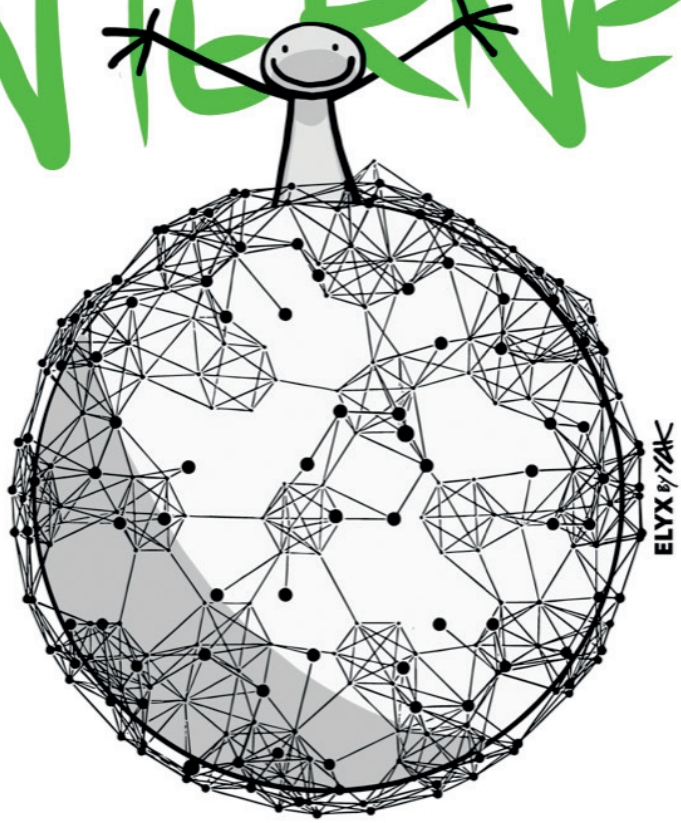
CORINNE PULICANI | NICOLAS CHAGNY | LUCIEN CASTEX | YACINE AÏT-KACI

DEVENIR GARDIEN DE SON INTERNET



COMMENT REPRENDRE LA MAIN SUR SA VIE ET SES DROITS NUMÉRIQUES

À destination des jeunes utilisatrices et utilisateurs d'Internet, de leurs familles, des enseignants, des éducateurs, des associations... et de tout cybercitoyen responsable, qui souhaitent œuvrer à la construction d'un Internet plus sûr, plus juste et plus transparent pour tous.

NEXTDAY! INNOVATION, CREATION & PROSPECTIVE

Internet Society France Chapter

FONDATION ELYX

Avec les soutiens

EDUCNUM.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

france•tv

afnic

LIVRE BLANC : DEVENIR GARDIEN DE SON INTERNET !

Comment reprendre la main sur sa vie et ses droits numériques

www.isoc.fr/education

Edité en format numérique par l'INTERNET SOCIETY FRANCE.
18, rue Geoffroy l'Asnier – c/o WF3 – F-75004 Paris
courriel : education@isoc.fr

Date de parution : Octobre 2018

Auteurs

Corinne Pulicani
Présidente du Think Tank NEXTDAY! & Vice-Présidente de l'Internet Society France, en charge de la culture.

Nicolas Chagny
Président de l'Internet Society France.

Lucien Castex
Enseignant, chercheur et Secrétaire Général de l'Internet Society France.

Yacine Aït Kaci
Créateur du personnage ELYX, premier ambassadeur virtuel des Nations Unies depuis 2015 et Vice-Président de la Fondation ELYX.

Illustrations et maquette : Yacine Aït Kaci, créateur du personnage Elyx
Iconographie et mise en page : Florian Aumont, graphiste

Remerciements

Les auteurs tiennent à remercier les nombreuses personnes ayant contribué à ce livre blanc par leurs conseils, apports et commentaires : Carina Chatain (CNIL / Collectif EDUCNUM) Sylvain Steer (CECIL), Adeline Pilon (Directrice Générale de la Fondation ELYX), Alexa Gutowski, Florence Casenove (Présidente de Zoom2024), Claire Mélanie Popineau, Jean-Pierre Gaussen, ainsi que les membres du collectif EDUCNUM et les experts de la CNIL pour leurs précieuses contributions.

À propos des auteurs

L'INTERNET SOCIETY FRANCE est le chapitre français de l'Internet Society, ONG internationale présente dans plus de 100 pays. Créée en 1996, l'Internet Society France a pour mission la protection des utilisateurs d'Internet et leur représentation au sein de instances de la Gouvernance de l'Internet. L'Internet Society France oeuvre pour un Internet Ouvert, un Internet "Pour Tous" et un Internet "Avec Tous".

NEXTDAY! est un Think Tank, conçu comme un laboratoire de cross innovation. Il explore et questionne les nouveaux usages et territoires d'expérimentations en lien avec l'innovation technologique à impact positif, "Tech for Good", ainsi que les nouvelles pratiques culturelles, économiques, éducatives et sociétales qui en découlent.
next-day.org

La FONDATION ELYX est une Fondation abritée par la Fondation FACE reconnue d'utilité publique. Ratifiée depuis juin 2018, la Fondation a pour vocation d'accompagner toutes organisations désirant s'inscrire dans l'Agenda 2030 des Nations-Unies. La Culture est au coeur de chaque action de la Fondation en tant qu'elle éveille les consciences tout en s'adressant à la sensibilité de tous.
foundation.elyx.net

SOMMAIRE

INTRODUCTION
Les nouvelles lois sur la protection des données personnelles et de la vie privée.

