faut jamais saisir de données confidentielles ou sensibles dans une IA générative dont on ne maîtrise pas les conditions de sécurité. Cette règle, qui peut paraître évidente, est pourtant régulièrement transgressée, parfois par simple méconnaissance des mécanismes sous-jacents.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) insiste particulièrement sur ce point : le danger ne concerne pas seulement les données utilisées pour entraîner le modèle en amont, mais également toutes celles qui sont saisies lors de son utilisation quotidienne. Par exemple, si un utilisateur copie-collé un extrait de document confidentiel dans une IA générative pour le reformuler ou le résumer, il perd immédiatement le contrôle sur la diffusion de cette information.

IA ET DONNÉES SENSIBLES : UNE FRONTIÈRE DÉJÀ FRANCHIE

Un cas d'école illustre parfaitement ce risque. En 2023, des ingénieurs de Samsung ont déposé des extraits de brevets confidentiels de l'entreprise dans ChatGPT pour travailler dessus. L'IA s'est alors entraînée avec ces nouvelles informations.

Résultat : en interrogeant l'outil sur des éléments précis concernant Samsung et ses produits, la solution répondait en s'appuyant sur le contenu des brevets, révélant ainsi des informations stratégiques qui auraient dû rester secrètes. Cet incident a conduit Samsung à interdire l'usage de ChatGPT en interne et à sensibiliser massivement ses employés aux risques de fuites de données.

2 L'empoisonnement du modèle d'IA

L'empoisonnement consiste à injecter volontairement des données malveillantes ou biaisées dans le processus d'apprentissage d'un modèle d'IA, ou lors de ses mises à jour ultérieures. L'objectif est de modifier subtilement son comportement pour qu'il produise des réponses incorrectes, dangereuses ou manipulées, sans que cela soit immédiatement détectable.

Cet empoisonnement peut se traduire par plusieurs scénarios préoccupants :

- Des réponses qui favorisent systématiquement une idéologie particulière, une marque commerciale ou un point de vue politique,
- La génération de contenus trompeurs, offensifs ou discriminatoires dissimulés sous une apparence neutre,
- L'insertion d'instructions dangereuses ou malveillantes dans des prompts apparemment anodins,
- La modification progressive des recommandations pour orienter les décisions des utilisateurs.

L'empoisonnement de l'IA est un type d'attaque particulièrement difficile à détecter car elle ne produit pas nécessairement d'erreurs visibles immédiatement. Le modèle continue de fonctionner normalement, mais son comportement est subtilement altéré.

C'est pourquoi il demeure toujours essentiel de vérifier systématiquement le contenu produit par l'IA et d'éviter autant que possible les systèmes entièrement automatisés dans les

processus critiques. La vérification humaine reste le meilleur des remparts. Il est recommandé de ne pas partager des données confidentielles ou sensibles dans une IA générative dont on ne maîtrise pas les conditions de sécurité. Cette règle, qui peut paraître évidente, est pourtant régulièrement transgressée, parfois par simple méconnaissance des mécanismes sous-jacents.

LES RISQUES LIÉS À L'ÉTHIQUE

Les biais constituent l'un des enjeux éthiques les plus préoccupants de l'IA générative. Ils apparaissent lorsque les données utilisées pour entraîner une IA ne sont pas représentatives de la diversité réelle ou contiennent des préjugés, conscients ou non.

Le cas de la génération d'images biaisées

Pour bien comprendre ce qu'est un biais, prenons une expérience simple que vous pouvez reproduire. Demandez à une IA générative d'images : « generate an image of a doctor in a hospital ». Puis, effectuez une deuxième requête en anglais en utilisant le terme neutre « doctor », qui ne spécifie pas le genre. Les images générées sont quasiment identiques. Dans les deux cas, le médecin est un homme blanc, d'âge moyen, portant une blouse blanche dans un environnement hospitalier aseptisé.

Cette observation n'est pas anecdotique. Une étude scientifique publiée en août 2024 a analysé systématiquement les biais démographiques dans les images de médecins générées par des IA. En comparant 1 000 images issues de cinq plateformes différentes avec les données réelles des médecins américains, les chercheurs ont constaté une surreprésentation flagrante des hommes blancs et une sous-représentation significative des femmes, des personnes asiatiques et d'Amérique latine. Ces biais, présents dans toutes les plateformes posent un risque majeur de renforcement des stéréotypes et de dévalorisation des efforts de diversité dans le secteur de la santé.

LES ENJEUX ENVIRONNEMENTAUX

1 Une consommation électrique croissante

Au-delà des questions de sécurité et d'éthique, l'IA générative soulève également des préoccupations environnementales majeures, souvent invisibles pour l'utilisateur final. Selon un avis récent sur la consommation énergétique liée à l'utilisation du numérique publié par l'Agence de l'environnement et de la maîtrise de l'énergie (ADEME), l'empreinte carbone du numérique en France représente déjà 4,4 % de l'empreinte nationale totale, soit 29,5 millions de tonnes d'équivalent CO_2, et 11 % de la consommation électrique du pays.

L'essor de l'intelligence artificielle s'accompagne d'un coût énergétique colossal. En 2024, les centres de données (data centers) dédiés à l'IA ont consommé environ 415 térawattheures (TWH) d'électricité, soit 1,5 % de la demande mondiale.

Selon l'Agence internationale de l'énergie, en raison de l'expansion des data centers, la consommation électrique des serveurs optimisés pour l'IA sera multipliée par cinq d'ici 2030. Cette croissance, estimée à +15 % par an, est quatre fois plus rapide que celle des autres secteurs économiques, ce qui pose un défi majeur pour la sécurité énergétique mondiale et la transition vers une économie bas carbone.

IRLANDE : LE PRIX FORT DU CLOUD

Le cas de l'Irlande met en lumière les tensions croissantes entre transition numérique et justice environnementale, des enjeux centraux pour l'économie sociale et solidaire. En 2023, les data centers absorbaient déjà près d'un cinquième de la consommation nationale d'électricité, tandis que le pays en comptait près de 90 en 2025. Cette concentration d'infrastructures énergivores bénéficie largement aux grandes entreprises technologiques, mais ses coûts : pression sur le réseau, émissions, concurrence sur l'accès à l'énergie, sont supportés localement par les territoires et les populations. Pour l'ESS, ce modèle interroge la soutenabilité sociale et écologique du numérique : il appelle à repenser les usages, la sobriété numérique et une gouvernance plus équitable des infrastructures, au service de l'intérêt général.

↑ SOMMAIRE

2 Quel est le coût écologique réel de l'IA ?

Si l'enjeu est réel, il convient cependant de noter que les différentes études évoquant les quantités de CO_2 produites lors de l'entraînement de modèles sont estimatives et varient selon la région et le mix énergétique. Aussi, le coût énergétique d'une requête sur ChatGPT varie grandement selon sa complexité. Difficile donc d'établir un comparatif énergétique clair entre une requête sur un LLM et une recherche Google. Dans ce contexte, un enjeu central de conception des modèles est précisément de réduire la consommation énergétique pour un niveau de performance donné.

Cela dit, les grands acteurs du numérique (les GAFAM) constatent déjà une augmentation significative de leurs émissions de gaz à effet de serre directement liée à ces nouveaux usages. Google a annoncé son intention de remettre en service d'ici 2029 une centrale nucléaire fermée depuis cinq ans pour répondre aux besoins immédiats de ses data centers. Google n'est pas le seul : de nombreuses entreprises technologiques cherchent activement à développer des petits réacteurs modulaires (SMR, Small Modular Reactors) pour répondre à cette demande énergétique explosive.

3 Vers une « IA frugale » ?

Face à ce constat, l'ADEME insiste sur la nécessité impérieuse de développer une IA « frugale », c'est-à-dire plus sobre en ressources et en énergie. Elle encourage le développement de petits modèles spécialisés, beaucoup moins gourmands que les grands modèles généralistes, ce qui présente des avantages non seulement environnementaux, mais aussi économiques et de souveraineté.

LES RISQUES HUMAINS

1 Le rôle essentiel du jugement humain

Lorsque l'IA générative est utilisée sans supervision humaine appropriée, il existe un risque majeur de délégation aveugle de tâches ou de décisions à la machine. Cette dépendance progressive peut conduire à des décisions erronées, à la diffusion d'informations inexactes ou trompeuses, voire à des actions dangereuses : validation de transactions financières, génération de contenus publics diffusés largement, administration de systèmes critiques, ou encore aide à la décision médicale.

L'ANSSI insiste particulièrement sur ce point dans ses recommandations : il est impératif d'intégrer systématiquement une validation humaine pour toute action ou décision à impact critique, afin de réduire significativement ce risque. L'humain doit rester le décideur final, l'IA n'étant qu'un outil d'aide à la décision.

2 Les dangers des IA « boîtes noires »

Les modèles d'IA générative, en particulier les grands modèles de langage (LLM), fonctionnent souvent comme des « boîtes noires » opaques, ce qui complique considérablement l'identification des causes profondes d'une erreur, d'un biais ou d'un comportement inattendu. Cette opacité rend également plus complexe l'investigation en cas d'incident de sécurité ou de dérive du système, et peut empêcher la détection rapide de manipulations malveillantes, comme les attaques par injection de prompt ou l'empoisonnement de données évoquées précédemment. Sur le plan humain, il peut entraîner une perte progressive de compétences et d'esprit critique chez les utilisateurs, qui deviennent dépendants de l'IA et moins aptes à détecter ou corriger ses erreurs.

LES RISQUES INFORMATIONNELS

Comme vu précédemment dans ce module, les modèles de langage génératifs produisent des textes fluides et convaincants, mais ils restent fondamentalement probabilistes : ils « devinent » la suite la plus vraisemblable d'une phrase sans vérifier systématiquement la véracité des faits avancés.

1 Les erreurs factuelles

Les erreurs factuelles peuvent prendre de multiples formes : dates inexactes, chiffres approximatifs, références juridiques erronées, citations attribuées à la mauvaise source, ou encore confusion entre deux événements ou deux personnes portant des noms similaires. Là où un moteur de recherche renvoie vers des documents à vérifier, un LLM fournit une réponse rédigée qui donne l'illusion d'un savoir stabilisé. Plus l'interface est fluide, plus le risque de « délégation intellectuelle » augmente : l'utilisateur tend à faire confiance au style plutôt qu'à la substance.

2 Les hallucinations

Les hallucinations représentent un niveau de risque encore supérieur, car le modèle ne se contente pas d'approximer un fait, il en fabrique un de toutes pièces. Il peut ainsi inventer des études scientifiques inexistantes, des arrêts de jurisprudence fictifs, des normes techniques jamais publiées, des citations plausibles mais fictives, en les insérant dans un récit cohérent. En communication ou en éducation, ces contenus inventés risquent d'alimenter la désinformation, en se mêlant à des éléments exacts dans un ensemble difficile à démêler pour un non-spécialiste.

