YACINE AIT-KACI
CAROLINE BOUDET
LUCIEN CASTEX
NICOLAS CHAGNY
CORINNE PULICANI

# DEVENIR GARDIEN DE SON INTERNET


**REPRENDRE LA MAIN SUR SES DONNÉES PERSONNELLES**
**APPRÉHENDER L'INTELLIGENCE ARTIFICIELLE**

AVEC LE SOUTIEN DU COLLECTIF EDUCNUM.

Internet Society France Chapter
FONDATION GoodPlanet
LA FONDATION ELYX SOUS L'ÉGIDE DE LA FONDATION BULLUKIAN

DEVENIR GARDIEN DE SON INTERNET

REPRENDRE LA MAIN
SUR SES DONNÉES PERSONNELLES
APPRÉHENDER
L'INTELLIGENCE ARTIFICIELLE

isoc.fr/education

**Édité par l'Internet Society (ISOC) France,
avec le soutien de la Fondation Internet Society.**

| | |
|---|---|
| **Dépôt légal** | Février 2025 |
| **ISSN** | En cours |
| **Impression** | Dupliprint Mayenne |


## AUTEURS

| | |
|---|---|
| **Yacine Ait Kaci** | Créateur du personnage ELYX, premier ambassadeur virtuel des Nations Unies depuis 2015 et Vice-Président de la Fondation ELYX. |
| **Caroline Boudet** | Journaliste indépendante et autrice. |
| **Lucien Castex** | Conseiller du Directeur général, Internet Gouvernance et société, à l'Afnic, membre de la Commission Nationale Consultative des Droits de l'Homme (CNCDH). |
| **Nicolas Chagny** | Président de l'Internet Society (ISOC) France, président de NS Pulse, cabinet de conseil pour les organisations et entreprises à impact positif, membre de la Commission Nationale Consultative des Droits de l'Homme (CNCDH). |
| **Corinne Pulicani** | Directrice du Domaine de Longchamp, Fondation GoodPlanet, Présidente du Think Tank NEXTDAY! & Vice-présidente de l'Internet Society France, en charge de l'éducation et de la culture. |
| **Cécile Charleux** | Directrice artistique. cc-studio.fr |


## REMERCIEMENTS

Les auteurs tiennent à remercier les nombreuses personnes ayant contribué à ce livre blanc par leurs conseils, apports, relectures, commentaires : Sébastien Bachollet, Carina Chatain (CNIL/Collectif EDUCNUM), Christophe Clouzeau (Temesis), Isabelle Diennet, Sylviane Peretz et Claire-Mélanie Popineau ainsi que les membres du collectif EDUCNUM et les experts de la CNIL.

## LICENCE



Internet Society France Chapter

L'Internet Society (ISOC) est une ONG internationale créée en 1992 dans le monde et en 1996 en France. C'est plus de 125 000 membres à travers le monde, une présence dans plus de 100 pays et près de 1 000 membres en France. Ceux-ci construisent le futur d'Internet, en en préservant ses fondements : un Internet libre, unique et ouvert à tous.

isoc.fr

FONDATION GoodPlanet

La Fondation GoodPlanet, reconnue d'utilité publique, a été créée en 2005 par Yann Arthus-Bertrand dans le prolongement de son travail artistique et de son engagement. Sa mission ? Sensibiliser le plus grand nombre aux enjeux écologiques et solidaires, et agir concrètement pour un monde plus durable, sur le terrain, en entreprises et au sein des collectivités.

goodplanet.org

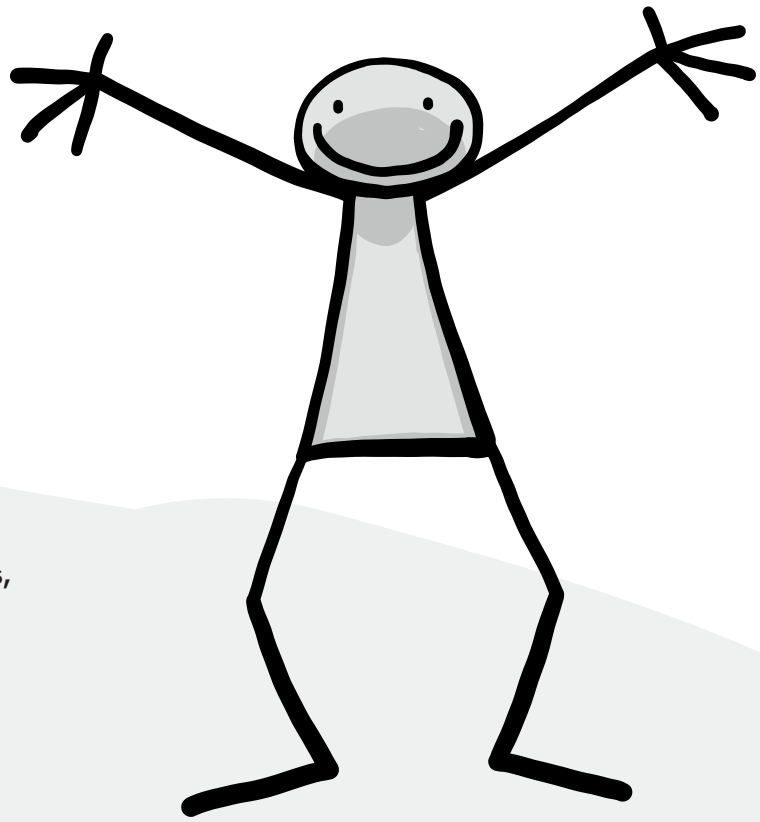
LA FONDATION ELYX SOUS L'ÉGIDE DE LA FONDATION BULLUKIAN

Depuis 2018, la Fondation ELYX sous l'égide de la fondation BULLUKIAN abrite la relation exclusive qu'entretient ELYX avec les Nations Unies ainsi qu'un programme de plaidoyer et d'éducation.

elyx.net/fondation

# SOMMAIRE





**À destination des familles, des parents, des enseignants, des éducateurs, des associations... et de tout cyber citoyen responsable, qui souhaite œuvrer à la construction d'un Internet plus sûr, plus juste et plus transparent pour tous.**

# INTRODUCTION

**LES DONNÉES, C'EST QUOI AU JUSTE ?**

Les données numériques sont un type de données exprimées en nombre le plus souvent stockées sous la forme de fichiers informatiques (texte, image...) ou indirectement (numéro de sécurité sociale, lieu et date de naissance, identifiant national élève, géolocalisation, numéro de téléphone, adresse électronique...).