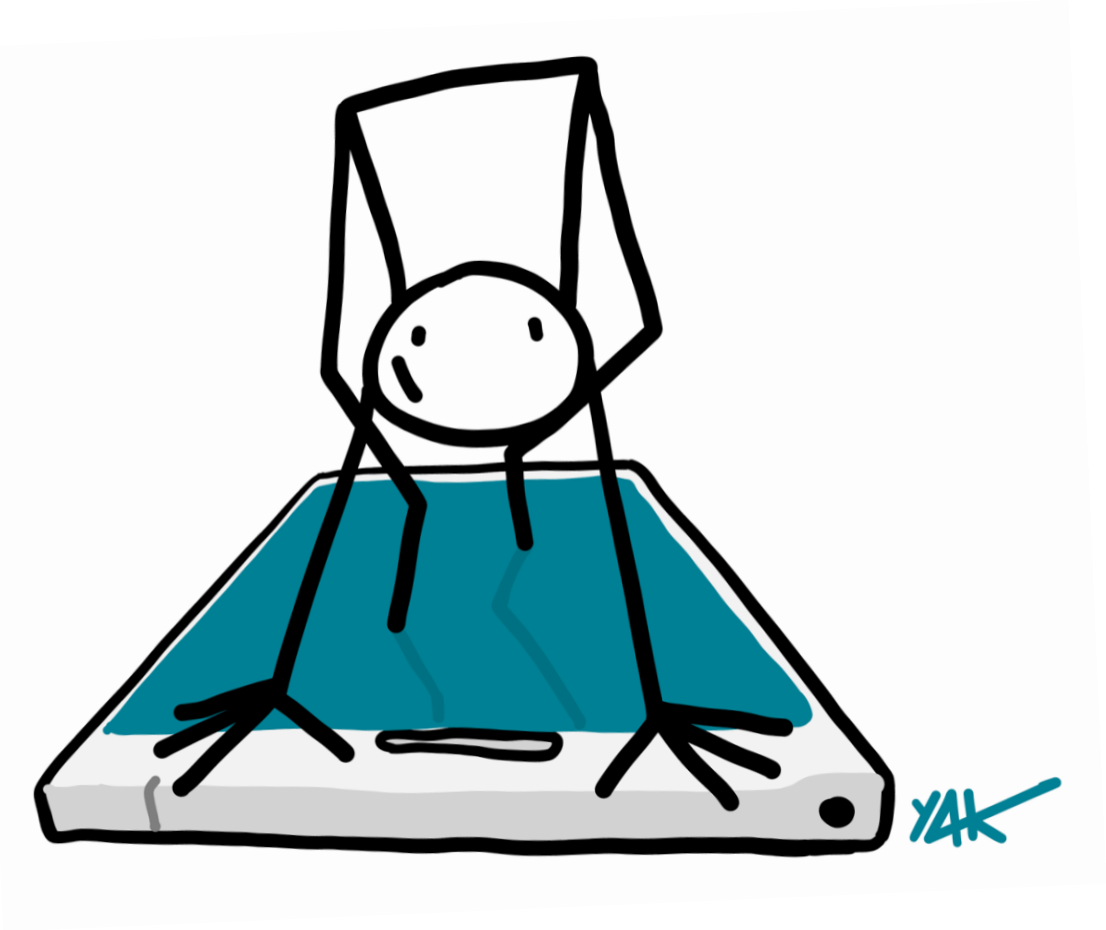
I INTERNET
Un espace de ressources formidable : Mais pas que...

II LES DONNÉES
Définition et conditions d'exploitations.

III LES RISQUES
À quels risques s'exposent les utilisateurs d'internet ?

IV CONSEILS POUR DEVENIR LE GARDIEN DE TON INTERNET
Quelques conseils pour devenir le gardien de ton internet.

V NUMÉROS ET INFORMATIONS UTILES



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

LES NOUVELLES LOIS SUR LA PROTECTION DES DONNÉES PERSONNELLES ET DE LA VIE PRIVÉE.

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. Depuis plus de 10 ans, leur utilisation massive, souvent à l'insu des personnes, pose un vrai problème de société.

Les données personnelles, ce sont toutes les informations qui permettent d'identifier une personne, directement (nom, prénom, photo, vidéo...) ou indirectement (numéro de sécurité sociale, lieu et date de naissance, identifiant national élève, géolocalisation, numéro de téléphone, adresse électronique...).

Ces données ne sont pas si éphémères qu'on le pense. Leur traitement peut permettre un traçage et un profilage ou fichage des individus, à but de commerce ou de contrôle, correspondant à la mise en place d'une surveillance électronique.

Il est difficile d'imaginer le nombre de données échangées chaque jour : c'est considérable !