COMMENT DÉTECTER LES HALLUCINATIONS

Développer un « détecteur d'hallucinations » mental est crucial. Voici les signaux d'alarme :

LA PRÉCISION SUSPECTE
L'IA donne des détails très spécifiques (dates exactes, pourcentages précis, citations longues) sur des sujets obscurs.

L'ABSENCE DE NUANCE
Si l'IA présente quelque chose de trop simple, trop tranché, méfiez-vous.

LES ANACHRONISMES
L'IA peut mélanger des éléments de différentes époques. Un maire citant une loi qui n'existait pas encore, par exemple.

LA COHÉRENCE TROP PARFAITE
Dans la vraie vie, il y a des contradictions, des incohérences. Si tout s'emboîte trop parfaitement, c'est peut-être construit.

L'ABSENCE DE SOURCES
L'IA peut citer des sources qui semblent plausibles mais n'existent pas. « Selon une étude de l'Université de [X] publiée en 2019 ». Vérifiez toujours.

3 L'importance de la vérification

Pour limiter ces dérives, il convient de considérer par défaut toute réponse générée comme une hypothèse à vérifier, et non comme un fait établi : cela implique de systématiser la relecture humaine, le croisement des informations avec des sources fiables et, lorsque c'est possible, l'exigence de références vérifiables.

LES RISQUES LIÉS À LA VIE PRIVÉE

1 L'utilisation des données personnelles

Aujourd'hui, les réseaux sociaux et les plateformes d'intelligence artificielle collectent une quantité croissante, et souvent sous-estimée, de données personnelles. Chaque publication, commentaire, interaction, « like » ou partage sur Facebook, Instagram, LinkedIn, X (anciennement Twitter) ou encore les échanges avec Gemini (Google) peuvent potentiellement être utilisés pour entraîner des modèles d'IA. Cela signifie concrètement que vos photos, vos textes, vos préférences personnelles et même vos conversations peuvent servir à améliorer les performances de ces outils commerciaux, souvent sans consentement explicite de votre part, ou avec un consentement obtenu de manière peu transparente.

META : CE QUE VOUS PUBLIEZ ENTRAÎNE L'IA

Prenons un exemple concret et récent : Meta, la société mère de Facebook, Instagram et WhatsApp, a informé ses utilisateurs européens que leurs publications publiques, leurs commentaires et leurs légendes de photos seraient utilisés pour entraîner ses intelligences artificielles à partir du 27 mai 2025. Pour l'instant, les messages privés échangés sur WhatsApp, protégés par le chiffrement de bout en bout, ne seraient pas concernés par cette collecte. En revanche, tout ce qui est publié en mode public peut être aspiré par les algorithmes et intégré aux données d'entraînement.

↑ SOMMAIRE

2 Quelles sont les conséquences ?

Lorsque vos données sont utilisées pour entraîner des IA, elles peuvent être mémorisées, analysées, recombinées et parfois réutilisées dans des contextes totalement inattendus. Par exemple, une IA conversationnelle pourrait théoriquement restituer à un autre utilisateur des informations sensibles qu'elle a « apprises » lors d'une précédente interaction avec vous, révélant ainsi involontairement des éléments de votre vie privée.

3 Comment s'opposer concrètement à la réutilisation de ses données personnelles ?

Heureusement, il existe des moyens concrets et accessibles pour agir et mieux protéger ses données. La Commission nationale de l'informatique et des libertés (CNIL) propose un guide pratique détaillé pour s'opposer à la réutilisation de ses données personnelles par les principales plateformes d'IA et de réseaux sociaux.

Sur Facebook et Instagram, il est possible de refuser explicitement l'utilisation de ses informations en se rendant dans le centre de confidentialité de votre compte et en remplissant un formulaire d'opposition dédié. Cette démarche peut être réalisée pour chaque compte individuellement, et une confirmation est normalement envoyée par e-mail une fois que votre demande de retrait du consentement a été prise en compte.

3.4 Bien utiliser l'IA générative

QU'EST-CE QU'UN PROMPT ?

Un prompt est un terme anglais que l'on peut traduire en français par « requête » ou « instruction ». Un prompt est tout simplement le texte, la question ou la consigne que l'on soumet à une intelligence artificielle ou à un chatbot pour obtenir une réponse. C'est l'interface de communication entre l'utilisateur humain et la machine. Par exemple, lorsque vous demandez à un chatbot « Donne-moi la météo à Lyon pour demain », cette phrase constitue le prompt. Le chatbot analyse ce prompt, le décompose, en extrait le sens et l'intention, puis génère une réponse adaptée en fonction de ses capacités et de ses données.

LE PROMPT ENGINEERING : STRUCTURER SES REQUÊTES POUR DES RÉPONSES OPTIMALES

Afin d'obtenir la réponse la plus pertinente possible de la part d'un agent conversationnel, il faut préparer un prompt précis et complet. Voici les éléments fondamentaux d'un prompt efficace :

L'INSTRUCTION

Il s'agit de la consigne principale donnée à l'IA, qui précise l'action attendue.

LE FORMAT DE RÉPONSE

Indiquer la forme attendue, par exemple « sous forme de liste à puce », favorise une sortie lisible et adaptée à vos besoins.

LE CONTEXTE

Préciser le domaine, la situation, l'objectif ou l'audience permet de personnaliser la réponse et d'assurer qu'elle soit pertinente.

LE TON

Demander un style particulier, tel qu'un ton « calme et clair », module la présentation et l'accessibilité des informations.

LE RÔLE / PERSONA

Spécifier que l'IA agit comme « un assistant personnel » dirige le niveau de détail, la posture et l'approche de la réponse.

ANONYMISER SES REQUÊTES : PROTÉGER LES DONNÉES PERSONNELLES

Protéger les identités, adresses, ou informations sensibles est essentiel, tant pour nos propres données que celles des tiers concernés.
Deux méthodes principales existent :

- **La généralisation :** Substituer la donnée personnelle par une catégorie ou un groupe (« ex : un bénévole senior avec des problèmes de dos dans une grande ville »).
- **L'approximation :** Utiliser une estimation, par exemple « environ 30 ans », « près de Rennes ».

CONTRÔLER LA VÉRACITÉ DES RÉPONSES DE L'IA

Il demeure impératif d'exercer un esprit critique sur toutes les réponses générées par l'IA. Les erreurs factuelles, interprétations erronées ou confusions subsistent, même dans des modèles avancés.

Limiter les biais et les discriminations dans les réponses de l'IA

- Formulez vos requêtes de façon neutre,
- Analysez toujours les réponses avec recul,
- Identifiez les critères utilisés par l'IA, et évaluez leur pertinence ou leur caractère discriminatoire.

3.5 Adopter l'IA au quotidien : guide pratique pour la rédaction de textes

L'ART DU « PROMPT ENGINEERING »

Les composants d'un prompt efficace pour la rédaction de texte :

- **Le contexte :** « Agis comme un journaliste expérimenté spécialisé dans les affaires municipales »,
- **La tâche :** Que voulez-vous ? « Rédige une introduction accrocheuse pour un article sur le nouveau plan de circulation »,
- **Le format :** Comment le voulez-vous ? « En 100 mots maximum, ton informatif mais accessible, avec une statistique marquante »,
- **Les contraintes :** Qu'est-ce qu'il ne faut pas ? « Évite le jargon technique, ne prends pas position politique »,
- **Les exemples :** Montrez ce que vous attendez « Dans le style de : Chaque matin, 15 000 voitures s'entassent dans le centre-ville… ».

3.6 Deepfake et risques informationnels

LA DÉSINFORMATION ET LES « DEEPFAKES » : LA NOUVELLE ÈRE DE LA MANIPULATION

Nous entrons dans une ère où fabriquer un mensonge crédible est devenu aussi simple que de commander une pizza. Quelques prompts bien formulés, et voilà : un faux communiqué de presse, une fausse déclaration d'un politique, une fausse Une de journal. Le tout en quelques secondes, pour seulement quelques centimes.

Prenons un exemple concret qui pourrait se passer dans votre région. Imaginez qu'un projet d'infrastructure divise votre communauté : disons, un projet de centrale éolienne. Avec l'IA générative, les opposants pourraient :

- Générer de faux témoignages de riverains d'autres régions racontant des nuisances causées par des éoliennes,
- Créer de fausses études scientifiques avec des graphiques et données inventées,
- Fabriquer de faux articles de presse locale d'autres régions relatant des problèmes imaginaires,
- Produire de fausses déclarations d'élus ou d'experts.

Le tout serait partagé sur les réseaux sociaux, dans les groupes WhatsApp locaux, peut-être même envoyé à votre rédaction. Sans vigilance extrême, certains de ces faux contenus pourraient se retrouver dans vos pages.

LES DEEPFAKES : QUAND VOIR N'EST PLUS CROIRE

Si les faux textes sont préoccupants, les deepfakes, ces vidéos et audios falsifiés, représentent un saut supplémentaire dans la manipulation. La technologie a progressé à une vitesse vertigineuse. Il y a 10 ans, les deepfakes étaient grossiers, facilement détectables. Aujourd'hui, ils peuvent tromper même des observateurs avertis.

Les implications pour le journalisme sont vertigineuses :

- **Le problème de la preuve :** Traditionnellement, une vidéo ou un enregistrement audio était une preuve plutôt solide. « J'ai la vidéo » signifiait « j'ai l'information ». Cette équation ne tient plus. Chaque « preuve » doit maintenant être questionnée, vérifiée, authentifiée.
- **L'effet de doute généralisé :** Paradoxalement, le plus grand danger des deepfakes est qu'ils créent un doute sur tout. Les politiques peuvent maintenant crier « Fake news ! » face à n'importe quelle vidéo compromettante. Le déni plausible devient systématique.
- **La course aux armements technologiques :** Nous sommes engagés dans une course sans fin entre les créateurs de deepfakes et les détecteurs. Chaque nouvelle génération de détection est rapidement contournée par une nouvelle génération de création.

LES BIAIS ALGORITHMIQUES : QUAND L'IA REPRODUIT ET AMPLIFIE NOS PRÉJUGÉS

Si les hallucinations sont des erreurs ponctuelles, les biais sont des déformations systématiques. Et ils sont partout dans l'IA générative, pour une raison simple : l'IA apprend à partir des données et des algorithmes d'apprentissage qui reflètent les biais de notre société.

Types de biais courants dans l'IA générative :

- **Biais de genre :** Demandez à une IA de générer une histoire sur deux personnages qui se rencontrent dans un bar : l'un travaille dans le secteur du luxe et l'autre dans le secteur du bâtiment. Il y a de fortes chances que le personnage du secteur du luxe soit une femme et que l'autre soit un homme, reproduisant les stéréotypes de genre.
- **Biais raciaux :** Les IA peuvent associer certaines ethnies à certains comportements, métiers ou caractéristiques, perpétuant des stéréotypes dangereux.
- **Biais socio-économiques :** Les réalités des classes populaires sont souvent sous-représentées ou mal représentées dans les données d'entraînement, dominées par les productions des classes moyennes et supérieures connectées.