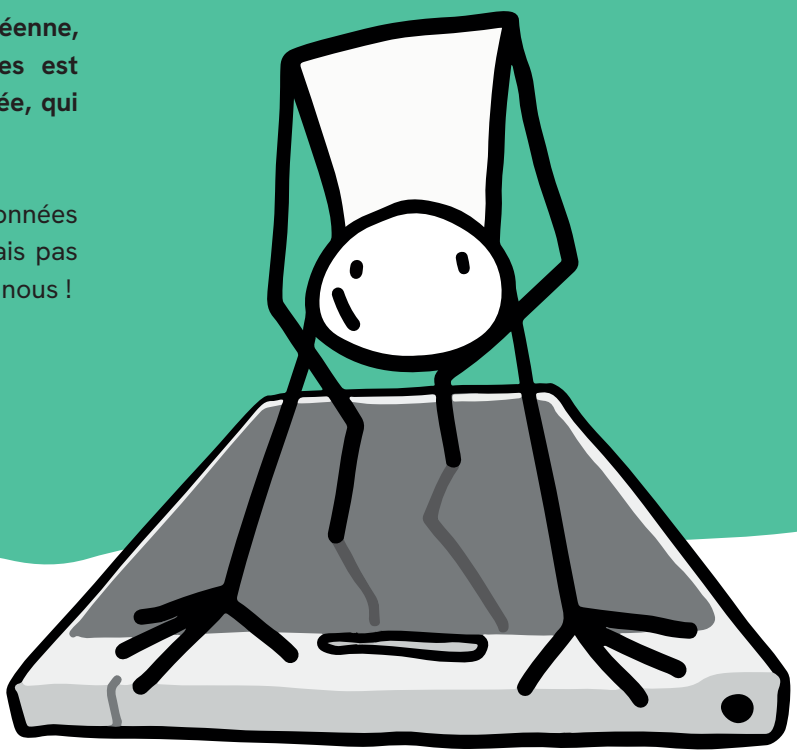
## IL EST DIFFICILE D'IMAGINER LE NOMBRE DE DONNÉES ÉCHANGÉES CHAQUE JOUR : C'EST CONSIDÉRABLE !

**Les données personnelles sont une émanation de chaque personne. Dans l'Union européenne, la protection des données personnelles est rattachée à la protection de la vie privée, qui est un droit fondamental.**

On a souvent l'impression que nos données personnelles sont éloignées de nous, mais pas du tout. Nos données personnelles, c'est nous !

Depuis près de 20 ans, l'utilisation massive des données, souvent à l'insu des personnes, pose un vrai problème de société. Car ces données ne sont pas éphémères. Leur traitement peut permettre de tracer, de profiler voire de ficher des individus, dans un but commercial ou de contrôle, correspondant à la mise en place d'une surveillance électronique.

Pour protéger les citoyens, trois principaux textes ont été mis en place au niveau européen : le Règlement général sur la protection des données (RGPD), ePrivacy (directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques) et le règlement sur les services numériques (DSA).



# LES LOIS SUR LA PROTECTION DES DONNÉES

**Le Règlement général sur la protection des données (RGPD),** qui a pour but de mettre fin à cette opacité en matière de traitement des données personnelles, s'applique dans les 28 États de l'Union européenne depuis le 25 mai 2018. En France, cette nouvelle réglementation européenne a renforcé les dispositions de la « loi informatique et liberté » de 1978 avec une extension et une coordination à toute l'Union européenne.

**17 483**

C'est le nombre de cas de violations de données en France notifiées à la CNIL de mai 2018 à mai 2023.
Plus de la moitié relèvent du piratage, le reste d'équipements perdus, volés ou publiés involontairement.

**La directive de 2002 sur la protection de la vie privée dans le secteur des communications électroniques, ou e-Privacy,** concerne le respect de la vie privée et la protection des données à caractère personnel dans toutes les communications électroniques.

La communauté européenne a adopté plusieurs directives et règlements : pour les marchés numériques (DMA), pour les services numériques (DSA) et, plus récemment, sur l'intelligence artificielle.

**Le règlement sur les services numériques (RSN ou DSA en anglais)** est entré en vigueur en 2023. Ce texte européen vise à « *créer un espace numérique plus sûr où les droits fondamentaux des utilisateurs sont protégés* ». Il encadre les plateformes numériques et les intermédiaires en ligne au sein de l'Union européenne : moteurs de recherche, réseaux sociaux, boutiques d'applications, plateformes de contenus... Le texte prévoit l'obligation, pour les très grandes plateformes, de mieux modérer les contenus illicites, haineux et la désinformation. Parmi les mesures : ouvrir l'accès à leurs données aux chercheurs, permettre aux internautes de désactiver l'algorithme et de signaler les contenus. Enfin, il interdit la publicité ciblée à destination de mineurs, ou basée sur des données privées comme l'orientation sexuelle ou les croyances religieuses.

Même si les lois existent, il est impératif de familiariser tous les usagers de services numériques, à ces enjeux, en créant un socle commun de connaissances éthiques, juridiques et techniques.

**Ce livre vous propose de mieux maîtriser votre degré d'exposition et de savoir agir efficacement en cas de problème.**

**Soyons tous des cybercitoyens actifs, attentifs et responsables. Œuvrons collectivement à la construction d'un Internet plus sûr, plus juste et plus transparent !**

PERSONNELLES ET DE LA VIE PRIVÉE.

# INTERNET


UN ESPACE DE RESSOURCES
FORMIDABLES... ET GRATUITES ?
PAS VRAIMENT.

**Internet offre un immense espace de ressources et une multitude de contenus consultables, pour la plupart, gratuitement. C'est un grand pas vers un libre accès aux savoirs, ainsi qu'à des services numériques, des réseaux sociaux, des sites d'informations, des jeux et applications… Mais attention !**

## SUR INTERNET, « SI TOUT EST GRATUIT, C'EST TOI LE PRODUIT ! »

Vous avez peut-être déjà lu cette phrase. Elle est claire : si on ne paye pas pour accéder à de nombreux contenus, services, réseaux, jeux, musiques, vidéos et applications en ligne, c'est qu'en échange de cette gratuité, certains fournisseurs de ces services exploitent nos données ou, par la publicité, nos temps de cerveau disponibles.

Indirectement, ils nous font également travailler gratuitement pour leurs intérêts : par exemple, en nous faisant reconnaître des objets dans des « captchas », ces séquences d'image où l'on doit cliquer sur les voitures, par exemple, ou en nous incitant à devenir leurs ambassadeurs en « likant » par un clic des contenus et en laissant des commentaires.

Ce n'est pas le cas pour tous les sites, par exemple les sites de services publics ou d'autres, comme Wikipédia. Mais l'exploitation à des fins publicitaires des données est la contrepartie la plus courante pour une utilisation « gratuite » des contenus et services proposés. Il faut en être conscient en naviguant.