Le Règlement Général sur la Protection des Données (RGPD), qui a pour but de mettre fin à cette opacité en matière de traitements des données personnelles, s'applique dans les 28 États de l'Union européenne depuis le 25 mai 2018. En France, cette nouvelle règlementation européenne a nécessité la mise à jour de la "loi informatique et liberté" de 1978.

SOYONS TOUS DES CYBERCITOYENS ACTIFS, ATTENTIFS ET RESPONSABLES.

Dans la suite logique du RGPD, un autre règlement est en cours d'adoption, appelé "e-PRIVACY". Ce projet de règlement, discuté au Conseil et au Parlement européen, concerne le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques. Il vise à renforcer encore davantage le RGPD pour **restaurer la confiance des personnes envers les canaux de communication numérique.**

Aujourd'hui, il est urgent de familiariser tous les usagers de services numériques, à ces enjeux, en créant un socle commun de connaissances éthiques, juridiques et techniques. 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.

Il s'agit pour chacun de mieux maitriser son 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 !

SI TOUT EST GRATUIT, C'EST TOI LE PRODUIT !

UN ESPACE DE RESSOURCES FORMIDABLES, MAIS PAS QUE...

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 !**

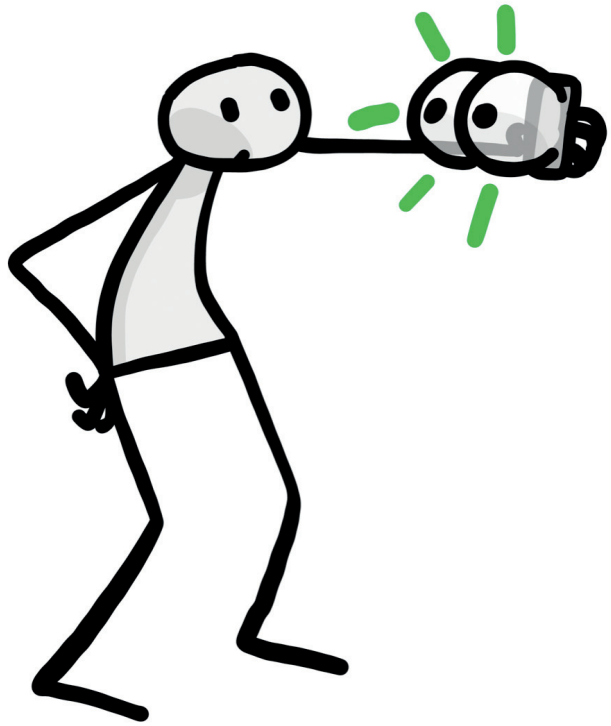
En effet, si on ne paye pas pour accéder à de nombreux contenus, services, réseaux, jeux, musiques, vidéos et applications en ligne, c'est que certains fournisseurs de ces services exploitent nos données ou, par la publicité, nos temps de cerveau disponibles. Indirectement, ils nous font également travailler gratuitement pour leurs intérêts propres. Par exemple, ils nous font reconnaitre des objets dans des "captchas" (série de lettres, d'images ou de chiffres souvent distordus ou barrés que certains sites mettent en place pour vérifier que l'utilisateur n'est pas un robot), ils nous incitent à devenir leurs ambassadeurs en "likant" des contenus et en laissant des commentaires etc.

Même si ce n'est pas le cas pour tous les sites web, par exemple les sites de services publics ou d'autres, comme Wikipédia, l'exploitation à des fins publicitaires des données est la contrepartie la plus courante pour une mise à disposition et une utilisation en apparence gratuite des contenus et services proposés.

Naviguer sur Internet, visiter différentes pages Web, laisser un commentaire, etc. 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 "recherchées" sont donc celles concernant les habitudes et les possibilités de consommation, comme celles sur la santé, les liens familiaux et amicaux, les études suivies, les trajets réguliers ou les hobbys, par exemple.

Elles sont encore plus convoitées si elles concernent les Jeunes, cibles privilégiées des publicitaires.



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

QU'EST-CE QU'UNE DONNÉE ?

Les données numériques sont une représentation exploitable des informations par les ordinateurs.

Avant d'être portées sur un ordinateur les informations sont "codées" par un développeur informatique, qui les transforme en données. L'ordinateur pourra ensuite les traiter facilement et automatiquement, les stocker, les transmettre à un autre ordinateur, rechercher une information parmi une grande quantité de données, les mettre en relation, etc.

C'est donc bien plus qu'un simple ensemble de "0 et de 1", c'est un ensemble d'indications que nous transmettons lors de nos pratiques et échanges numériques : textes, échanges vocaux, photos, 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, etc.

Dans notre vie quotidienne, nous créons et échangeons sans cesse des données sans nous en apercevoir. Pour pouvoir les traiter et les exploiter, les développeurs informatiques conçoivent aussi des méthodes pour résoudre des problèmes, fournir des résultats exploitables et ajuster, ainsi, finement les contenus et services numériques. On appelle cela des algorithmes. Le résultat de certains algorithmes permet, par exemple, de repérer des répétitions et d'identifier des "modèles de comportements". **Automatiquement, 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, dans le cas d'un moteur de recherche, il pourra afficher, simultanément aux informations demandées, de la publicité et les contenus les plus rentables issus de sites internet qui ont payé pour apparaître en début de liste dans les résultats de la requête. **Il est ainsi possible d'identifier statistiquement que le lecteur de tel livre a des chances de s'intéresser à tel autre livre ou produit en recoupant les informations d'un grand nombre d'utilisateurs.**

Pour un autre exemple, il est possible de choisir la ville où se dérouleront certains concerts en fonction de la localisation et du nombre de "like" obtenus en par des groupes de musique qui diffusent "en ligne" leurs morceaux.