CONFIDENTIALITÉ ET PROPRIÉTÉ DES DONNÉES | PROTÉGER SES SOURCES ET SON TRAVAIL

C'est l'une des erreurs les plus graves qu'on peut commettre avec l'IA générative, et pourtant elle est terriblement facile à faire. Vous travaillez tard, vous devez terminer une note, un rapport ou le CR d'une réunion. ChatGPT est là, gratuit, efficace. Vous envoyez l'audio ou l'intégralité d'un texte pour générer une note synthétique. En quelques minutes, vous avez votre texte. Pratique, non ? Sauf que vous venez peut-être de compromettre vos données confidentielles.

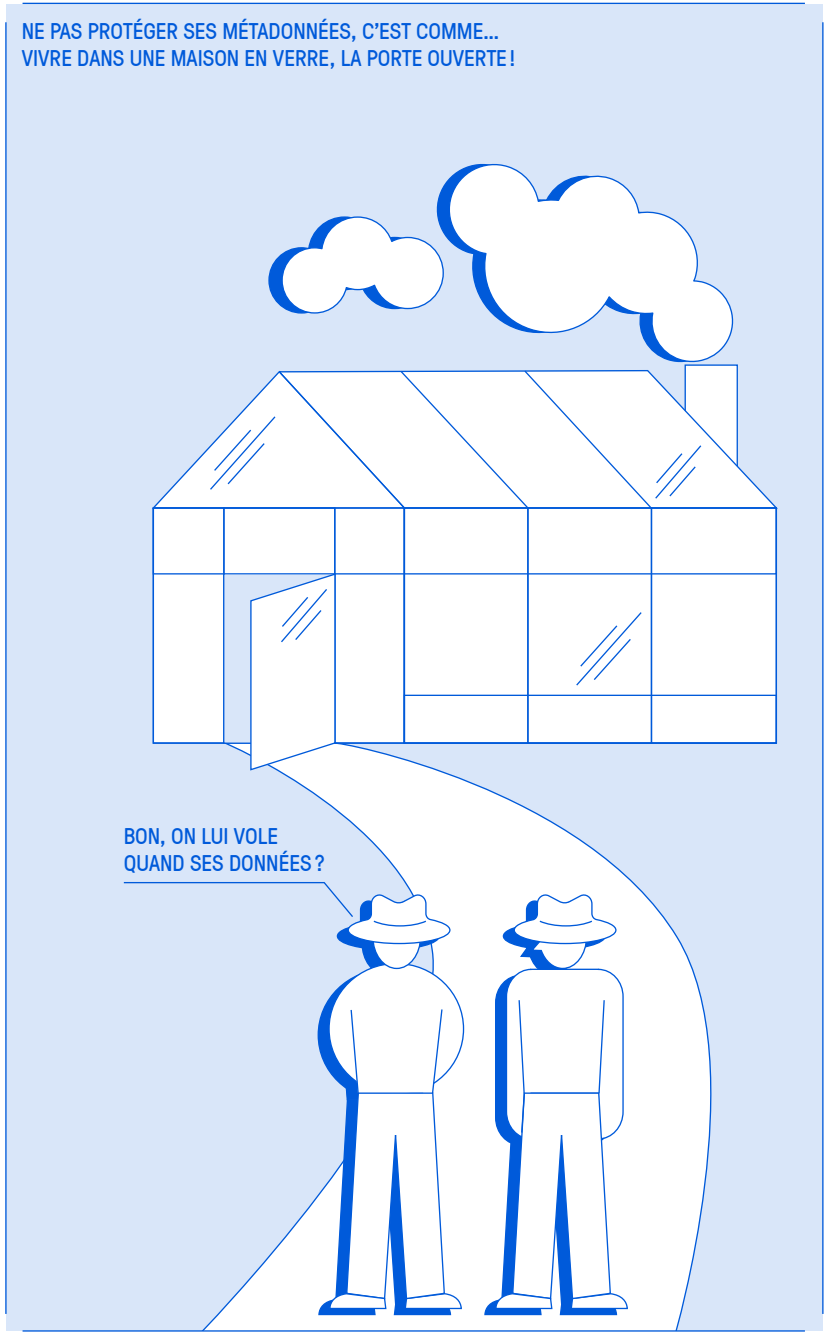
Quand vous entrez des données dans un système d'IA commercial, ces données ne disparaissent pas après utilisation. Elles peuvent être :

- Stockées sur des serveurs
- Utilisées pour améliorer le modèle,
- Accessibles aux employés de l'entreprise,
- Vulnérables aux fuites ou aux piratages,
- Soumises aux demandes légales des autorités.

LE CAS PARTICULIER DES MÉTADONNÉES

Les journalistes oublient souvent les métadonnées, ces informations invisibles attachées aux fichiers. Une photo contient l'heure, le lieu, l'appareil utilisé. Un document Word peut contenir l'historique des modifications, les commentaires supprimés, l'identité de l'auteur. Quand vous joignez ces fichiers dans une IA pour analyse, toutes ces métadonnées partent avec. C'est une fuite d'information potentielle. Pensez donc à :

- Vérifier et nettoyer les métadonnées avant tout versement dans un outil d'IA,
- Utiliser des outils spécialisés comme MAT2 ou Exifcleaner qui sont open-source,
- Préférez le copier-coller de texte brut quand c'est possible.



L'impact environmental de l'IA

7 068 DATA CENTERS DANS LE MONDE.

NOMBRE DE DATA CENTERS PAR PAYS

4 184
ÉTATS-UNIS

515
ROYAUME-UNI

514
ALLEMAGNE

369
CHINE

345
FRANCE

296
INDE

287
CANADA

272
AUSTRALIE

257
JAPON

219
ITALIE

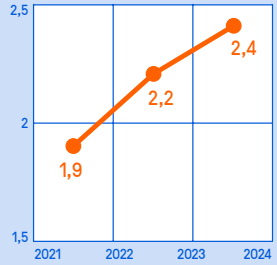
205
BRÉSIL

195
ESPAGNE

Source : Statista, 2026

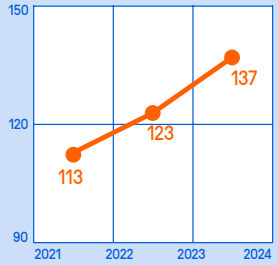
L'EMPREINTE ENVIRONNEMENTALE DES OPÉRATEURS DE CENTRES DE DONNÉES EN FRANCE PAR AN

CONSOMMATION
ÉLÉCTRIQUE EN TWH.



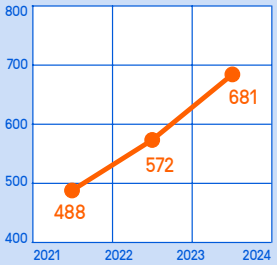
En 2024, les centres de données en France ont consommé l'équivalent de la consommation électrique de Bordeaux Métropole.

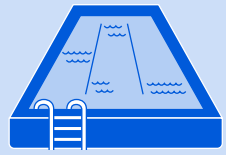
ÉMISSION DE GAZ À EFFET DE SERRE
EN MILLIERS DE TCO_2 EQ.



En 2024, les centre de données en France ont consommé l'équivalent de 65.500 allers retours Paris-New York.

VOLUME D'EAU PRÉLÉVÉE
DIRECTEMENT EN MILLIERS DE M^3





En 2024, les centres de données en France ont consommé l'équivalent de 7 567 piscines olympiques.

Source : ARCEP, 2025. « Pour un numérique soutenable » édition 2025 : le résumé en infographies (17 avril 2025) p.4

↑ SOMMAIRE

À retenir
L'intelligence artificielle

L'intelligence artificielle générative redéfinit nos usages numériques et professionnels. Mais son déploiement s'accompagne de défis majeurs, qu'il s'agisse de la protection des données, de la gestion des risques, ou de la lutte contre les biais et les discriminations.

Pour profiter pleinement de ces opportunités sans négliger les dangers :

1
Protégez et anonymisez autant que possible vos données personnelles.

2
Vérifiez systématiquement la véracité des informations délivrées par l'IA.

3
Soutenez les solutions respectueuses des normes européennes pour la souveraineté et la sécurité.

4
Favorisez une IA « frugale » peu consommatrice en ressources et responsable sur le plan environnemental.

5
Gardez systématiquement le contrôle humain sur toutes décisions critiques.

6
Face à l'évolution rapide de ces technologies, la curiosité et la vigilance resteront vos meilleurs atouts. Restez informé, partagez vos connaissances et contribuez à un futur numérique plus sûr et inclusif.

SOUVERAINETÉ NUMÉRIQUE

4

Ce module vous invite à explorer trois dimensions de la souveraineté numérique :

1. Comprendre les enjeux à travers une analyse critique des solutions populaires. Ex. Google Drive, WhatsApp, Slack, Canva,
2. Identifier les risques : sécurité, confidentialité, dépendance technologique,
3. Découvrir des alternatives : outils libres et souverains pour reprendre le contrôle.

Pour aborder un sujet aussi vaste que la souveraineté numérique, il faut d'abord partir d'un constat : nous vivons pleinement dans l'ère du cloud computing, nos données et nos outils sont stockés systématiquement dans des serveurs auxquels nous avons accès à travers une connexion Internet. Pour les plus jeunes d'entre nous, cette manière de concevoir nos outils informatiques est devenue la norme ; pour les plus anciens, la transition s'est opérée plus ou moins naturellement, au gré de l'évolution de nos usages.

4.1 Le Cloud computing

Le cloud computing est aujourd'hui omniprésent dans notre quotidien : il permet de stocker des données et d'utiliser des logiciels ou des services en ligne sans qu'ils soient installés directement sur nos appareils. Des outils de travail collaboratif aux plateformes de streaming où nous accédons à nos films et séries préférés, tout repose sur des serveurs distants opérés par de grandes entreprises technologiques.

QU'EST-CE QUE LE CLOUD COMPUTING ?

Selon la CNIL, le cloud computing désigne une pratique numérique : « nos applications et nos données ne se trouvent plus sur un ordinateur déterminé, mais dans un nuage composé de nombreux serveurs distants interconnectés ». Autrement dit, il est de plus en plus rare que nous installions nos outils ou sauvegardions nos fichiers sur nos ordinateurs. Nous les stockons désormais directement dans ce fameux nuage, qui, en réalité, ne nous appartient pas. Nous utilisons chaque jour des services qui semblent pratiques, intuitifs, voire gratuits. Cette externalisation offre souplesse et efficacité, mais elle soulève une question fondamentale : qui contrôle réellement vos outils, vos données et les usages qui en sont faits ? Derrière l'apparente immatérialité du cloud, se joue un enjeu central de souveraineté numérique, de dépendance technologique et de maîtrise de l'information. A quel prix payons-nous réellement cette commodité ?