**Visiter différentes pages Web, laisser un commentaire… sont autant d'informations que les fournisseurs de services numériques utilisent pour cerner finement les pratiques, les goûts et les habitudes des personnes. Ces données et leurs combinaisons rapportent de l'argent notamment par l'affichage de publicités très ciblées.**

Les données les plus convoitées sont celles concernant les habitudes et les possibilités de consommation, et donc aussi celles sur la santé, les liens familiaux et amicaux, les études suivies, les trajets réguliers ou les hobbies, par exemple. Elles sont encore plus recherchées si elles concernent les jeunes, cibles privilégiées des publicitaires.

## POUR UN INTERNET ÉCORESPONSABLE

**Le saviez-vous ?**
**En France, 10 % de la consommation électrique annuelle vient des services numériques, selon l'Ademe.**
**Et 2,5 % de l'empreinte carbone de la France est liée au numérique : c'est plus que les déchets !**
**Chacun peut agir au niveau quotidien pour diminuer cet impact.**

**Pour commencer, ne renouvelez votre téléphone ou votre ordinateur que lorsque c'est vraiment nécessaire, le matériel a un très gros impact sur l'environnement (jusqu'à 80 % des impacts globaux selon les analyses du cycle de vie) !**

# DONNÉES

## COMMENT ET POURQUOI MES DONNÉES SONT-ELLES EXPLOITÉES ?

## À QUOI SERVENT LES DONNÉES ?

**Les données numériques sont des informations stockées sur un ordinateur qui pourra ensuite les traiter facilement et automatiquement, les transmettre à un autre ordinateur,** rechercher une information parmi une grande quantité de données, les mettre en relation... Bien plus qu'un ensemble de 0 et de 1, c'est une grande quantité d'indications sur nous-mêmes que nous transmettons lors de nos pratiques et échanges numériques : textes, échanges vocaux, sites visités, logiciels installés, position géographique, type d'appareil, applications installées, coordonnées, sujets préférés, pages Web consultées, achats réalisés en ligne ou enregistrés sur une carte de fidélité...

## ET LES ALGORITHMES ?

**Pour traiter et exploiter toutes ces données, les développeurs informatiques conçoivent des méthodes** pour résoudre des problèmes, fournir des résultats exploitables et ajuster, ainsi, finement les contenus et services numériques. On appelle cela des algorithmes.

Certains logiciels et algorithmes collectent les données que nous émettons, les analysent, les interprètent et font des liens avec d'autres informations déjà mémorisées. Ils proposent ainsi des choix réduits, orientés vers une finalité pratique. Par exemple, un moteur de recherche affichera, simultanément aux informations demandées, de la publicité et des contenus issus de sites internet qui ont payé pour apparaître en début de liste dans les résultats de la requête.

DANS NOTRE VIE QUOTIDIENNE, NOUS ÉCHANGEONS SANS CESSE DES DONNÉES SANS NOUS EN APERCEVOIR.

C'est ainsi qu'il vous est peut-être arrivé de tomber par hasard, sur un réseau social, sur une publicité concernant un produit que vous avez cherché auparavant sur internet.

Plus on utilise les mêmes sites ou applications qui nous profilent, plus ces derniers peuvent collecter de données sur nous. Cela est particulièrement sensible, quand on se réfère aux géants d'Internet, souvent appelés les « GAFAM » (pour Google, Amazon, Facebook, Apple, Microsoft), qui possèdent de multiples plateformes, sites, applications et services, étant ainsi capables de suivre une très grande partie de nos navigations...

La transparence est importante, il est donc bon de savoir qui possède quoi. Meta possède Facebook, Instagram et Whatsapp ; Google possède YouTube, et des services comme Google Earth, Google Maps ou le marché d'applications, Google Play. Google est également présent sur de nombreux sites qui utilisent son outil de statistiques « Google analytics » ou même ses polices de caractères.

## COMMENT ET POURQUOI TRAITE-T-ON MES DONNÉES ?

**Le traitement des données peut être légal et non intrusif. Il existe des outils qui sont au service des internautes. Malheureusement certains sont créés ou détournés à des fins de traçage. Exemples :**

### LES COOKIES

**Ces petits fichiers sont déposés sur le disque dur de notre ordinateur** par le site visité pour permettre de reconnaître l'internaute lors d'une prochaine visite et d'éviter de lui redemander toujours les mêmes informations. Cependant, certains cookies dits « tiers » viennent de sites partenaires. Un site d'information peut par exemple accueillir des bannières de publicité contenant elles-mêmes des cookies.

Vérifiez les paramètres de votre navigateur et notamment ceux relatifs aux cookies. Le blocage des cookies tiers notamment permet de limiter la collecte de données par des tiers. Vous pouvez également tester des outils tels que Lightbeam, qui permettent de mettre en évidence la collecte de vos données de navigation. Il existe également des navigateurs qui visent spécifiquement à protéger la vie privée de leurs utilisateurs, tels que Firefox ou Brave par exemple.

**Plus simplement, lorsqu'on vous pose la question d'accepter tous les cookies ou d'en refuser certains, avant de cliquer sans réfléchir, prenez votre temps. Par exemple, vous pouvez refuser les cookies tiers dont le tiers vous est inconnu ou les cookies publicitaires. Vous pouvez aussi choisir de rester anonyme et refuser tous les cookies.**

### LA GÉOLOCALISATION

**Elle permet de savoir à quels endroits nous nous rendons** et d'en déduire nos trajets réguliers, nos hobbys, notre activité, nos habitudes de consommation.... Nous pouvons être géolocalisés en permanence parfois à notre insu. C'est le cas en ne désactivant pas le GPS ou le wifi, mais c'est également le principe même de téléphonie mobile, qui nécessite une localisation permanente afin de communiquer notre position à des bornes pour nous permettre de recevoir un appel.

### L'ADRESSE IP

**Une adresse IP, abréviation d'adresse de protocole Internet (Internet Protocol address), est un numéro d'identification lié à tout appareil connecté au réseau.** Ce numéro d'identité permet d'identifier la machine sur le réseau et lui permet de communiquer avec d'autres appareils et sites. Malheureusement elle permet aussi de savoir que c'est le même appareil qui a été sur différents sites et ainsi de retracer ses navigations.

Certains services permettent de masquer son adresse IP sur Internet, même si cela ne fonctionne pas à 100%. On parle de réseau privé virtuel (VPN) ou de serveurs proxy. Le réseau TOR permet également de séparer le lien entre l'appareil à l'origine de la communication et les navigations, rendant très difficile la possibilité de retracer les navigations.