Ainsi, plus on utilise les mêmes sites ou applications qui nous profilent, plus ces derniers peuvent collecter de données sur nous. Cela devient 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 recouper des données et de suivre une très grande partie de nos navigations et de nos activités en ligne.

LA TRANSPARENCE EST IMPORTANTE

il est bon de savoir qui possède qui. Par exemple Facebook possède Instagram, ainsi que Whatsapp et OculusVR ; Google possède YouTube, et propose de nombreux 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 !

Le traitement des données peut être légal et non intrusif. Il existe des outils qui sont au service des internautes. Malheureusement beaucoup de ces outils sont créés ou détournés à des fins de traçage. Ainsi, mieux les connaitre permet de comprendre et d'appréhender les risques issus de nos pratiques les plus anodines.

LES COOKIES

Ce sont de petits fichiers déposés sur le disque dur de notre ordinateur par le site visité pour permettre de reconnaitre 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. **L'internaute est alors espionné insidieusement par des entreprises dont il ignore la présence sur le site.**

LA GÉOLOCALISATION

Elle permet de savoir à quels endroits nous nous rendons ou d'où nous envoyons nos informations et d'en déduire nos trajets réguliers, nos hobbys, notre activité, nos habitudes de consommation comme nos petits soucis personnels. 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 en anglais), est un numéro d'identification lié à un appareil connecté au réseau. **Ce numéro d'identité permet d'identifier la machine sur le réseau et de lui permettre de communiquer avec d'autres appareils ou sites internet. 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. 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 EN UTILISANT SES COMPTES PERSONNELS

Si elle facilite l'inscription, la fonction, permettant de s'inscrire sur un site à l'aide d'un compte, possédé sur un autre site (par exemple avec son compte Facebook), constitue un vrai danger pour vos données personnelles. En effet, en liant ces deux comptes vous donnez 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. Avec cet envoi, **d'autres informations sont générées pour être comprises par les ordinateurs qui vont s'occuper de la transmission du message : 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…

Ces plateformes ne sont pas anodines pour un enfant. En raison de leurs contenus, ce sont avant tout des réseaux sociaux pour adultes ou pour jeunes aguerris. Il faut savoir évaluer l'information et être en mesure de développer un esprit critique.

LES MESSAGERIES INSTANTANÉES

Elles permettent de communiquer facilement avec ses proches et contacts, 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 à Facebook, lui donne accès à tous vos numéros de téléphones et aux métadonnées de vos échanges ... C'est pourquoi, au moment de choisir un service, pensez à vérifier ses paramètres et son mode de fonctionnement : posez-vous la question de qui peut avoir accès à vos données et vérifier que vous voyez bien le petit cadenas indiquant que le site est protégé. Certains services sont plus respectueux que d'autres !

LES APPLICATIONS MOBILES

La plus grande partie du temps passé sur mobile est consacrée à des applications : réseaux sociaux, messageries, divertissement et jeux. C'est d'autant plus vrai, à partir du collège où l'on possède souvent son premier smartphone, utilisé seul pour ses activités numériques favorites. Si la plupart des applications remplissent leurs fonctions, 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 forcément pouvoir vous géolocaliser ou accéder à vos contacts ? **Soyez vigilants et renseignez-vous sur ces applications !**

C'est le temps moyen passé sur les réseaux sociaux en 2017. Cette moyenne augmente d'année en année. Sur le podium des sites plébiscités : Snapchat, Instagram et Facebook. Effet de groupe, envie d'être à la mode, pratiques familiales, etc. conduisent **des enfants de 8, 9 ou 10 ans à avoir déjà des comptes, ou à surfer régulièrement sur ces plateformes en se faisant tracer et en s'y accoutumant**.

En France, l'âge requis pour exprimer seul son consentement à un service numérique est de 15 ans (en dehors de cadres strictement réservés à des missions de services publics, par exemple).

Une étude de Génération Numérique, parue en 2017, constate ainsi que **62 % des jeunes de 12 ans** (soit l'âge de l'entrée en classe de 5e) et **45,7 % des jeunes de 11 ans** (entrée en classe de 6e) **possèdent au moins un compte sur un réseau social**.

LES OBJETS CONNECTÉS ET LEURS APPLICATIONS ASSOCIÉES

Montres géolocalisées, applications de santé, aide aux devoirs, appareils de domotique, jeux et consoles vidéos apportent des fonctionnalités, certes, mais recueillent aussi une multitude d'informations, en particulier sur vos pratiques.