L'ENJEU DE LA SOUVERAINETÉ NUMÉRIQUE

Selon l'éditeur de logiciels français Oodrive, la souveraineté numérique est la capacité d'une personne, d'une organisation ou d'une nation à garder la maîtrise de ses données, de ses infrastructures et de ses outils informatiques. Pourquoi cela importe-t-il ? Chaque jour, nous générons des données précieuses : messages privés, photos de famille, documents professionnels, historiques de navigation. Ces données sont collectées, analysées, parfois revendues à des tiers ou exploitées à des fins que nous ignorons. Enfin, la souveraineté numérique touche aussi à notre capacité de maintenir nos activités économiques et associatives en cas de panne ou de crise géopolitique majeure.

4.2 Les risques de la dépendance numérique

LE CLOUD | LE CAS DE DE GOOGLE DRIVE : PRATIQUE, MAIS À QUEL PRIX ?

Google Workspace est une suite d'outils en ligne de Google qui sert d'espace de travail complet. De la messagerie Gmail, aux réunions Google Meet en passant par Google Sheets ou Google Docs, la simplicité de ce réseau d'applications et l'interopérabilité entre eux en a fait un succès majeur de Google. Mais derrière cette façade se cachent pourtant des réalités moins rassurantes.

1 Google conserve l'accès à vos clés de chiffrement

Bien que Google Drive chiffre vos données, l'entreprise détient les clés de déchiffrement. Contrairement aux systèmes à « connaissance zéro » (zero-knowledge), Google peut accéder à vos fichiers, les scanner avec ses algorithmes de reconnaissance d'images, et les partager avec les autorités en réponse à des demandes légales. C'est un problème fondamental : Google détient les clés de vos données. Toutefois, depuis 2023 le « Client-side encryption » (CSE) pour certains comptes professionnels haut de gamme (Workspace Enterprise Plus, Education Plus) permet à l'utilisateur de contrôler ses propres clés de chiffrement. Malheureusement, cette fonction reste absente pour les comptes gratuits.

2 Absence de chiffrement de bout en bout par défaut

Le chiffrement de bout en bout signifie que seul vous et le destinataire pouvez lire le message ou accéder au fichier. Google Drive n'en dispose pas par défaut pour les comptes standards. C'est le cas de la plupart des fournisseurs cloud grand public : Dropbox, Microsoft OneDrive, Apple iCloud qui fonctionnent selon le même principe par défaut. C'est devenu un standard de l'industrie, car il permet la synchronisation, la recherche intelligente et la collaboration en temps réel. Le chiffrement de bout en bout, bien que plus sécurisé, rendrait ces fonctionnalités impossibles ou considérablement plus complexes.

3 Intégrations tierces et surface d'attaque accrue

Pour assurer une expérience toujours plus simplifiée, Google Drive s'intègre à des centaines d'applications tierces. Une application malveillante ou compromise pourrait théoriquement accéder à votre compte Google. Google met cependant à disposition des outils de gestion : révision des autorisations accordées aux applications tierces, authentification à deux facteurs obligatoire pour les comptes sensibles, alertes de sécurité en cas d'activité suspecte. Le risque existe, mais il reste gérable avec une bonne hygiène numérique.

4 Votre objectif : faire un choix éclairé

En utilisant Google Drive gratuitement, vous ne payez pas avec de l'argent, mais vous confiez vos données à une infrastructure qui n'est pas sous votre contrôle total. Bien que Google affirme ne pas utiliser vos fichiers privés à des fins publicitaires, l'entreprise conserve l'accès technique à vos données et peut les scanner pour répondre aux demandes légales, ou améliorer ses services. De plus, tout contenu que vous rendez public pourrait être utilisé pour entraîner les modèles d'IA de Google. Faut-il pour autant fuir Google Drive ? Pas nécessairement. Pour un usage personnel standard le service reste raisonnablement sûr et offre un excellent rapport commodité-risque. En revanche, si vous manipulez des données sensibles (informations médicales confidentielles, documents juridiques stratégiques, données personnelles de tiers) les limites évoquées deviennent parfaitement légitimes.

Dans ces cas précis, il devient justifié d'opter pour des solutions zero-knowledge comme Tresorit, Sync.com ou ProtonDrive, où même le fournisseur ne peut accéder à vos fichiers. Une autre option consiste à chiffrer manuellement vos fichiers sensibles avant de les télécharger sur Drive, en utilisant des outils open-source comme Cryptomator ou VeraCrypt. La question n'est donc pas de savoir si Google Drive est « sûr » ou « dangereux » dans l'absolu, mais plutôt : est-il adapté à l'usage que vous en faites ? La réponse dépend de la sensibilité de vos données, et du niveau de contrôle que vous souhaitez conserver.

LES MESSAGERIES PRIVÉES : LE CAS DE WHATSAPP

Si les applications de messagerie ne sont généralement pas classées parmi les applications de cloud computing au sens classique (comme Google Drive), elles s'appuient pourtant largement sur des infrastructures cloud. La sensibilité des informations qu'on y partage mérite donc une attention particulière.

1 WhatsApp : chiffrement de bout en bout, mais des métadonnées exposées

Depuis 2016 et l'intégration du protocole Signal à son fonctionnement, WhatsApp s'est forgé une solide réputation en matière de sécurité, grâce à l'utilisation du chiffrement de bout en bout. Cet atout s'ajoute à une interface simple et conviviale, ainsi qu'à une immense base d'utilisateurs qui facilite la communication. Cependant, cet important travail pour s'imposer comme une solution de messagerie sécurisée accessible au plus grand nombre cache certaines limites. Parmi celles-ci figure un point essentiel : les métadonnées restent accessibles.

2 L'accès aux métadonnées et à vos contacts

Même si vos messages sont chiffrés, WhatsApp conserve des métadonnées telles que l'identité de vos correspondants, la fréquence et les horaires de vos échanges, le type d'appareil utilisé ou encore votre adresse IP. Ces informations peuvent en révéler beaucoup sur votre vie, sans même avoir à lire le contenu de vos messages. De plus, par défaut, votre profil WhatsApp (numéro de téléphone, photo, statut) est visible pour l'ensemble de vos contacts et peut être indexé. Autre limite : WhatsApp appartient au géant Meta, une entreprise dont l'historique en matière de protection de la vie privée est pour le moins discutable (ex : scandale Cambridge Analytica).

3 Le chiffrement de bout-en-bout

Par ailleurs, le chiffrement sur WhatsApp ne s'applique pas automatiquement aux sauvegardes dans le cloud. Par défaut, lorsque vous sauvegardez vos conversations sur iCloud ou Google Drive, ces sauvegardes ne sont pas chiffrées de bout en bout. Depuis 2021, WhatsApp propose cependant une option de « sauvegarde chiffrée de bout en bout », permettant de protéger également les sauvegardes stockées sur iCloud ou Google Drive. Cette option repose sur un mot de passe ou une clé de récupération définie par l'utilisateur. Une fois

↑ SOMMAIRE

activées, les sauvegardes sont chiffrées avant d'être envoyées dans le cloud, et ni Apple, ni Google, ni WhatsApp ne peuvent en lire le contenu.

LE NAVIGATEUR WEB : UN MAILLON SOUVENT OUBLIÉ

Quand on parle de souveraineté numérique, on évoque plus rarement le rôle du navigateur... Alors qu'il est, en réalité, l'un des maillons les plus critiques. C'est par lui que transite la majorité de nos usages en ligne, et c'est aussi lui qui sert d'interface privilégiée par les géants du numérique pour collecter des données sur vos habitudes.

Un « système d'exploitation » intrusif ?

Le navigateur n'est pas juste un logiciel parmi d'autres, c'est devenu le « système d'exploitation du web » et, mal conçu ou mal choisi, il peut se transformer en outil de suivi extrêmement intrusif. Or deux mécanismes en particulier posent particulièrement problème.

1 Le fingerprinting (empreinte numérique)

Même sans cookies, un site peut vous identifier de manière quasi unique en combinant des éléments de configuration (taille et résolution d'écran, polices installées, extensions, langue, fuseau horaire, modèle d'appareil, capacités graphiques, etc.). Les navigateurs basés sur l'écosystème Google (comme Chrome) exposent historiquement beaucoup d'API et de signaux qui facilitent ce profilage fin, très prisé dans l'industrie publicitaire.

2 La synchronisation de compte

Lorsque vous utilisez Chrome connecté à votre compte Google, l'historique de navigation, les favoris, voire les mots de passe et onglets peuvent être synchronisés dans le cloud de Google. Pratique pour retrouver ses données sur plusieurs appareils, mais cela signifie aussi que ces informations se retrouvent centralisées chez un acteur unique, avec tous les enjeux de confidentialité et juridiques que cela implique.

3 La quasi-hégémonie de Google

À cela s'ajoute un enjeu de souveraineté plus discret, mais tout aussi important : la quasi-hégémonie du moteur Chromium (le socle technique de Chrome). La majorité des navigateurs grand public

s'appuie désormais sur ce moteur : Chrome, Edge, Brave, Opera, Vivaldi et bien d'autres. En contrôlant l'évolution de Chromium, Google influence de fait les standards techniques du web : l'introduction de Manifest v3, par exemple, réduit les capacités de certains bloqueurs de publicité comme uBlock Origin, ce qui impacte tous les navigateurs qui suivent la branche principale de Chromium.

4 Firefox, l'exception Mozilla

Dans ce paysage, Mozilla Firefox occupe une place particulière : il repose sur son propre moteur (Gecko), développé par une fondation à but non lucratif, avec une gouvernance distincte de Google. Techniquement, Firefox constitue un véritable contre-pouvoir : si demain Google décidait de fermer le code de Chromium ou d'imposer des choix techniques défavorables aux utilisateurs, Firefox continuerait d'exister indépendamment. Des variantes « durcies » comme LibreWolf cherchent même à réduire encore la télémétrie et certains compromis ergonomie / confidentialité, pour les publics les plus exigeants.

L'idée n'est pas de dire qu'il existerait un « navigateur parfait », mais de rappeler que votre choix de navigateur conditionne largement ce que les plateformes peuvent voir de votre activité, et qui contrôle les règles du jeu. Reprendre la main sur ce simple choix est souvent l'un des gestes les plus puissants, et les plus sous-estimés, en matière de souveraineté numérique.

4.3 Les alternatives numériques au GAFAM

Passons maintenant aux solutions pratiques. Il est temps de découvrir les outils qui permettent concrètement de reconquérir votre souveraineté numérique. Ces alternatives existent, elles sont matures, et beaucoup sont plus accessibles que vous ne l'imaginez.

STOCKAGE ET PRODUCTIVITÉ : SE LIBÉRER DE GOOGLE DRIVE

Google Drive n'est pas le seul logiciel de travail collaboratif. D'autres solutions existent à ce jour. Dans ce chapitre nous vous présentons d'autres outils que votre organisation pourrait utiliser.

1 Nextcloud

Nextcloud est une solution open source qui vous permet d'héberger vos propres fichiers en gardant le contrôle total. Le code source est entièrement ouvert et transparent, vous pouvez l'auto-héberger ou opter pour un hébergement géré auprès de fournisseurs européens certifiés RGPD. Tout comme Google Drive, Nextcloud ne se contente pas du stockage. Il offre la collaboration en temps réel sur des documents (via LibreOffice ou ONLYOFFICE), des calendriers partagés, la gestion de contacts, et même de la visioconférence. Le chiffrement de bout en bout est disponible pour vos fichiers les plus sensibles. Aucune métadonnée n'est collectée à des fins publicitaires.