## L'INSCRIPTION AVEC UN COMPTE

**La fonction inscription avec un compte d'une autre application** (par exemple via son compte Facebook) constitue un vrai danger pour vos données personnelles. En effet, en liant ces deux comptes vous donnez encore plus d'informations au site initial et augmentez d'autant votre degré d'exposition.

## LES COURRIERS ÉLECTRONIQUES ET LES MÉTADONNÉES

**Quand vous envoyez à un ami le texte "je t'invite à mon anniversaire" avec une photo de votre invitation, c'est le contenu du message.** Mais avec cet envoi, d'autres informations sont générées : on les appelle les métadonnées. Il s'agit, par exemple, des données techniques de transmission, des adresses électroniques concernées, des identifiants des correspondants, de la date et l'heure du message, des données d'identification de l'appareil d'envoi (pouvant indiquer sa position et de l'identifier), de la taille du message et de ses pièces jointes... Un simple mail en dit beaucoup sur vous !

## LES MESSAGERIES INSTANTANÉES

Elles sont pratiques et ludiques, mais savez-vous vraiment ce que vous offrez à ces plateformes ? Les photos et vidéos envoyées sur SnapChat restent stockées sur leurs serveurs. WhatsApp, qui appartient au même groupe que Facebook, lui donne accès à tous vos numéros de téléphones et aux métadonnées de vos échanges... Au moment de choisir un service, pensez à vérifier ses paramètres et son mode de fonctionnement, et que vous voyez bien dans l'adresse le petit cadenas indiquant que le site est protégé.

## LES APPLICATIONS MOBILES

**La plus grande partie du temps passé sur mobile est consacrée à des applications : réseaux sociaux, messageries, divertissement et jeux.** Avant d'installer une application, il faut être vigilant aux permissions accordées. Une application de messagerie peut vouloir accéder à votre appareil photo pour permettre d'en joindre une à votre envoi. Cependant, pourquoi une application de jeu voudrait pouvoir vous géolocaliser ou accéder à vos contacts ?

### 18H/SEMAINE

C'est, en moyenne, le temps passé par les 13-19 ans sur Internet, selon l'étude Junior Connect de 2022. Leur usage privilégié est celui des réseaux sociaux de vidéo (TikTok, Snapchat...)

### 15 ANS

En France, c'est l'âge de « la majorité numérique », requis pour exprimer seul son consentement à un service numérique (en dehors de cadres strictement réservés à des missions de services publics, par exemple).

### 71 %

C'est la proportion des 11-12 ans qui vont régulièrement sur un réseau social en 2023, selon une étude Born Social. L'accès à ces réseaux est théoriquement interdit avant 13 ans. En outre, 83 % des jeunes ont déjà un smartphone à 12 ans, d'après l'association Génération Numérique.

## LES OBJETS CONNECTÉS ET LEURS APPLICATIONS ASSOCIÉES

Montres géolocalisées, applications de santé, appareils de domotique, jeux et consoles vidéos… On estime entre 30 et 80 millions le nombre d'objets connectés sur la planète. S'ils facilitent la vie, ils recueillent aussi une multitude d'informations, en particulier sur vos pratiques.

## RÉSEAUX SOCIAUX ET SITES COMMUNAUTAIRES

Les réseaux sociaux offrent de nombreux avantages : communication, information, jeux… Attention toutefois, les risques de déconvenues y sont également démultipliés. L'illusion d'anonymat, la résonance d'Internet, la grande confusion entre les comptes professionnels et les comptes privés, sont autant de facteurs à risques.

# LE CAS TADATA-FRANCE

Le site et l'application Tadata ont envisagé de proposer aux 15-25 ans de gagner facilement et rapidement de l'argent contre la vente de leurs données personnelles.
L'Internet Society (ISOC) France a alerté la CNIL 2020 à ce sujet.
En effet, les données personnelles sont un droit fondamental et ne devraient pas à ce titre pouvoir faire l'objet d'une marchandisation.

Par ailleurs, l'Internet Society France a constaté de nombreuses non conformités en termes de transparence sur la confidentialité, l'âge d'accès au service…

**Ces non-conformités ont été corrigées depuis mais vos données sont trop précieuses pour les monnayer, à éviter, donc.**

# POUR UN INTERNET ÉCORESPONSABLE

**Tous les réseaux ne consomment pas la même quantité d'énergie. Ainsi la fibre est moins énergivore que le cuivre de l'ADSL.**

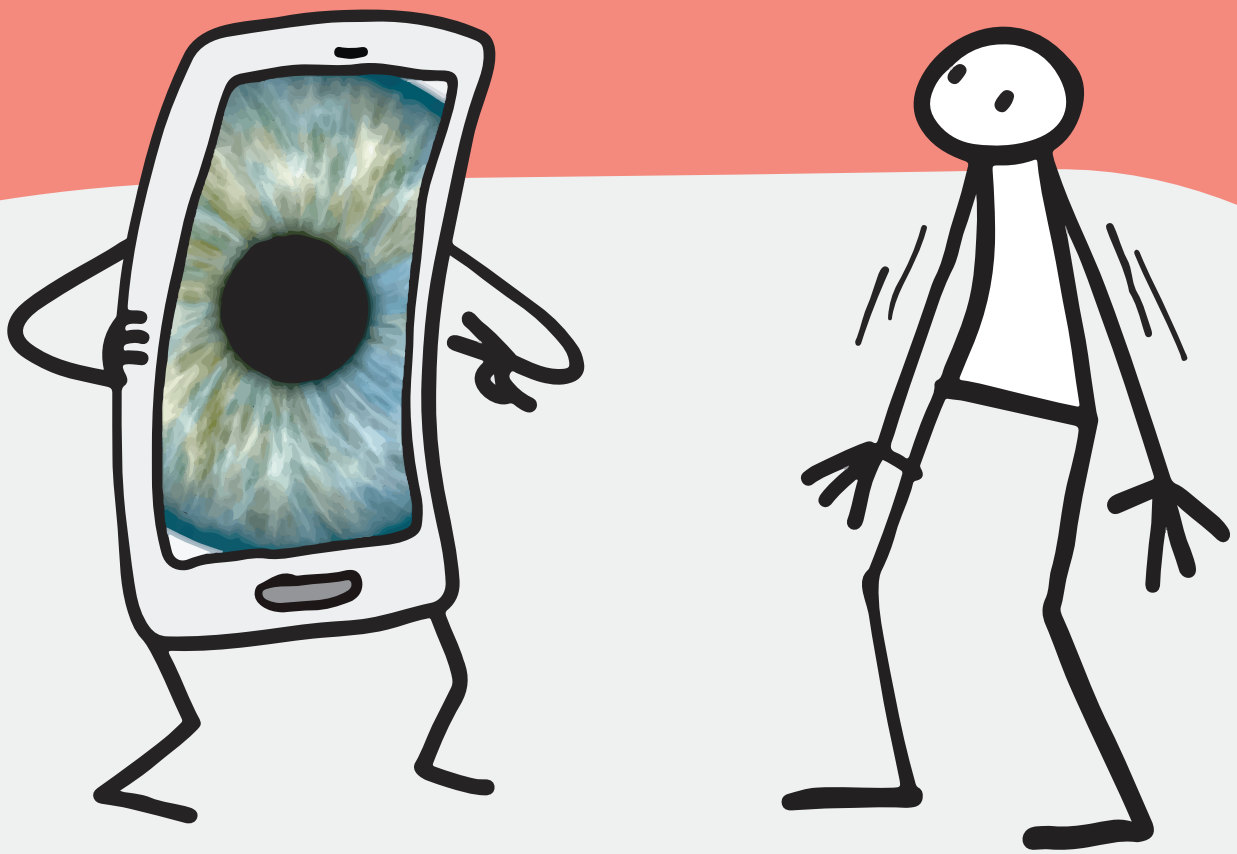
**Privilégiez une connexion internet fixe (fibre, ADSL) dès que possible : elle est moins consommatrice d'électricité que les réseaux mobile (4G ou 5G).**