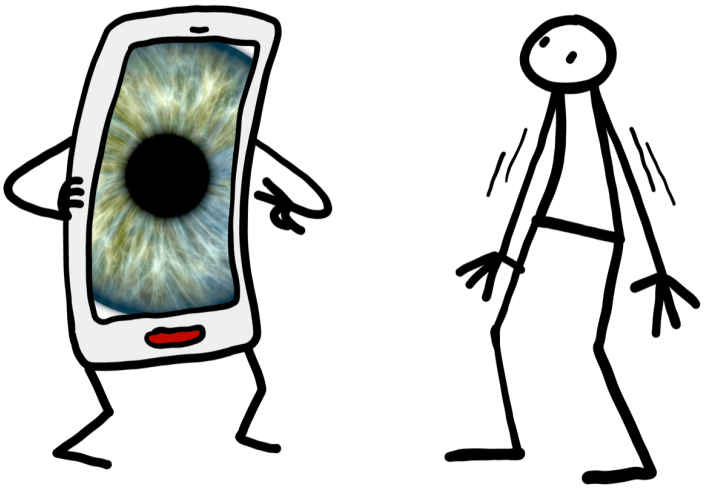
Un audit mené en mai 2016 par 25 autorités de protection des données dans le monde, rassemblées au sein du Global Privacy Enforcement Network (GPEN - réseau d'organismes agissant au sein de l'OCDE pour la protection de la vie privée), révèle que 68 % des 300 objets connectés analysés ne donnent aucune information sur les conditions de stockage et de sécurité des données. Plus grave, 59 % ne fournissent pas une information claire et complète sur la collecte et les conditions d'exploitation des données personnelles des utilisateurs. Le consentement éclairé des utilisateurs doit pourtant être central.

RÉSEAUX WIFI PUBLICS, UN DANGER ?

De nombreux réseaux Wifi, gratuitement accessibles, le sont en échange de la collecte de données de navigation. De plus certaines de ces connexions n'offrent pas des garanties suffisantes en termes de sécurité. Un pirate informatique peut ainsi récupérer des données, parfois très sensibles (mot de passes, données bancaires…), en se faisant simplement passer pour le Wifi gratuit d'un restaurant ou d'un quartier.

LES RÉSEAUX SOCIAUX ET SITES COMMUNAUTAIRES

Les réseaux sociaux offrent de nombreux avantages : ils permettent d'échanger avec ses amis et sa famille éloignés géographiquement, de dialoguer, de faire ses devoirs, de s'informer, de jouer en ligne ou de partager des informations autour de ses activités et pratiques favorites. **Attention toutefois, les risques de déconvenues y sont également démultipliés. L'illusion d'anonymat, la résonnance d'Internet, la grande confusion entre les comptes professionnels et les comptes privés, sont autant de "facteurs à risques".**



PERMANENCE DES INFORMATIONS DANS LE TEMPS

Les réseaux sociaux comme Facebook s'accordent une licence d'utilisation sur les informations et contenus que vous partagez sur chaque plateforme. De plus, vos publications peuvent se retrouver, parfois, par une simple capture d'écran ou des partages successifs, avec une portée ou sur des sites que l'on n'imaginait pas. Pensez toujours à faire 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 renforcé par le Règlement Général sur la Protection des Données (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 : postures peu valorisantes, mots dits dans un état d'énervement, sans réfléchir ou pour blaguer ; images échangées dans le cadre d'une discussion personnelle comme avec un·e amoureux·se... **Il faut avoir en permanence 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. Les contenus que l'on trouve couramment publiés ne sont pas destinés aux plus jeunes.

À QUELS RISQUES S'EXPOSENT LES UTILISATEURS D'INTERNET ?

! CONTENUS CHOQUANTS

De nombreux comptes notamment sur Twitter, Facebook ou encore Tumblr peuvent diffuser des images ou des propos violents, pornographiques avec des contenus essentiellement visuels (photos, vidéos). Ces contenus donnent une image erronée, et souvent truquée, de de la société ou encore des rapports humains. Des contenus très violents, incitant à la haine et des campagnes de désinformation sont fréquemment diffusées sur les réseaux sociaux. Ayez toujours à l'esprit qu'il n'y a pas d'autorité globale de régulation des contenus. **C'est à tout le monde (internautes, associations, institutions…) qu'il revient d'être vigilant et de dénoncer ces pratiques et de promouvoir des contenus positifs.**

PIRATAGE

Souvent sur les réseaux sociaux un message viral propose de suivre un lien corrompu, de télécharger des applications non sécurisées ou de répondre à des campagnes de hameçonnage (phishing en anglais) pour soutirer des informations, etc. Par inattention, on s'expose à des risques de piratage ou d'installation de logiciels malveillants… **Ces risques sont d'autant plus élevés que, sur certaines plateformes, il est très difficile de différencier 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, la parodie, les moqueries ou, plus grave, de véritables campagnes de dénigrement et de commentaires humiliants. Cela peut se manifester par la création de groupes de dénigrement, qui parfois tournent au drame pour la victime.

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 ! **Il faut être conscient que le cyberharcèlement est aussi grave que le harcèlement classique**. Il a pour particularité que les auteur·es ne sont pas nécessairement identifiables et qu'il ne s'arrête pas une fois la victime chez elle.