2 La Suite Numérique : l'initiative d'État

Lancée en 2025 par le gouvernement français, La Suite Numérique représente la réponse officielle de l'État aux GAFAM. Cette plateforme gratuite regroupe Tchap (messagerie chiffrée utilisée par l'administration), France Transfert (partage de fichiers sécurisé), Grist (tableur collaboratif), un éditeur de documents, et des outils de visioconférence.

Plus de 70 % des administrations françaises l'ont adoptée début 2025, prouvant sa viabilité à grande échelle. Accessible à tous les citoyens, elle constitue une alternative crédible et entièrement gratuite pour ceux qui cherchent une solution francophone, hébergée en France, et portée par une volonté politique claire de souveraineté numérique.

3 kSuite d'Infomaniak : l'alternative Suisse

kSuite, développée par l'hébergeur suisse Infomaniak, propose une suite complète (mail, agenda, contacts, Drive, visioconférence) avec un positionnement unique : souveraineté suisse, engagement écologique fort (datacenters 100 % énergies renouvelables), et interface moderne rivalisant avec Google Workspace.

Infomaniak se distingue par sa transparence radicale : publication annuelle de son bilan carbone, engagement à ne jamais revendre les données, hébergement exclusif en Suisse. L'offre gratuite est généreuse, les tarifs payants raisonnables, et le support client réputé excellent.

4 OVH, le cloud français et européen

Cette entreprise fondée à Roubaix et devenue l'un des principaux acteurs européens du cloud, incarne une vision du numérique fondée sur la souveraineté technologique, la protection des données et l'indépendance stratégique de l'Europe.

Face à la domination des géants américains et asiatiques du secteur, l'entreprise défend un modèle alternatif reposant sur des infrastructures localisées en Europe, une plus grande transparence dans la gestion des données et le respect des réglementations européennes, notamment le RGPD.

Le groupe développe ses propres serveurs, maîtrise une grande partie de sa chaîne technologique et investit dans des centres de données à haute efficacité énergétique afin de réduire l'empreinte environnementale du numérique.

Par ailleurs, l'entreprise joue un rôle croissant dans la cybersécurité et les infrastructures stratégiques européennes. En 2026, OVHcloud a été associée à un contrat de 180 millions d'euros attribué par la Commission européenne pour le développement et l'exploitation de services cloud souverains destinés aux institutions et aux acteurs publics européens. Cette collaboration illustre la volonté de l'Union européenne de soutenir des acteurs technologiques capables de garantir l'hébergement sécurisé des données sensibles sur le territoire européen.

MESSAGERIE SÉCURISÉE : AU-DELÀ DE WHATSAPP

Il existe bien d'autres solutions de messagerie à WhatsApp que nous vous présentons dans ce chapitre.

1 Signal : la référence

Cette application est considérée par les experts en sécurité comme la référence absolue en confidentialité. Le chiffrement de bout en bout est activé par défaut sur tous les messages, appels vocaux et vidéo. Contrairement à WhatsApp, Signal a été conçu pour minimiser les informations qu'il détient sur vous. L'application ne connaît même pas vos contacts ni avec qui vous communiquez. Elle ne conserve que votre numéro de téléphone et la date de dernière connexion. Développée par la Signal Foundation, organisation à but non lucratif financée par des dons, sans publicité ni revente de données. Messages éphémères, appels de groupe, partage de fichiers : tout y est.

2 Element et Matrix : open source et interopérabilité

Element s'appuie sur Matrix, un protocole de communication décentralisé et standardisé, soit l'équivalent pour la messagerie de ce qu'est le protocole e-mail. Au lieu de créer encore une application incompatible, Matrix établit un standard ouvert permettant à différents services de communiquer entre eux. Element offre un chiffrement de bout en bout, un code open source, la possibilité d'auto-héberger votre instance, et le support de discussions publiques ou privées. Le gouvernement français et l'armée allemande ont adopté Matrix pour leurs communications internes sensibles. Bien que réservée aux agents publics, son existence démontre qu'une messagerie souveraine à grande échelle est techniquement viable.

UN ÉCOSYSTÈME EUROPÉEN QUI GRANDIT

Outre ces deux problématiques centrales, que sont les outils de productivité et les messageries privées, le domaine de l'open-source a su se développer par lui-même dans l'ombre des géants d'Internet.

1 Le développement de l'open source

En France, le mouvement de souveraineté numérique a notamment été porté par l'écosystème associatif bien avant que la sphère politique ne s'en empare et il est impossible de ne pas mentionner des organisations

comme Framasoft qui proposent des dizaines de services libres gratuits et adaptés aux structures associatives. Jitsi Meet est l'alternative open source à Zoom et Google Meet, Penpot peut devenir votre prochaine version auto-hébergée de Canva.

2 VPN et gestionnaire de mots de passe

D'autres outils méritent une attention plus particulière comme les VPN ou les gestionnaires de mots de passe. Pour rappel, un VPN chiffre votre trafic Internet et masque votre adresse IP, mais exige une confiance totale envers le fournisseur. Privilégiez les VPN basés en Europe, avec politique « zéro logs » vérifiée par audit. Le suédois Mullvad se distingue par son approche radicale : pas de compte avec e-mail, juste un numéro généré aléatoirement, paiement en cash accepté, code partiellement open source, audits réguliers. Côté gestionnaire de mots de passe, Bitwarden, est une référence open source avec une version gratuite complète avec synchronisation illimitée, authentification à deux facteurs, auto-hébergement possible.

3 Pour finir : et l'IA dans tout ça ?

Au-delà des offres d'IA proposées par les géants américains (Google, Microsoft, OpenAI, Meta), un écosystème d'acteurs existe notamment en Europe. Ces solutions ne remplacent pas encore entièrement les suites « tout-en-un » comme Google Workspace dopées à l'IA, mais elles offrent des briques plus souveraines pour certains usages. On peut citer, par exemple, des modèles ouverts développés par des acteurs européens ou internationaux comme ceux de Mistral AI qui peuvent être auto-hébergés ou intégrés dans des environnements maîtrisés, réduisant ainsi l'exposition des données à des acteurs externes.

↑ SOMMAIRE

4.4 Les principes de la souveraineté numérique

Face à la domination des géants technologiques américains et à l'émergence de puissances numériques chinoises, l'Union Européenne a pris le pari d'adopter une approche proactive. L'objectif ? Bâtir un cadre réglementaire visant à protéger ses citoyens, et tenter de créer les conditions d'émergence d'une industrie numérique européenne souveraine.

LES SOLUTIONS JURIDIQUES ET POLITIQUES

1 La loi SREN : le cloud souverain avant tout

En mai 2024, la France a franchi une étape supplémentaire avec l'adoption de la loi SREN (Sécuriser et Réguler l'Espace Numérique). Ce texte marque un tournant dans la doctrine française du cloud computing. Désormais, les données sensibles de l'État doivent être hébergées via des infrastructures qualifiées selon le référentiel SecNumCloud, une certification élaborée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Bien sûr, la réalité sur le terrain reste complexe. Début 2024, Microsoft a été choisi pour héberger les données médicales des Français via le Health Data Hub, et EDF a opté pour AWS pour une partie de ses données. Ces décisions ont suscité de vives controverses et illustrent la difficulté pour la France et l'Europe de concilier leurs ambitions de souveraineté avec les réalités économiques et techniques d'un marché dominé par les acteurs américains. Néanmoins, l'intention politique est claire, et les outils législatifs se mettent progressivement en place.

2 L'AI Act : réguler l'Intelligence Artificielle

En 2024, l'Union Européenne a également franchi une nouvelle étape en adoptant le premier cadre législatif régulant l'intelligence artificielle. Le règlement européen sur l'IA (AI Act) est entré en vigueur le 1er août 2024, et son ambition est considérable : encadrer le développement et l'utilisation des systèmes d'IA pour garantir qu'ils respectent les droits fondamentaux, la démocratie et l'État de droit. Il classe les systèmes d'IA en quatre catégories principales : risque inacceptable (systèmes

interdits comme la notation sociale ou la reconnaissance biométrique de masse), risque élevé (secteurs sensibles comme la santé, l'emploi ou la justice), risque limité (obligation de transparence, comme indiquer qu'un contenu est généré par IA), et risque minimal ou nul.

3 Le Cyber Resilience Act : renforcer la résilience des produits connectés

En parallèle de ces cadres globaux, le Cyber Resilience Act intègre une notion jusque-là absente au niveau européen : la cybersécurité « by design ». Concrètement, ce règlement vise à imposer des standards de cybersécurité stricts à tous les produits numériques mis sur le marché européen, en particulier les objets connectés (IoT). En exigeant des mises à jour de sécurité obligatoires, une divulgation rapide des vulnérabilités, et une documentation technique claire, le CRA adresse un risque majeur : la prolifération de dispositifs non sécurisés exposant les utilisateurs et les infrastructures critiques.

4.5 Migrer à son rythme : une feuille de route en 5 étapes !

On vous a préparé une feuille de route pour y voir un peu plus clair et entamer, peut-être dès aujourd'hui, le long chemin vers la souveraineté numérique :

COMMENCER PAR UN AUDIT PERSONNEL

Listez tous les services que vous utilisez régulièrement. Pour chacun, demandez-vous : où sont mes données ? Quelles informations sont collectées ? Cette entreprise est-elle soumise au Cloud Act ? Ces données sont-elles sensibles ? Cet audit permet de prioriser : commencez par remplacer les services traitant vos données les plus sensibles.

EXPÉRIMENTER SANS PRESSION

Installez Signal et invitez quelques amis proches. Créez un compte sur Nextcloud ou sur La Suite Numérique pour tester. Téléchargez LibreOffice et ouvrez un document. Organisez un appel test sur Jitsi. Cette phase d'expérimentation doit durer quelques semaines, sans pression. Autorisez-vous à trouver certains outils moins pratiques, c'est normal. L'important est de vous familiariser progressivement.