**Chez vous, basculez votre téléphone en WiFi dès que vous le pouvez et privilégiez la connexion avec un câble ethernet pour vos appareils (ordinateur, console de jeux, TV connectée…).**

**Pensez également à éteindre votre box internet lorsque vous ne l'utilisez plus : 95 % de sa consommation électrique ne dépend pas du trafic internet qu'elle offre (source État internet en France, édition 2024 par l'Arcep).**

# RISQUES

## À QUELS RISQUES S'EXPOSE-T-ON SUR INTERNET ET LES RÉSEAUX SOCIAUX ?



## DES INFORMATIONS « INEFFAÇABLES » ?

**Les réseaux sociaux comme Facebook s'accordent une licence d'utilisation sur les informations et contenus que vous partagez sur chaque plateforme.** Par une simple capture d'écran ou des partages successifs, vos publications peuvent se retrouver sur des sites que l'on n'imaginait pas. Faites attention à ce que vous publiez et à qui pourra y accéder. Pensez aussi que l'on change tout au long de sa vie et qu'un futur employeur pourrait avoir accès à vos erreurs de jeunesse. Afin de protéger les utilisateurs, un droit à l'oubli numérique a été prévu par le RGPD.

## REPRISE ET DIVULGATION DE CONTENUS PRIVÉS

**Il peut sembler amusant, pour animer son réseau, de se mettre en scène ou de diffuser des contenus privés…** Gardez à l'esprit qu'il n'y a aucune garantie de confidentialité. Tout contenu peut être copié-collé, repris par d'autres internautes et rediffusé. Une photo de groupe, prise lors d'une soirée par exemple, peut être taguée par des amis et permettre de vous identifier et ainsi prendre des proportions inimaginées.

## MANIPULATIONS COMMERCIALES OU IDÉOLOGIQUES

**Les réseaux sociaux sont utilisés massivement par des marques, des associations, des personnalités influentes ou des acteurs politiques,** pour mener des campagnes, recruter des fans ou des adhérents, faire de la publicité cachée. Depuis 2023, la « Loi influenceurs » oblige les créateurs de contenu à indiquer si leur contenu est rémunéré ou s'ils ont reçu des cadeaux.

## CONTENUS CHOQUANTS

**De nombreux comptes, notamment sur Twitter, Facebook, TikTok… peuvent receler des images pornographiques (photos, vidéos).** Ces contenus donnent une image erronée, et souvent truquée, des rapports humains et des relations amoureuses. D'autres contenus, très violents, incitant à la haine et des campagnes de désinformation (fake news) sont accessibles facilement sur ces sites. Ayez toujours à l'esprit qu'il n'y a pas d'autorité régulatrice officielle des contenus. C'est à chacun (internautes, associations, institutions…) qu'il revient d'être vigilant et de dénoncer ces pratiques (voir nos pages informatiques pratiques) et de promouvoir des contenus positifs plutôt que ceux toxiques.

## PIRATAGE

**Un post viral sur les réseaux, ou un message par e-mail, peuvent proposer de suivre un lien corrompu.** Celui-ci mène à télécharger des applications non sécurisées ou répondre à des campagnes de phishing (hameçonnage) pour soutirer des informations de connexion, etc. Par inattention, on s'expose à des risques de piratage, d'installation de virus ou de logiciels malveillants… Ces risques sont d'autant plus élevés qu'il peut être très difficile de faire la différence entre une publicité, un lien de piratage et un contenu légitime.

## HARCÈLEMENT

**Votre présence sur internet et en particulier sur un réseau social peut amener à subir des remarques désobligeantes** ou plus grave, de véritables campagnes de dénigrement et de commentaires humiliants. Pour certains, cela peut faire l'effet d'un défouloir ou exprimer un sentiment de toute-puissance, mais hélas, pour les victimes cela peut faire très mal !
Le cyberharcèlement est aussi grave que le harcèlement classique, c'est un délit passible jusqu'à dix ans de prison. Il a pour particularité que les auteurs se cachent parfois derrière l'anonymat et qu'il ne s'arrête pas une fois la victime chez elle.

## PRATIQUES À CARACTÈRE SEXUEL

**Il existe sur les réseaux des personnes mal intentionnées qui se font passer pour des « séducteurs inconnus »** et essaient de gagner votre confiance, des faux découvreurs de talents qui vous demandent de poser en bikini, voire d'aller plus loin. Il ne faut jamais communiquer de photos ou de données privées vous concernant à des personnes que vous ne connaissez pas dans la vie réelle. Elles risqueraient de s'en servir pour faire pression, ou pire. De même, n'acceptez pas non plus de rendez-vous de la part de ces personnes.

## DÉSINFORMATION/ENDOCTRINEMENT

Selon une étude Ipsos de 2022, 94 % des 16-30 ans utilisent au moins un réseau social ou média en ligne pour s'informer sur l'actualité. On peut y trouver beaucoup plus de contenus, sur beaucoup de sujets mais la qualité des informations y est très variable.

Sur de nombreux sites, médias en ligne, blogs et réseaux sociaux, l'information n'est validée que par l'auteur du propos, contrairement aux pratiques des rédactions des médias professionnels (aussi présents sur Internet), qui sont tenus de vérifier l'information et leurs sources.

On parle beaucoup de désinformation (ou de « fake news » pour fausse information), de légendes urbaines ou de vidéos trafiquées. Grâce à leur contenu sensationnaliste, ils peuvent faire le tour du monde ; à l'inverse de leurs potentiels démentis ou « débunkage » qui, le plus souvent, ne bénéficient pas de la même diffusion.