LE CAS "YOUTUBE"

Le cas de YouTube, véritable "chaine de télévision" gratuite, est intéressant. Tout comme leurs ainés, les jeunes, et parfois les très jeunes, font l'objet d'un ciblage publicitaire et d'une captation des données. La consommation de contenus produits par les YouTubeurs stars du moment, véritables influenceurs en matière de consommation, parfois rémunérés ou encouragés par des marques, pose question. Même des parents s'y mettent et exposent leur famille. La particularité de YouTube est qu'il est souvent très difficile de détecter une vidéo à vocation commerciale, d'un contenu sponsorisé ou d'une vidéo réellement personnelle, tant l'engagement des YouTubeurs par des marques est complexe (nombre de fans, originalité du contenu, capacité à se mettre en scène...). Pour ces services rendus, certains perçoivent des gratifications diverses, outre le fait d'être suivis par des milliers de fans !

Cette popularité virtuelle peut être très chronophage conduisant parfois à des conduites à risques pour entretenir ou augmenter son audience : propos déplacés voire haineux, postures ridicules ou dangereuses, longues veillées nocturnes, décrochage scolaire... Il faut veiller à une bonne répartition de ses activités.

DÉSINFORMATION / ENDOCTRINEMENT

Internet prend une place croissante dans l'accès à l'information face aux médias centralisés tels que la télévision ou la presse papier. **On peut y trouver beaucoup plus de contenus, sur beaucoup de sujets mais la qualité des informations y est très variable**, même si certains sites annoncent veiller à une certaine éthique de leurs contenus. **Sur de nombreux sites, médias en ligne, blogs et réseaux sociaux, l'information n'est validée que par l'auteur des propos, contrairement aux pratiques des médias professionnels (aussi présents sur Internet), qui sont tenus de respecter une déontologie du journaliste et ainsi de vérifier la validité d'une information et la fiabilité de leurs sources**. On parle beaucoup de désinformation ou "d'infox" (fausse information, ou encore Fake News en anglais), de légendes urbaines ou de vidéos truquées. Leur caractère sensationnel peut leur faire 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, doctrinale 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'évènements afin de manipuler l'opinion et d'orienter nos convictions. Développer un esprit critique est ici essentiel, tout comme de vérifier les informations qui nous semblent étonnantes ou marquantes, en les recoupant avec d'autres sources d'information de confiance ou officielles. **Si l'information ne s'y trouve pas ... méfiance ! Une réelle politique d'éducation au numérique et à l'information doit être pensée et intégrée aux programmes.**

À QUELS RISQUES S'EXPOSENT LES UTILISATEURS D'INTERNET ?

PRATIQUES À CARACTÈRE SEXUEL

Il existe des "séducteurs inconnus" qui essaient de gagner votre confiance en jouant l'ami compréhensif, en partageant vos centres d'intérêt et en vous faisant des compliments. Vous pouvez aussi vous exposer à des faux découvreurs de talents, qui disent être à la recherche de nouveaux visages pour des agences de mannequins qui vous demandent de poser en bikini, voire d'aller plus loin. Ces personnes qui vous abordent sont mal intentionnées. **Il ne faut jamais communiquer de photos ou de données privées vous concernant à des inconnus**, elles risqueraient de s'en servir pour faire pression, ou pire. Cela peut sembler évident, mais n'acceptez pas non plus de rendez-vous de la part de ces personnes !

DÉSINTÉRÊT POUR LA VIE RÉELLE

Ce phénomène est très bien décrit par le magazine Wired dans son article "Why Teens Aren't Partying Anymore" (pourquoi les jeunes ne font plus la fête). **Internet semble tout offrir au point de susciter un certain désintérêt pour la "vraie" vie et les échanges non numérisés, qui peuvent paraitre plus fades, face à tout ce qui est affiché et accessible en ligne.** 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 et un réel pouvoir hypnotique. À tel point, que les pédiatres proscrivent même toute exposition avant l'âge de 6 ans.

CONSEILS

RECOMMANDATIONS GÉNÉRALES POUR UN COMPORTEMENT RESPONSABLE

- 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 et à vos besoins. Qwant Junior, par exemple, (qwantjunior.com) est un moteur de recherche idéal pour les moins de 12 ans.

- Discutez régulièrement en famille, avec des adultes référents ou des ainés : Quels sites aimez-vous consulter ? Avec qui "tchattez" vous ? Qu'est-ce que vous avez découvert de nouveau ? Comprenez bien la différence entre de vrais amis 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.

- Soyez solidaire de vos amis et évitez les actes blessants : du plus anodin, "taguer" un ami sur une photo peu valorisante, au plus grave : diffuser des propos méchants ou s'associer à des actes de "social bashing" : ne faites pas ce que vous n'aimeriez pas qu'on vous fasse et tout acte qui risque de blesser quelqu'un.

- Réfléchissez avant de publier tout contenu 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, n'hésitez pas à alerter votre entourage ou le site concerné. Les utilisateurs d'Internet doivent être solidaires !

- Préférez des éditeurs européens d'applications ou de contenus : ils sont soumis à des règlementations plus strictes, même si maintenant la nouvelle loi sur la protection des données va contraindre les grands groupes étrangers à plus de transparence.

QUELQUES CONSEILS POUR DEVENIR LE GARDIEN DE SON INTERNET.