MIGRER SERVICE APRÈS SERVICE

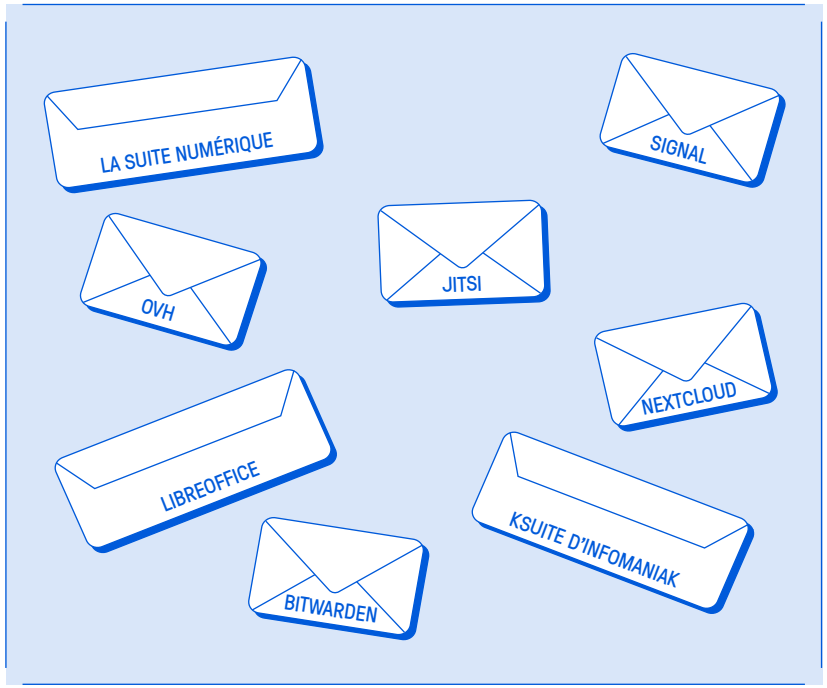
Commencez par vos nouveaux fichiers importants : sauvegardez-les sur Nextcloud plutôt que Google Drive. Encouragez votre cercle proche à utiliser Signal pour les conversations familiales, tout en gardant WhatsApp dans votre vie professionnelle. Transférez progressivement vos mots de passe vers Bitwarden, quelques comptes par jour. Cette période de transition, où vous utilisez deux systèmes en parallèle, peut sembler redondante mais elle est essentielle pour éviter les ruptures brutales. Après quelques mois, évaluez ce qui fonctionne bien. Automatisez ce qui peut l'être : sauvegardes, synchronisations. Documentez vos solutions pour les partager avec votre entourage.

ACCEPTER LES COMPROMIS

Vous n'avez pas besoin d'être parfait. Beaucoup devront garder WhatsApp pour leur famille ou Google Drive pour leur entreprise. C'est acceptable. L'important n'est pas d'atteindre une pureté idéologique mais de progresser vers plus de contrôle. Utiliser Signal pour les conversations confidentielles et WhatsApp pour le reste est un compromis raisonnable. La souveraineté numérique n'est pas tout ou rien, c'est un spectre, un équilibre personnel entre commodité et contrôle.

IMPLIQUER VOTRE ENTOURAGE

Les outils de communication ne valent que si d'autres les utilisent. Chaque personne que vous convainquez d'installer Signal rend l'application plus utile pour tous. Proposez plutôt que d'imposer. Invitez des amis à essayer Signal en expliquant simplement pourquoi. Suggérez à votre association d'explorer Nextcloud. Organisez un atelier informel. Le bouche-à-oreille et l'exemple personnel sont infiniment plus efficaces que les grands discours.



À retenir
La souveraineté numérique

Des outils commodes et gratuits comme Google Drive ou WhatsApp ont des revers en termes de confidentialité et de protection des données.

Les outils existent et les alternatives sont viables. Le cadre juridique européen se construit. Les communautés sont actives et accueillantes. Les prochaines étapes dépendent de nous.

La souveraineté numérique n'est pas une destination finale mais un chemin continu d'apprentissage et d'ajustement. Ce qui compte, c'est le mouvement, la direction. Installer Signal et convaincre trois amis, c'est une victoire.

Les 5 étapes à suivre pour être souverain :

1. Commencer par un audit personnel
2. Expérimenter sans pression
3. Migrer service après service
4. Impliquer votre entourage
5. Accepter les compromis

↑ SOMMAIRE

RGPD : DONNÉES ET CONFORMITÉ

5

Comment protéger les données personnelles de votre structure tout en respectant le Réglement Général sur la Protection des données (RGPD) ? Ce module vous permet de :

- Comprendre ce qu'est une donnée personnelle et identifier celles que vous traitez,
- Connaître les droits des personnes concernées et savoir comment y répondre,
- Appliquer les principes fondamentaux du RGPD dans vos pratiques quotidiennes,
- Mettre en place les mesures de sécurité appropriées,
- Documenter votre conformité et savoir réagir en cas d'incident.

Tâchons, dans un premier temps, de définir précisément le RGPD, ses acteurs et les notions à assimiler avant d'aller plus loin.

5.1 Des réponses politiques et juridiques de l'UE

Depuis l'ouverture d'Internet au grand public, jusqu'à l'avènement du cloud en passant par l'explosion des réseaux sociaux, notre vie numérique n'a cessé de se développer.

DÉCODEZ LE RGPD POUR PROTÉGER LES DONNÉES QUE L'ON VOUS CONFIE

Une année et un texte ont marqué un tournant dans la façon dont l'Europe envisage ces thématiques : l'adoption du dit « RGPD ». Le Règlement Général sur la Protection des Données (RGPD) est un texte législatif européen adopté en 2016 et entré en application le 25 mai 2018. Il constitue le socle de la protection des données personnelles au sein de l'Union Européenne, remplaçant une directive de 1995 devenue obsolète suite aux transformations numériques. L'essence de ce texte peut se résumer en une idée simple : il consacre le fait que protéger les données personnelles dont vous avez la charge n'est pas seulement un devoir moral envers les personnes qui vous font confiance, c'est également une obligation légale.

LE RGPD : UN TEXTE DONT LES BÉNÉFICES SONT ENCORE MÉCONNUS

Depuis plus de sept ans, le RGPD s'applique à toute organisation, publique ou privée, qui traite des données personnelles de personnes se trouvant sur le territoire européen, quelle que soit la taille de la structure ou son lieu d'implantation. Pourtant, le RGPD reste encore largement méconnu, notamment dans le secteur associatif. Beaucoup le perçoivent comme un ensemble de contraintes administratives supplémentaires, une paperasse inutile qui viendrait alourdir leur charge de travail déjà importante. Le RGPD n'est pas un fardeau. C'est un cadre protecteur qui, bien compris et bien appliqué, permet de sécuriser votre activité, de renforcer la confiance de vos parties prenantes, et de structurer vos pratiques de manière pérenne.

5.2 Le RGPD, comprendre le cadre juridique

D'OÙ VIENT LE RGPD ?

Le RGPD n'est néanmoins pas le premier texte venant consacrer les principes de protection des données personnelles. En effet, la Loi Informatique et Libertés (LIL) de 1978 contribuait déjà à poser les bases en la matière et à en désigner une autorité de contrôle qu'est la CNIL.

LES ACTEURS DU RGPD

Pour bien appréhender le RGPD, il faut d'abord identifier les différents acteurs qui sont concernés par ce texte, leurs responsabilités et leurs droits respectifs :

- Le responsable de traitement est la personne physique ou morale (généralement l'organisation elle-même) qui détermine les finalités et les moyens du traitement des données personnelles.
- Le sous-traitant est une personne physique ou morale qui traite des données personnelles pour le compte et sur instruction du responsable de traitement.
- Le délégué à la protection des données (DPO) est une personne désignée par l'organisation pour piloter la conformité au RGPD, conseiller le responsable de traitement, et servir de point de contact avec la CNIL et les personnes concernées.
- La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité de contrôle française créée en 1978 et chargée de veiller au respect des principes de protection des données personnelles. Elle a pour missions d'informer, de conseiller, de contrôler et de sanctionner.
- Enfin, la personne concernée désigne toute personne physique dont les données sont traitées. Il s'agit de vos bénéficiaires, de vos adhérents, de vos salariés, de vos bénévoles, de vos donateurs, ou même de simples visiteurs de votre site web.

LES NOTIONS CLÉS DU RGPD

Maintenant que nous avons une vision d'ensemble des différents acteurs liés par le RGPD, il convient de maîtriser quelques notions fondamentales qui structurent l'ensemble du règlement.

- Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Elle englobe les données évidentes comme le nom, le prénom, l'adresse électronique, le numéro de téléphone, mais également des éléments moins directs comme un numéro d'adhérent, une adresse IP, un identifiant de connexion, ou même une photographie.
- La pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, numéro, etc.). Ainsi, les données ne peuvent plus être attribuées à une personne identifiée, sans information supplémentaire (table de correspondance entre le numéro ou l'alias et le nom / prénom de la personne).
- L'anonymisation consiste à utiliser un ensemble de techniques de manière à rendre impossible toute identification de la personne par quelque moyen que ce soit et de manière irréversible.
- Certaines données sont qualifiées de sensibles et bénéficient d'une protection renforcée. Il s'agit des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, biométriques, concernant la santé, la vie sexuelle ou l'orientation sexuelle.

LE RGPD PRÉVOIT 5 BASES LÉGALES PRINCIPALES

1. le consentement de la personne concernée
2. l'exécution d'un contrat
3. le respect d'une obligation légale
4. la sauvegarde des intérêts vitaux
5. l'exécution d'une mission d'intérêt public, ou l'intérêt légitime du responsable de traitement

LES SIX GRANDS PRINCIPES DU RGPD

Nous voici donc déjà bien avancés. Les notions et acteurs centraux du RGPD sont identifiés, il faut désormais entrer dans le cœur du sujet, à savoir tout mettre en œuvre au sein de votre organisme pour respecter au mieux le RGPD. Prenons comme référence le site de la CNIL et suivons les six principes qu'il énonce pour dérouler les actions concrètes à mettre en œuvre. Appliquez-les dès à présent dans votre organisation.

1 Ne collectez que les données vraiment nécessaires pour atteindre votre objectif

Commençons par ce qui doit devenir le centre de pilotage de votre politique RGPD : le registre des activités de traitement. Ce document obligatoire vous permet de recenser et d'analyser les traitements de données personnelles qui vous sont confiées et d'identifier les parties prenantes qui interviennent, les catégories de données traitées, leurs finalités, leurs durées de conservation et les mesures de sécurité mises en place pour les protéger.

Le principe de minimisation

Cette pratique se nomme « le principe de minimisation » dans le RGPD. Comme le définit la CNIL, il « prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. » Pour donner un cas d'application, il n'est pas nécessaire de fournir le statut marital d'un salarié dans un fichier RH.

APPLIQUEZ LE PRINCIPE DE MINIMISATION AU QUOTIDIEN

Pour appliquer ce principe au quotidien, vous pouvez créer les outils et documents suivants :

CRÉER DES FICHES DE TRAITEMENT AVEC TROIS BLOCS : FINALITÉ, BASE LÉGALE, LISTE DES DONNÉES STRICTEMENT NÉCESSAIRES.

REVOIR VOS FORMULAIRES EXISTANTS (PAPIER ET EN LIGNE) ET SUPPRIMER LES CHAMPS SUPERFLUS.

↑ SOMMAIRE

2 Soyez transparent

Au moment de vous confier des informations les concernant, les personnes dont vous traitez les données doivent comprendre ce que vous faites, pourquoi vous le faites, et quels sont leurs droits.

COMMENT APPLIQUER LA TRANSPARENCE DANS VOTRE ORGANISATION ?