De telles fausses informations peuvent porter une volonté politique ou encore religieuse. Certaines organisations ont développé une véritable expertise dans ce domaine et ont intérêt à faire croire à la réalité de faits ou d'événements pour manipuler l'opinion et orienter nos convictions avec des théories du complot. Développer un esprit critique est ici essentiel. Vous ne prendriez pas pour une vérité ce que vous dit un inconnu dans la rue : ayez la même attitude sur le net.

Devant toute info qui vous semble étonnante ou marquante : recoupez avec des sources d'information officielles (site de grand média, gouvernement). Dans tous les cas, prenez du recul avant de partager une information et faites toujours appel à votre esprit critique en la lisant.

## DÉSINTÉRÊT POUR LA VIE RÉELLE ET CAPTATION D'ATTENTION

**Internet semble tout offrir au point de susciter un certain désintérêt pour la vraie vie et les échanges non numérisés,** qui peuvent paraître plus fades, face à tout ce qui est affiché et accessible en ligne. D'autant plus que la plupart des applis comme Tik Tok sont conçues pour retenir l'attention de l'internaute le plus longtemps possible. Attention à ne pas se perdre et à équilibrer ses temps d'activités : sports, lectures, sorties, découvertes, jeux, culture, bénévolat et échanges réels avec ses proches et ses amis ! Sans compter que l'abus d'écrans a un effet direct sur la concentration, la santé (sommeil, vision) et un réel pouvoir hypnotique. À tel point, que certains pédiatres proscrivent même toute exposition avant l'âge de 6 ans.

# LE CAS TIKTOK ET SON ALGORITHME

Le réseau de partage de vidéos, extrêmement utilisé par les plus jeunes, comporte plusieurs risques en raison de la conception de son algorithme. Celui-ci est basé sur des recommandations dont le but intrinsèque est de conserver l'attention des utilisateurs et utilisatrices le plus longtemps possible, ce qui peut entraîner rapidement une addiction.

Plus grave, Amnesty International a révélé fin 2023 que « *le système de recommandation de TikTok et les pratiques intrusives de collecte de données qui l'accompagnent représentent un danger pour les jeunes utilisateurs et utilisatrices de la plateforme en amplifiant le contenu sur la dépression et le suicide qui risque d'aggraver des problèmes de santé mentale existants.* »

# POUR UN INTERNET ÉCORESPONSABLE

**Sur votre smartphone, désinstallez régulièrement les applis que vous n'utilisez plus (les mises à jour consomment des données).**

**Désactivez les notifications qui ne vous servent pas.**

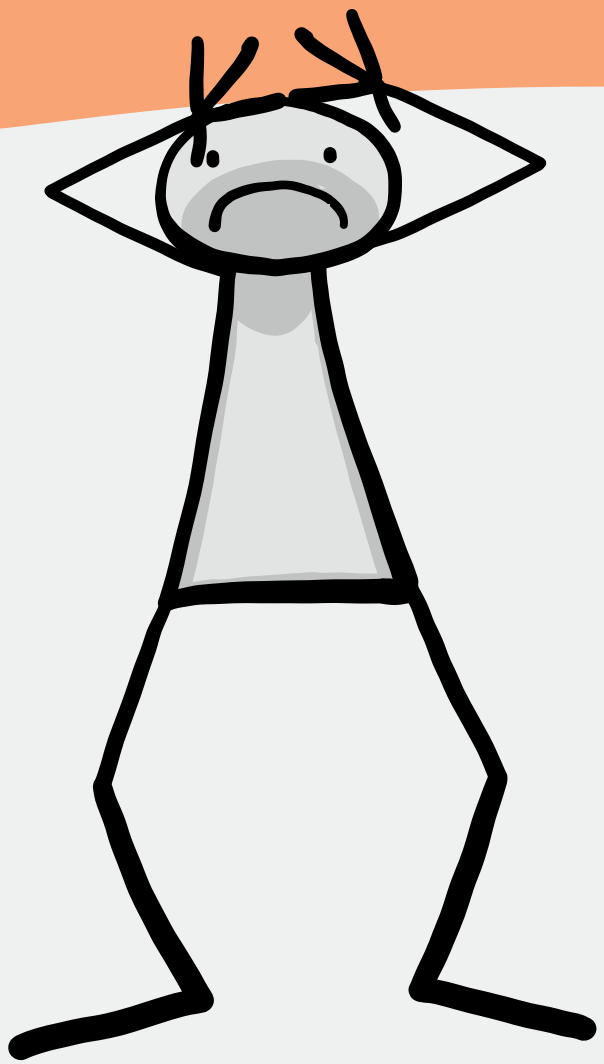
**Pour écouter de la musique, privilégiez le streaming audio à la vidéo, qui est le type de contenu le plus gourmand en ressources numériques.**

**Supprimer vos photos et vidéos après chaque utilisation afin de désencombrer le stockage à la fois sur votre smartphone et les serveurs Cloud.**

**Enfin, pensez que les réseaux sociaux sont conçus pour capter au maximum votre attention, alors soyez plus forts qu'eux et ne les utilisez qu'à bon escient.**

# INTELLIGENCE ARTIFICIELLE

## FAUT-IL EN AVOIR PEUR ?



# INTELLIGENCE ARTIFICIELLE (IA)

**Quand on vous parle d'IA, vous pensez à des machines futuristes qui vont dominer les humains, à des vidéos et photos de mieux en mieux truquées, à des emplois supprimés ? Pourtant l'intelligence artificielle est plus présente dans votre quotidien numérique que vous ne l'imaginez : par exemple en retouchant automatiquement les photos de votre smartphone, en suivant en temps réel l'itinéraire le plus rapide quand vous roulez…**

## QU'EST-CE (VRAIMENT) QUE L'INTELLIGENCE ARTIFICIELLE ?

L'IA est une technologie qui regroupe un ensemble d'outils. Ce terme désigne tout outil utilisé par une machine afin de « *reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité* », selon la définition adoptée par le Parlement Européen. Plus largement, l'intelligence artificielle recouvre les capacités de simulation des processus d'intelligence humaine par des systèmes informatiques : apprentissage, calcul, prise de décision…

Attention, l'IA ne se résume pas à l'IA générative, plus récente, dont l'exemple le plus connu est ChatGPT, qui peut écrire des textes, ou les IA utilisés pour créer des photos et des vidéos.