- En cas de doute sur l'utilisation de vos données personnelles, ne pas hésiter à saisir et à demander conseil à la CNIL ou à des associations spécialisés pour dénoncer les abus. Des initiatives comme ebastille.org ou la Quadrature du Net peuvent être particulièrement utiles.

- Attention aux applications 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 !

- Limitez au maximum les informations que vous transmettez en ligne à ce qui est strictement nécessaire et idéalement aux seuls services et sites de confiance.

- Renseignez-vous sur conditions générales d'utilisation (CGU) des sites, sinon gare aux déconvenues ! Selon un sondage Opinion Way réalisé en mai 2018 pour l'Internet Society France, 7 français sur 10 ne lisent pas ou rarement les CGU ; sur le pourcentage de ceux qui les lisent, 48% des sondés comprennent "plutôt mal" le texte des Conditions Générales d'Utilisation, et 9% "très mal" ! De part leur volume (à titre d'exemple, les CGU de Facebook, Twitter et Google font respectivement, 9, 8 et 7 pages), leurs termes juridiques et leurs tournures de phrases complexes, elles sont non-accessibles pour un internaute sans connaissance du droit explique l'Internet Society. Cela révèle un réel manque de transparence de la part les sites et plateformes, puisque les internautes s'engagent au moment de les consulter en ligne sans maîtriser les enjeux de cet engagement, ce qui peuvent avoir des conséquences fâcheuses. à titre d'exemple, un article publié en juillet 2018 par la CNIL, évoquait les résultats éloquents d'une expérience menée par deux universitaires américains. 543 étudiants devaient tester un nouveau réseau social. Résultat : 74 % n'ont pas lu une seule ligne des CGU et les 26 % restants y ont consacré en moyenne 73 secondes. Or, l'une des clauses obligeait le signataire à donner son premier enfant à l'éditeur ou à en concevoir un d'ici à 2050, toujours pour le donner !

- Vérifiez toujours l'information en la recoupant sur d'autres sources : medias reconnus, agences de presse comme l'Agence France Presse ou directement à la source. Recoupez l'information ! Si une information n'apparait nulle part ou si la source est "suspecte", elle a des chances d'être fausse.

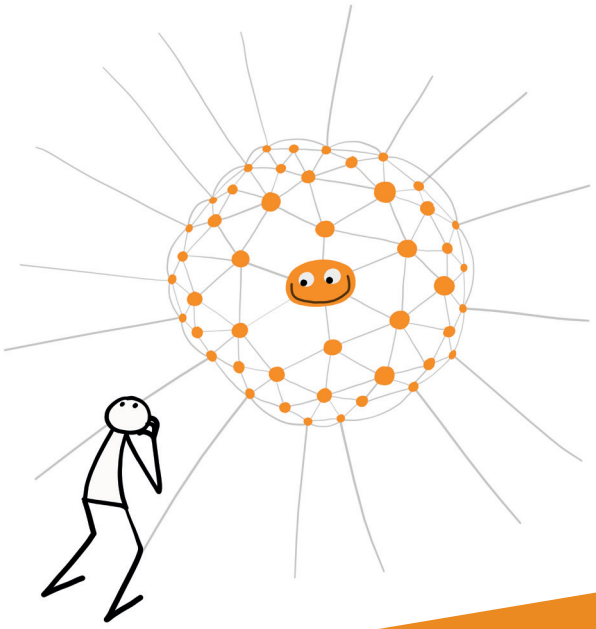
- Si vous êtes victime de harcèlement, ou bien, si vous voyez d'autres personnes s'en prendre à quelqu'un, avertissez le plus rapidement un adulte, parents, professeurs ou autres proches référents, voire un des organismes cités plus bas. Souvent les victimes d'humiliations n'osent pas en parler, par crainte, par honte ou bien parce qu'elles sont manipulées.

- **Apprenez à être un activiste positif du net : Internet est une vraie communauté d'échanges. Beaucoup d'internautes sont solidaires et bienveillants, à vous d'adopter aussi ce comportement ouvert et positif pour en tirer le meilleur parti.**

  Dénoncez les mauvaises pratiques, saisissez vos amis et appelez-les à la rescousse dès que vous vous sentez attaqué, ne restez jamais seul face à un problème rencontré sur le net ! **La communauté est là pour vous aider, de même que de nombreux organismes. Désamorcez immédiatement tous discours haineux. Pour cela des outils en ligne, tels que la plateforme Seriously (https://www.seriously.ong/) peuvent vous aider.**

EN FAMILLE ET AVEC VOS PROCHES

- **Échangez autour de vos activités numériques. Vous entamerez facilement une discussion positive sur le sujet.**
- **Arrivez ensemble à des points d'accord. Écoutez les arguments formulés par vos parents ou vos ainés et arrivez à un compromis.**
- **Contrôlez de temps en temps votre e-réputation : tapez votre nom entre guillemets. Ainsi, vous saurez tout ce que l'on peut trouver sur vous et pourrez éventuellement essayer de le supprimer ou de le limiter.**
- **Conservez les adresses utiles mentionnées à la fin de ce livre blanc et n'hésitez pas à les faire circuler autour de vous.**



QUELQUES SOLUTIONS TECHNIQUES SIMPLES POUR UN "SURF" PLUS TRANQUILLE.