La transparence est un pilier du RGPD. Au moment où vous collectez les données, la personne doit ainsi savoir :

- Qui est responsable du traitement (nom de la structure, coordonnées de contact) ?
- À quoi vont servir les données (finalités) ?
- Sur quelle base légale repose le traitement ?
- Combien de temps seront-elles conservées ? Quels critères permettent de déterminer cette durée ?
- Quels sont ses droits (accès, rectification, effacement, opposition, limitation, portabilité, saisir la CNIL) et comment les exercer ?
- Est-ce qu'il y a des transferts hors Union Européenne ? Avec quelles garanties ?

3 Organisez et facilitez l'exercice des droits des personnes

Informer sur les droits ne suffit pas : vous devez aussi organiser votre structure pour être réellement capable d'y répondre dans de bonnes conditions.

COMMENT VOUS PROTÉGER ?

Pour faciliter l'exercice de ces droits, vous pouvez d'ores et déjà prévoir :

- Une adresse e-mail dédiée (du type « donneespersonnelles@... » ou « rgpd@... »),
- Un formulaire en ligne ou une rubrique sur votre site expliquant la démarche,
- Une adresse postale pour les personnes qui ne sont pas à l'aise avec le numérique.

Veillez à ce que ces informations soient cohérentes avec vos mentions d'information et votre politique de confidentialité.

Ensuite, définissez un processus interne clair :

- Réception de la demande (e-mail, courrier, formulaire),
- Vérification de l'identité du demandeur et de la légitimité de la demande (surtout en cas de données sensibles ou de risque d'usurpation),
- Recensement des données dans vos différents systèmes (fichiers, logiciels, archives),
- Analyse de la demande (acceptation, refus motivé, limitation, délai supplémentaire si nécessaire),
- Réponse dans un délai d'un mois, en expliquant ce qui a été fait.

En cas de demande complexe, vous pouvez prolonger le délai de deux mois supplémentaires, à condition d'en informer la personne dans le premier mois.

4 Fixez des durées de conservation

Enfonçons une porte ouverte : on ne peut pas conserver des données personnelles indéfiniment. La durée de conservation doit être en cohérence avec la finalité du traitement et, le cas échéant, avec les obligations légales applicables.

DÉTERMINEZ LA DURÉE DE CONSERVATION DES DONNÉES ET LE METTRE EN ŒUVRE

Il vous revient alors de déterminer une durée de conservation en « base active », pendant laquelle les données sont utilisées pour la gestion courante. Le cas échéant, une durée d'archivage (accès restreint, pour répondre à des obligations légales, des contrôles ou des contentieux potentiels). Un mode de suppression ou d'anonymisation à l'issue de ces durées.

COMMENT METTRE EN ŒUVRE CES DURÉES DE CONSERVATION ?

Pour mettre en œuvre ces durées de conservation, vous pouvez paramétrer des règles automatiques de suppression ou d'anonymisation ou planifier des campagnes régulières de « nettoyage » des fichiers. Pensez également à adapter vos contrats avec vos sous-traitants pour qu'ils respectent aussi ces durées.

5 Sécurisez les données et identifiez les risques

Un fléau majeur touche tout type d'organisme : la violation de données. La CNIL définit une violation de données comme un incident de sécurité ayant des conséquences sur la confidentialité, l'intégrité ou la disponibilité des données personnelles (perte, accès non autorisé, divulgation, altération).

QUE FAIRE EN CAS DE VIOLATION DES DONNÉES ?

Votre rôle en tant que responsable de traitement vous contraint à plusieurs obligations en cas de violation de données. Parmi elles, vous devez vous préparer à détecter et qualifier un incident (quelles données, combien de personnes concernées, quelles conséquences possibles), mettre en œuvre rapidement des mesures correctives. D'abord, il vous faut informer l'autorité compétente à ce sujet – la CNIL – dans un délai de 72h pour déposer une déclaration initiale. Ensuite, s'il y a un risque élevé, il faut prévenir les personnes concernées.

6 Inscrivez la mise en conformité dans une démarche continue

Le dernier des six principes listé par la CNIL nous paraît être une conclusion parfaite à ce module : inscrire la mise en conformité dans une démarche continue.

Pour avancer de manière réaliste et adaptée à vos moyens, vous pouvez structurer votre démarche de mise en conformité en plusieurs phases, l'occasion de cocher pour une dernière fois quelques cases :

- Une première phase d'état des lieux vise à cartographier vos traitements, vos outils et vos sous-traitants, puis à repérer les écarts les plus critiques, par exemple des données sensibles insuffisamment sécurisées ou une absence totale d'information des personnes.
- Une deuxième phase consiste à mettre en place les fondamentaux : formaliser le registre, actualiser les formulaires et les mentions d'information, déployer les mesures de sécurité de base, organiser l'exercice des droits, définir une procédure de gestion des incidents et encadrer par écrit les relations avec vos prestataires.
- Dans une troisième phase, vous entrez dans une logique d'amélioration continue : revues régulières du registre, mise à jour des durées de conservation et des politiques internes, renforcement de la formation et de la sensibilisation des équipes, lancement d'analyses d'impact lorsque cela s'avère nécessaire.

En adoptant cette ligne de conduite, vous ne cherchez pas une perfection théorique inaccessible, mais une conformité pragmatique et évolutive. Le RGPD devient alors moins une contrainte qu'un cadre de confiance : pour les personnes que vous accompagnez, pour vos partenaires, pour vos équipes, et pour la pérennité de votre structure.

5.3 Vos droits dans l'espace numérique

Lorsque vous avez constaté une infraction à vos droits dans l'espace numérique, vous pouvez porter plainte auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

CE QUI PEUT FAIRE L'OBJET D'UNE PLAINTE

La CNIL protège vos données personnelles : son action porte donc sur les questions liées au RGPD. Vous pouvez la saisir dès qu'une atteinte à vos données est constatée. Cela inclut, par exemple, un refus injustifié de crédit, une demande d'accès à vos informations auprès d'un organisme, la suppression d'un contenu sur un réseau social au titre du droit à l'oubli, le signalement de spams, ou encore l'usage abusif de vidéosurveillance en entreprise. La liste complète des situations et vos droits sont disponibles sur le site de la CNIL.

PRÉPARER ET TRANSMETTRE LA PLAINTE

Avant de déposer une plainte, réunissez une description claire des faits, l'identité de l'organisme visé (nom, coordonnées, SIREN), vos informations et toute preuve utile (échanges, captures, URL). La plainte doit être en français ; un mandat est nécessaire si vous agissez pour autrui. Le dépôt le plus rapide se fait via le service en ligne de la CNIL, avec création de compte pour suivre l'avancement. L'envoi par courrier reste possible : CNIL – Service des plaintes, 3 place de Fontenoy, 75007 Paris.

SUIVI ET RECOURS

La CNIL vérifie la complétude du dossier, contacte l'organisme si la plainte concerne l'exercice d'un droit et peut intervenir selon les manquements constatés. Une première réponse est donnée sous trois mois. En cas d'insatisfaction, un recours gracieux puis, en dernier ressort, un recours devant le Conseil d'État sont possibles.

À retenir
Comprendre et appliquer vos droits dans le cyberespace

Pour votre organisation vous pouvez créer les outils et documents suivants :

- Créer des fiches de traitement avec trois blocs : finalité, base légale, liste des données strictement nécessaires.
- Revoir vos formulaires existants (papier et en ligne) et supprimer les champs superflus.
- Adopter une « checklist formulaire » : toute nouvelle collecte passe par une validation RGPD (finalité + base légale + minimisation).
- Si vous pensez subir une infraction vous pouvez déposer une plainte auprès de la CNIL notamment en ligne sur leur site.
- Vous avez le devoir d'adopter la démarche du legal checking pour informer le plus justement votre audience.

Le RGPD prévoit 5 bases légales principales :

1. le consentement de la personne concernée
2. l'exécution d'un contrat
3. le respect d'une obligation légale
4. la sauvegarde des intérêts vitaux
5. l'exécution d'une mission d'intérêt public, ou l'intérêt légitime du responsable de traitement

↑ SOMMAIRE

Glossaire

L'authentification multifacteur (MFA)
L'authentification multifacteur vise à limiter le risque d'accès d'acteurs malveillants à certains outils et services informatiques d'une organisation. Le plus souvent, le MFA est une application sur un autre device que votre ordinateur (comme votre téléphone) afin d'être certain que ce n'est pas une personne tierce qui essaye de s'introduire via votre compte.

Cloud computing ou informatique dans les nuages
Le « cloud computing » est un anglicisme qui renvoie au réseau d'applications et de données hébergé dans un nuage, dit « cloud » composé de serveurs distants interconnectés plutôt que directement sur un ordinateur. Pour être concret, le cloud renvoie à vos espaces de travail partagés comme Google Drive par exemple.

Cyberespace
Le cyberespace désigne l'espace virtuel créé par l'interconnexion des réseaux numériques au niveau mondial. Il ne s'agit pas d'un lieu physique, mais d'un environnement constitué d'ordinateurs, de serveurs, de câbles sous-marins, de satellites, de smartphones et de milliards de données en circulation. Chaque mail envoyé, chaque paiement en ligne, chaque message sur un réseau social y transite.

Cybermenace
Ce concept renvoie aux risques d'attaques informatiques auxquels sont confrontées les organisations publiques comme privées. Elle résulte le plus souvent d'une faille, d'un virus ou d'un logiciel malveillant. La menace qui pèse sur ces organisations est protéiforme ; en raison de la diversité des acteurs concernés (hacker, groupe lié à la criminalité organisée, État) et des types d'attaques menés (*phishing*, rançongiciel, usurpation d'identité, etc.) Les motivations sont tout autant diverses bien qu'elles soient le plus souvent économiques et / ou politiques.

Une cybermenace désigne tout risque ou intention malveillante susceptible de compromettre un système d'information. Elle ne correspond pas encore à une attaque, mais à la possibilité qu'un acteur exploite une faille ou une vulnérabilité.

Ces menaces peuvent émaner de cybercriminels, États-nations, hacktivistes ou employés malveillants, et prendre diverses formes : *malwares*, campagnes de *phishing*, *ransomwares*, attaques DDoS, ou encore vols d'identifiants.

Cyber-résilience
La cyber-résilience renvoie à la capacité d'une organisation à faire face à une défaillance deson système informatique. Face à l'augmentation des actes de cyber malveillance, elle renvoie donc à une organisation à s'organiser de façon collective pour y faire face.

Dark web
Le Dark Web désigne la partie non indexée d'Internet, accessible uniquement via des réseaux anonymes comme Tor ou I2P. Il est fréquemment utilisé pour l'échange de données volées, la vente d'outils de piratage ou la diffusion de services illégaux, représentant ainsi un écosystème clé du cybercrime.

Deepfake
Un *deepfake* désigne un contenu audiovisuel falsifié à l'aide de l'intelligence artificielle, rendant possible la création de vidéos ou d'audios où une personne semble dire ou faire des choses qu'elle n'a jamais faites. Cette technologie représente un risque croissant pour la cybersécurité et la manipulation de l'information.