## L'INTELLIGENCE ARTIFICIELLE NE DATE PAS D'HIER

Les travaux sur l'automatisation des machines, au siècle dernier, en constituaient les prémisses. Ce qui a changé dans la dernière décennie est, d'une part, la capacité de calcul des ordinateurs et l'explosion du nombre de données à exploiter, et d'autre part, un accès plus facile et large à ces nouvelles technologies. Ces paramètres ont permis d'augmenter énormément les possibilités de l'intelligence artificielle.

## L'IA EST DÉJÀ PARTOUT AUTOUR DE VOUS

Dans le domaine de la santé, elle aide à faire des diagnostics assistés par ordinateur, une meilleure analyse de l'imagerie médicale que celle d'un être humain. Dans les transports avec le développement des véhicules autonomes ou des applis d'itinéraires, dans l'industrie avec les robots et dans de nombreuses applis de votre smartphone.

## NI INTELLIGENTE, NI ARTIFICIELLE

Derrière une IA, il y a toujours des humains. En effet, tout outil d'IA repose sur des algorithmes définis par des humains. Elle ne peut rien apprendre d'elle-même sans les données fournies, elles aussi, par des humains.

## UNE IA PEUT-ELLE FAIRE DES ERREURS ?

Oui ! Justement parce que derrière l'IA, il y a des humains qui ne sont pas infaillibles. Des biais, parfois inconscients, lors de la programmation des algorithmes peuvent avoir pour conséquence des erreurs. Un exemple concret : la plupart des algorithmes sont créés par des hommes. En conséquence, si vous demandez à une IA de générer une photo avec un conseil de direction, elle risque fort de ne comporter… que des hommes.

## COMMENT BIEN COHABITER AVEC L'INTELLIGENCE ARTIFICIELLE ?

Toute technologie peut devenir un danger si elle est entre de mauvaises mains – comme le simple exemple d'une voiture conduite par un chauffard. De même, l'IA peut servir à des desseins dangereux (comme la désinformation sur les réseaux sociaux, par exemple).

C'est pourquoi il est crucial de veiller à ce que l'humain puisse garder la main et avoir des informations transparentes sur l'utilisation de l'IA. La CNIL a développé cet objectif dans un rapport sur les enjeux éthiques de l'intelligence artificielle où les questions d'autonomie et de prise de décision automatisée sont abordées. Certains recrutements professionnels intègrent ainsi des choix faits par l'IA. Mais dans ce cas, le RGPD prévoit que toute personne a le droit de

s'opposer à certains traitements automatisés lorsque ceux-ci n'intègrent pas une intervention humaine dans le processus de décision.

De même, il devient très important de demander plus de transparence quand une vidéo ou une image a été générée par une IA, et de développer au maximum l'esprit critique des internautes face à ce qu'ils visionnent. Ce qui passe par l'éducation au numérique dès le plus jeune âge.

L'Union européenne a adopté le règlement européen sur l'intelligence artificielle (IA) en juin 2024 pour aider à son développement sans porter atteinte aux droits fondamentaux.

## COMMENT RECONNAÎTRE UN TEXTE, UNE PHOTO, GÉNÉRÉE PAR UNE IA ?

Il n'existe pas de méthode simple et 100 % fiable pour reconnaître un texte ou une photo générés par une IA. Néanmoins, certains réflexes, outils et votre esprit critique devraient vous permettre de vous ôter le doute. Certaines plateformes invitent aussi les auteurs à déclarer que leur production vient d'une IA.

**Repérez les bizarreries dans la rédaction**
L'usage répété de mots de transition (comme « en outre », « par conséquent »...) peut indiquer qu'une IA a généré le texte, car elle en utilise souvent trop pour relier des phrases courtes et hachées. De même pour la présence de mots incongrus, de mots qui sont en dehors du contexte, trop complexes, et la répétition exagérée de mots clés.

**Utilisez certains outils en ligne**
Il existe des outils en ligne dans lesquels vous pouvez copier-coller votre texte afin de vérifier s'il a été généré par une IA. On peut citer CopyLeaks ou Originality.

**Photos : traquez les détails !**
Les images générées par les IA peuvent être bluffantes de réalisme. Néanmoins, l'IA « rate » souvent quelques détails (nombre de doigts sur une main, par exemple) qui sont un indice de la provenance de l'image.

**Vérifiez les sources et les citations**
Vous pouvez par exemple copier-coller une citation dans un moteur de recherche afin de vérifier qu'elle a bien le même auteur que celui indiqué dans le texte.

**Faites preuve d'esprit critique**
Même si des outils de vérification en ligne apparaissent, l'IA va évoluer et perfectionner ses textes et images avec le temps. Le meilleur moyen de vérifier une information en ligne reste... votre esprit critique : prenez le temps de recouper une information, par exemple en la cherchant sur des sites officiels (comme ceux du gouvernement) ou des médias traditionnels (agence de presse et journaux).

## POUR UN INTERNET (ET UNE INTELLIGENCE ARTIFICIELLE) ÉCORESPONSABLE

**Une recherche sur un moteur en ligne consomme jusqu'à 10 fois moins qu'une requête ChatGPT (source Les e-novateurs, fév. 2023).**

**Évidemment l'IA est attrayante pour résumer un texte, générer du contenu ou des images.**

**Mais réfléchissez-y fortement avant de l'utiliser car son coût environnemental est tel que le nombre de serveurs va devoir doubler d'ici à 2030. Sans parler de la consommation d'eau nécessaire pour les refroidir.**

# CONSEILS

## POUR DEVENIR LE GARDIEN DE SON INTERNET

**À votre niveau individuel, vous pouvez mettre en place des solutions responsables pour vous et votre famille :**

**Vérifiez que les paramètres de protection de la vie privée sont activés et correctement configurés** sur toutes les plateformes utilisées.

**Limitez la navigation et les échanges dans un périmètre adapté à votre âge ou celui de vos enfants et à vos besoins.** Pour cela des outils en ligne, tels que la plate-forme Seriously www.seriously.ong peuvent vous aider.

**Discutez régulièrement en famille, avec des adultes référents ou des aînés :**
Quels sites aimez-vous consulter ?
Avec qui « tchattez » vous ?
Qu'est-ce que vous avez découvert de nouveau ?
Faites bien comprendre la différence entre de vrais amis (de la "vie réelle" ) et de simples connaissances numériques.

**Gardez en tête l'importance de la protection de vos données personnelles et de celles de vos amis !**
Parlez-en dans votre réseau.

**Ne faites pas ce que vous n'aimeriez pas qu'on vous fasse** et tout acte qui risque de blesser quelqu'un, évitez les actes blessants : du plus anodin, « taguer » un ami sans son accord sur une pho-to peu valorisante, au plus grave : diffuser des propos méchants ou s'associer à des actes de « social bashing ».