- **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).**

- **Optimisez 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 et un lien qui commence par "HTTPS" signifient que la page est sécurisée. 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. Le hameçonnage (ou phishing) est une pratique où un pirate se fait passer pour une entreprise, une administration ou un proche pour demander des mots de passe ou encore des numéros de compte.**

- **Effacez régulièrement votre historique de navigation et vos cookies pour éviter que quiconque n'accède à votre historique ou s'en serve pour vous tracer en ligne.**

- **Paramétrez vos appareils pour que la géolocalisation ne soit pas activée par défaut et pensez à la désactiver quand elle n'est pas nécessaire.**

- **Limitez les traçeurs dans vos navigations Web grâce à des modules comme uBlock Origin (qui bloquera aussi les publicités), Privacy Badger, Ghostery, ou d'autres outils de blocage.** 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.

- **Faites 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.**

- **Pour simplifier la lecture des CGU, recourez à des outils tels que POLISIS, ou TOSDR.org, ainsi qu'à des services décryptant le contenu des CGU. Pour plus d'informations, consultez également le programme de simplification des CGU de l'Internet Society France, accessible sur le site: confiance.isoc.fr**

LES SITES INTERNET EN FRANCE

- afnic.fr
- asso-generationnumerique.org
- bibliosansfrontieres.org
- cnil.fr
- clemi.fr
- ebastille.org
- education.francetv.fr
- educnum.fr
- e-enfance.org
- internetsanscrainte.fr
- isoc.fr
- laquadrature.net/fr
- lececil.org
- nonauharcelement.education.gouv.fr/ressources/guides/plan-de-prevention-mis-en-place-a-lechelle-nationale
- qwantjunior.com
- savoirdevenir.net
- seriously.ong

COMMENT ADRESSER UNE PLAINTE OU UNE RÉCLAMATION ?

Sur le site internet de la CNIL (www.cnil.fr)
Dans certains cas déterminés, par le téléservice de plainte en ligne.
Dans les autres cas non prévus par le téléservice, le service ‘‘Besoin d’aide’’.

Par courrier postal en écrivant à la CNIL
CNIL, 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Sur le site de ebastille (www.ebastille.org)
Dépôt de ‘‘e-doléances’’ dans le but de mener des actions de recours collectifs.

Sur le site de La Quadrature du net (www.laquadrature.net/fr)

NUMÉROS ET INFORMATIONS UTILES POUR ALLER PLUS LOIN.

LES NUMÉROS À APPELER

3020

"Non au harcèlement", numéro vert mis en place par l'éducation nationale.

0800 200 000

"Net Écoute" de l'association e-enfance, est le numéro vert national spécialisé dans les problématiques que rencontrent les enfants et les ados dans leurs pratiques numériques. Il est gratuit et confidentiel.

SÉLECTION DE CONTENUS PÉDAGOGIQUES

- **"Bienvenue dans ton monde avec Elyx"** de **Yacine Aït Kaci**.
- **"Éduquer au numérique"** par **Animafac** : www.animafac.net
- **"Guide de survie des aventuriers d'Internet"** par **Le CECIL** : www.lececil.org
- **"Programme "Permis Internet"** par **Axa prévention** : www.permisinternet.fr
- **"Guide de la Famille Tout Écran"** par **le CLEMI** : www.clemi.fr
- **"Guide Comment accompagner et protéger votre enfant"** par **la Fédération française des télécoms** : www.fftelecoms.org
- **"Guide de l'Internet sans embrouilles"** par **Génération numérique** : asso-generationnumerique.fr
- **"Éducation aux Écrans : parcours citoyen en 4 étapes"** par les CEMEA : www.cemea.asso.fr
- **"Éducation aux réseaux sociaux"** par **Les petits débrouillards** (sur Youtube)
- **"Modules pédagogiques numériques"** par **l'institut National de la Consommation** : www.inc-conso.fr
- **Le documentaire "Nothing to hide"** : vimeo.com/nothingtohide
- **france.tveducation : "Les clés des médias", "La collab' de l'info", "1 jour 1 question", "3 minutes pour coder", "Data Sciences vs Fake", "Decod'actu", "#dans la toile "** : education.francetv.fr
- **"Thomas contre les GAFA"** Petits spots accessibles à tous (SPICEE sur Youtube)
- **Le programme de simplification des CGU** (Conditions Générales d'Utilisation) de **l'Internet Society France** : confiance.isoc.fr
- **Outil de vérification de vidéos** : invid-project.eu

DEVENIR GARDIEN DE SON INTERNET !

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, en créant un socle commun de connaissances éthiques, juridiques et techniques. 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.

Il s'agit pour chacun de mieux maitriser son degré d'exposition et de savoir agir efficacement en cas de problème. Soyons tous des cybercitoyens actifs, attentifs et responsables. Oeuvrons collectivement à la construction d'un Internet plus sûr, plus juste et plus transparent.

AUTEURS

Corinne Pulicani, Nicolas Chagny, Lucien Castex, Yacine Aït Kaci

www.isoc.fr/education

ELYX by YAK

NEXTDAY! INNOVATION, CREATION & PROSPECTIVE

Internet Society France Chapter

FONDATION ELYX

Avec les soutiens

EDUCNUM. CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

france•tv

afnic