Donnée personnelle
Une donnée personnelle renvoie à toute information directe ou directe pouvant faire l'objet d'une collecte. D'une part, les informations directes sont votre prénom, nom, ou votre adresse postale. D'autre part, votre comportement sur Internet ou les réseaux sociaux constitue une information directe. Les données rattachées à une personne physique sont considérées comme des données personnelles à la différence de celles liées à une entreprise, un organisme, une administration ou une fondation.

Manipulation de l'information
C'est l'ensemble des actions malveillantes visant à diffuser des informations falsifiées, déformées (désinformation) ou partielles (malinformation) dans le cyberespace afin de remettre en cause la stabilité politique et / ou économique d'une organisation humaine.

↑ SOMMAIRE

Phishing ou hameçonnage

Phishing (ou hameçonnage) désigne une technique de fraude visant à inciter une victime à divulguer (identifiants, données bancaires, etc.) en usurpant l'identité d'un tiers de confiance, généralement via un e-mail, un SMS (smishing) ou un appel téléphonique (vishing).

Rançongiciel ou *ransomware*

Le *ransomware* (ou rançongiciel) est un logiciel malveillant qui chiffre des fichiers ou bloque l'accès à un système, exigeant le paiement d'une rançon pour restaurer l'accès. Il s'introduit dans un système via des e-mails piégés, des failles logicielles ou des sites compromis. Une fois actif, il chiffre les données critiques et exige une rançon (souvent en crypto monnaie) pour fournir la clé de déchiffrement.

Techniques, tactiques et procédures (TTPs)

Les TTPs (Tactics, Techniques, and Procedures) représentent les tactiques, techniques et procédures employées par les attaquants pour mener à bien leurs attaques. Par l'analyse de ces éléments, les spécialistes en cyber peuvent mieux comprendre le modus operandi des attaquants, anticiper leurs actions et mettre en place des contre-mesures efficaces.

Vulnérabilité

Faille de sécurité pouvant affecter un logiciel, un système d'information ou encore un composant matériel. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités sont généralement corrigées lors des mises à jour ou par des correctifs publiés par les éditeurs.

Source : CNIL, ANSSI, Advens, VIGINUM, France Num.

La cyber, un travail collectif

Ce guide est le résultat d'une démarche collective, construite grâce à la participation et aux échanges de l'ensemble des acteurs impliqués. Un immense merci à Alexandre Fayeulle, David Buhan et Grégoire Ducret qui permettent à Advens de construire une entreprise engagée au service de l'intérêt général, capable de protéger les acteurs vulnérables, essentiels à notre société et à notre démocratie. Une entreprise où performance et impact convergent et apprennent à se nourrir mutuellement.

Ce travail collaboratif s'est appuyé sur l'écoute, le dialogue et la mise en commun des savoirs. Il reflète une volonté partagée de co-construire des solutions adaptées, en tenant compte des réalités de terrain et des besoins exprimés.

Merci aux Advengers pour leur temps et pour leur engagement : Thibaut Allagbe, Erwan Battais, Mélodie Bouffier, Zoe Bressol, Sarah Carayol, Nicolas Carpentier, Fabian Cosset, Remi Martin De Abia, Aurélia Delfosse, Laure Deroche, Céline Dekeyser, David Deleau, Agathe Desflots, Guillaume Djourabtchi, Tanguy Ekizian, Emmanuel Haudebourg, Thibaut Havet, Aurélien Kittel, Cyprien Leseurre, Hugo Lausenaz-Pire, Frédéric Leclef, Sylvie Lepoutre, Tristan Lemonnier, Benjamin Leroux, Cyprien Leseurre, Quentin Louisiade, Matthieu Jonard, Jérémie Jordin, Léonard Keat, Isabelle Moguo, Eva Nassery, Claire Pétillot, Alice Picard, Tristan Savalle, Céline Vercruysse et Solène Vizier.

Merci à la formidable équipe d'Advens for People and Planet : Elsa Bouterin, Amandine Bretones, Sylvain Derreumaux, Charlotte Flesch, Grégoire Ducret, Lucile Gasber-Aad et Jade Mermet.

Un grand merci aux partenaires de Cyber for Good qui permettent de créer un collectif extraordinaire d'entreprises privées et acteurs publics, associations et coopératives : Aurélien Bayon, Carin Madsen Kollberg et toute l'équipe de Devoteam, Marc-Antoine Brillant, Victoria Blin, Léa Surugue, Elsie Russier de VIGINUM, Vincent Couronne et toute la rédaction de Les Surligneurs, Hervé Letoqueux et Nelly Pailley de Check First, Lucie Bouttier et Julie Kieffer de Share it, Augustien Courtier de Latitudes, Solidatech, Corentin Hue (France Générosités), Maxime Pauvert (Benevolt), Aline Morestin (Campus Cyber et C4T), Timothée Gosselin, Arnaud Cazenove et Bertille Mazari (Indie Hoster & Lasuite.coop), Virgile Deville (DINUM), Rémi Gerbet et toute l'équipe de Wikimedia France, Assoconnect, HelloAsso, CRESS Ile-de-France, Philanthro-Lab, makesense, à Camille Dorival (CareNews), Véronique Mathelin, Pierre Noro, Benjamin Treilhes, Théo Corsetti et Gaspard Loiseau (Science Po Paris), Julien Noé, Alice Pouillier et toute l'équipe de coop.médias.

Un merci tout particulier à Federica Calzoni et Fedrigoni France, et à Thanh-Phong Lê, Margaux Heylen et Marianne Poinsot de Travaux Pratiques pour la réalisation du guide et sa direction artistique. À Johan Giraud pour la création du très beau site cyberforgood.org.

Un grand merci à Amine Baba Aissa que nous lisons très souvent dans Numerama, et qui nous a accompagné dans la rédaction de ce guide.

↑ SOMMAIRE

↑ SOMMAIRE

↑ SOMMAIRE

Direction de publication
Giulio Zucchini

Coordination éditoriale
Ninon Bonnet de Paillerets

Rédaction
Advens :
Aurélia Delfosse
Jérémie Jordin
Léonard Keat
Hugo Lausenaz-Pire
Benjamin Leroux
Quentin Louisiade
Jade Marmet
Claire Pétillot
Alice Picard
Tristan Savalle

Numerama :
Amine Baba Aissa

Les Surligneurs :
Vincent Couronne

VIGINUM
Victoria Blin
Léa Surugue
Elsie Russier

Conception éditoriale et graphique
Travaux-Pratiques
Margaux Heylen
Thanh-Phong Lê
Marianne Poinsot

Impression
Le Réveil de la Marne

Papiers
Fedrigoni Arena High Definition white 120g, intérieur
Fedrigoni Symbol Freelife E/E33 Raster 200g, couverture

Mai 2026

cyberforgood.org
contact@cyberforgood.org

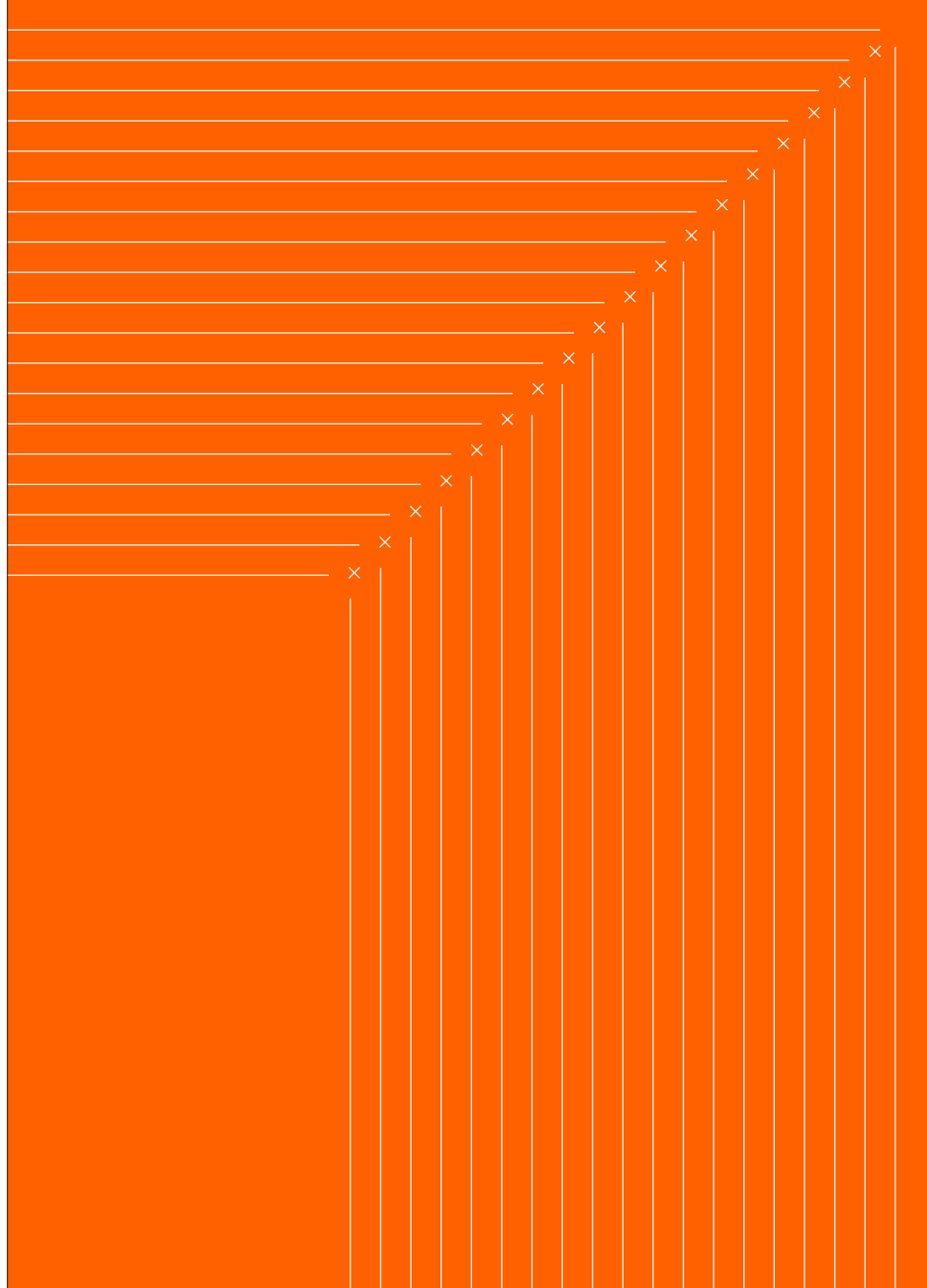
Advens for People and Planet

CYBER FOR GOOD

Advens CYBERSECURITY

devoteam Foundation

FEDRIGONI



TOUT CE QU'IL FAUT SAVOIR POUR PROTÉGER NOS DONNÉES

CYBERSÉCURITÉ

SOUVERAINETÉ NUMÉRIQUE

INTELLIGENCE ARTIFICIELLE

VULNÉRABILITÉS NUMÉRIQUES

ADVENS FOR PEOPLE AND PLANET