**Réfléchissez avant de publier tout contenu :**
À quoi cela va-t-il servir ?
Quelles peuvent être les conséquences ?
Et veillez au respect de l'image d'autrui : mieux vaut faire rire par son humour qu'aux dépens des autres.

**Dès qu'un contenu est dérangeant ou dès le premier signe de dénigrement sur les réseaux, n'hésitez pas à alerter votre entourage ou le site concerné.** Les utilisateurs d'Internet doivent être solidaires !

**Renseignez-vous et préférez des éditeurs d'applications ou de contenus respectueux des règlements et lois euro-péens :** ils sont soumis à des réglementations strictes.

# CONSEILS

**Vous avez un doute sur l'utilisation de vos données personnelles ?** Ne restez pas seul avec vos questions. La CNIL est là pour vous aider, n'hésitez pas à la saisir ou demander conseil.

**Attention lorsque vous utilisez des réseaux wifi publics,** évitez à tout prix d'utiliser des sites Web non sécurisés sur ces réseaux et faites particulièrement attention aux éventuelles alertes de sécurité de votre navigateur.

**Gare aux applis gratuites.** Si certaines sont tout à fait légitimes, d'autres peuvent exploiter vos données ou infecter votre téléphone. Préférez payer un peu pour une application ou un contenu de qualité. Là encore : renseignez-vous !

**Si l'on vous propose de gagner de l'argent sans rien faire, c'est très probablement une arnaque.** Sur Internet, pas plus que dans le monde réel, rien n'est magique.

**Apprenez à reconnaître le phishing par SMS.** Certains arnaqueurs vous en envoient en se faisant passer pour des marques de confiance (La Poste, l'Assurance maladie, des services de livraison comme UPS) et vous demandent de vous connecter à un site internet qui ressemble énormément à un site officiel. Quelques indices pour les reconnaître : un numéro de téléphone que vous ne connaissez pas, un texte qui contient un sentiment d'urgence à vous connecter, des fautes d'orthographe... En cas de doute, il n'y a pas de doute, ne vous connectez pas et recontactez l'émetteur par son site ou son numéro de téléphone officiel. Dans tous les cas, prenez votre temps.

**Attention avant de signer les conditions générales d'utilisation (CGU) des sites,** sinon gare aux déconvenues ! Une grande majorité des Français ne les lisent pas avant de les signer. D'autant qu'elles sont souvent longues de plusieurs pages, et que leurs tournures de phrases complexes les rendent inaccessibles sans connaissance du droit, selon l'Internet Society France. Or, des clauses abusives peuvent s'y trouver !

**Vérifiez toujours une information en la recoupant sur d'autres sources :** médias reconnus, agences de presse comme l'Agence France Presse ou directement à la source ! Si une information n'apparaît nulle part ou si la source est suspecte, elle a des chances d'être fausse. D'autres indices comme une offre magique pour gagner de l'argent facilement ou pour acheter un produit à un prix très bas cachent souvent une arnaque.

**Si vous êtes victime ou témoin de harcèlement en ligne,** avertissez le plus rapidement un adulte, parent, professeurs ou autres proches référents, voire un des organismes cités plus bas. Il faut oser parler, même si cela paraît difficile en crainte de représailles.

**Contrôlez de temps en temps votre e-réputation :** tapez votre nom entre guillemets dans un moteur de recherche. Ainsi, vous saurez tout ce que l'on peut trouver sur vous et pourrez éventuellement essayer de le supprimer ou de le limiter.

# CONSEILS COTÉ TECHNIQUE

**Installez un antivirus fiable.**

**Utilisez un filtre sur votre navigateur et votre moteur de recherche** (préférences de navigation, contrôle parental, etc.) de votre choix (il en existe de nombreux, adaptés à chaque site ou type de navigation).

**Prenez le temps de lire et régler les paramètres de confidentialité sur les applications et les réseaux sociaux.**

**Vérifiez la sécurité des sites Web sur lesquels vous communiquez vos données.** Un petit cadenas en haut à gauche, un lien qui commence par « HTTPS » signifient que la page est sécurisée et l'adresse du site qui est bien l'adresse officielle. Si elle ne l'est pas, ne communiquez surtout pas d'informations personnelles.

**Ne donnez pas d'informations trop sensibles sans vous assurer de l'identité du destinataire.** Votre banque ne vous demandera par exemple jamais vos codes d'accès par mail ou sms. Prudence !

# INFORMATIONS PRATIQUES

## SITES INTERNET

cnil.fr

education.gouv.fr/non-au-harcelement

educnum.fr

e-enfance.org

internetsanscrainte.fr

isoc.fr

laquadrature.net/fr

savoirdevenir.net

seriously.ong

## QUE FAIRE EN CAS DE CYBERHARCÈLEMENT ?

**3018**

**Non au harcèlement**

Numéro vert opéré par l'Association e-Enfance (appel gratuit).
Également disponible sur application mobile,
par tchat/messenger, et par e-mail :
e-enfance.org/besoin-daide/

## COMMENT ADRESSER UNE PLAINTE CONCERNANT VOS DONNÉES PERSONNELLES ?

Sur le site internet de la CNIL www.cnil.fr

Par courrier postal en écrivant à la CNIL
3 place de Fontenoy TSA 80715 – 75334 PARIS CEDEX 07

# DEVENIR GARDIEN DE SON INTERNET

**REPRENDRE LA MAIN SUR SES DONNÉES PERSONNELLES**
**APPRÉHENDER L'INTELLIGENCE ARTIFICIELLE**

YACINE AIT-KACI
CAROLINE BOUDET
LUCIEN CASTEX
NICOLAS CHAGNY
CORINNE PULICANI

Internet offre un immense espace de ressources et une multiplicité de contenus consultables, pour la plupart, gratuitement. C'est un grand pas vers un libre accès aux savoirs, ainsi qu'à des services numériques, des réseaux sociaux, des sites d'informations, des jeux et applications à la mode... Mais attention !

## "SI C'EST GRATUIT, C'EST TOI LE PRODUIT !"

Aujourd'hui, il est urgent de familiariser tous les usagers de services numériques, aux enjeux de la protection des données personnelles et de la vie privée. Il faut, notamment, renforcer le niveau de vigilance des publics fragilisés, des jeunes, de leurs familles, des enseignants et de tous ceux qui interviennent en milieu scolaire ou associatif.

Ce livre est là pour vous aider à mieux **maîtriser votre degré d'exposition et à savoir agir efficacement en cas de problème sur Internet.** Soyons tous des cybercitoyens actifs, attentifs et responsables. Œuvrons collectivement à la construction d'un Internet plus sûr, plus juste et plus transparent.

**isoc.fr/education**

Internet Society France Chapter

Internet Society Foundation