



MANUEL DE MAÎTRISE DE L'INTERNET

” Accompagner les
utilisateurs dans
le monde en ligne



Construire une Europe
pour et avec les enfants
www.coe.int/children



MANUEL DE MAÎTRISE DE L'INTERNET

Accompagner
les utilisateurs
dans le monde en ligne

Conseil de l'Europe

Édition anglaise :

Internet Literacy Handbook

Les opinions exprimées dans cet ouvrage sont celles des auteurs et ne reflètent pas nécessairement la politique officielle du Conseil de l'Europe.

Tous droits réservés. Aucun extrait de cette publication ne peut être traduit, reproduit, enregistré ou transmis, sous quelque forme et par quelque moyen que ce soit, électronique (CD-ROM, Internet, etc.), mécanique, photocopie, enregistrement ou de toute autre manière, sans l'autorisation préalable écrite de la Direction de la Communication (F-67075 Strasbourg Cedex ou publishing@coe.int).

Couverture, mise en page et conception graphique : Iddifix

Éditions du Conseil de l'Europe
F-67075 Strasbourg Cedex
<http://book.coe.int>

Auteurs : Janice Richardson, Elizabeth Milovidov et Martin Schmalzried

© Conseil de l'Europe, décembre 2017
Imprimé dans les ateliers du Conseil de l'Europe

Sommaire

AVANT-PROPOS	7
INTRODUCTION	9
1. INTERNET – EN TOUT TEMPS ET EN TOUT LIEU	
Fiche d'information 1 – Se connecter	13
Fiche d'information 2 – Présence en ligne et « nuage »	19
Fiche d'information 3 – Web 2.0, Web 3.0 et plus	25
Fiche d'information 4 – Blogs et vidéoblogs	31
Fiche d'information 5 – Internet en mobilité	37
2. INTERNET – MISE EN RELATION DES PERSONNES ET DES IDÉES	
Fiche d'information 6 – Courrier électronique et communication	45
Fiche d'information 7 – Salons de discussion (dialogue en ligne ou <i>chat</i>) et messagerie instantanée	51
Fiche d'information 8 – Réseaux sociaux et partage social	57
Fiche d'information 9 – Protection de la vie privée et paramètres de confidentialité	63
3. INTERNET – PARTICIPATION À LA SOCIÉTÉ DU SAVOIR	
Fiche d'information 10 – Recherche d'informations	73
Fiche d'information 11 – Trouver des informations de qualité sur le web	79
Fiche d'information 12 – Apprentissage à distance et formations en ligne ouvertes à tous (MOOC)	85
Fiche d'information 13 – Achats en ligne	91
4. INTERNET – POUR TOUS	
Fiche d'information 14 – Vidéos, musique et images sur Internet	97
Fiche d'information 15 – Créativité	103
Fiche d'information 16 – Jeux	107
Fiche d'information 17 – Citoyenneté numérique	111
Fiche d'information 18 – La parentalité à l'ère du numérique : une approche positive et proactive	119
5. INTERNET – RÉPONDRE AUX DÉFIS ACTUELS	
Fiche d'information 19 – Cybercriminalité : spam, logiciels malveillants, fraude et sécurité	127
Fiche d'information 20 – Classification/étiquetage et filtrage	133
Fiche d'information 21 – Harcèlement en ligne : intimidation, traque et trolling	139
Fiche d'information 22 – Obtenir de l'aide	145
6. INTERNET – ET DEMAIN ?	
Fiche d'information 23 – Internet des objets	151
Fiche d'information 24 – Intelligence artificielle, automatisation et bouleversements technologiques	157
Fiche d'information 25 – Réalité virtuelle et réalité augmentée	163
Fiche d'information 26 – Êtes-vous le produit ? Big data, exploration de données et respect de la vie privée	169

Remerciements

Janice Richardson est consultante dans le domaine des droits de l'enfant en ligne depuis plusieurs dizaines d'années et a dirigé l'équipe de rédaction du présent manuel. Coordinatrice jusqu'en 2014 du réseau Insafe de la Commission européenne, qui regroupe une trentaine de pays, et plus récemment du réseau de lutte contre le harcèlement ENABLE, elle est également membre du Comité consultatif de Facebook sur la sécurité.

Dr. Elizabeth Milovidov, J.D. est consultante en sécurité électronique et jouit d'une expérience de plus de vingt ans en tant qu'avocate, professeur de droit et défenseuse des droits des enfants. Son but est de doter les parents et les enfants des compétences dont ils ont besoin sur toutes les questions liées à Internet, aux technologies et aux réseaux sociaux. Elle a également fondé DigitalParentingCoach.com.

Martin Schmalzried est responsable des politiques pour la Confédération des organisations familiales de l'Union européenne (COFACE) et spécialiste en nouvelles technologies et en sécurisation d'Internet. Il préside le projet SIP BENCH III (analyse comparative des outils de contrôle parental) et participe à plusieurs projets et initiatives de l'UE dans ce domaine.

Avant-propos

■ S'il ne fallait qu'un seul mot pour qualifier l'importance de maîtriser Internet aujourd'hui, ce serait « majeure ». Avec bientôt 3,5 milliards d'utilisateurs, dont près de 20 % en Europe, Internet constitue une source intarissable d'informations à découvrir et à partager. Mais la complexité du monde en ligne est telle qu'il n'est pas toujours facile d'y naviguer en sécurité. C'est pourquoi il faut en connaître les bases.

■ Le présent manuel présente dans un langage simple et accessible toutes les informations dont l'Internaute aura besoin. Il ne s'agit pas d'une toute nouvelle publication, mais d'un ensemble de conseils pratiques se voulant évolutif sur la manière d'appréhender un flux de données toujours plus important. La version en ligne du manuel a été conçue avec le même souci de clarté, de manière à ce que ses différents chapitres puissent être présentés à des groupes en classe ou dans des centres socioculturels, notamment au moyen des graphismes attrayants. Il peut ainsi être utilisé comme outil de formation pour tous les âges.

■ Dans cette tentative de débrouiller les complexités du réseau, le manuel aborde également les questions éthiques et les risques liés au partage d'informations : si nous voulons utiliser Internet pour combler notre soif de connaissance et partager nos réflexions et nos opinions, nous devons le faire de manière responsable. Les principes relatifs aux droits de l'homme sont valables en ligne comme dans la vie réelle. Cela implique, par exemple, de respecter la liberté d'expression et la vie privée d'autrui en ligne tout en veillant à ce que les nôtres soient respectées. Comment assurer la sécurité de nos données à caractère personnel dans l'environnement numérique ? Comment réagir face à du contenu illicite ou lorsque l'on est la cible de manœuvres d'intimidation ou de propos haineux ? Les réponses à ces questions et bien d'autres sont présentées ici sous la forme de recommandations et d'astuces destinées à un public réceptif, lequel est invité à faire preuve d'esprit critique à l'égard de ce qu'il voit et lit en ligne et à faire des choix sûrs et éclairés.

■ Notre présence en ligne pour partager des idées nous permet également d'apprendre et de comprendre beaucoup de choses ; les échanges peuvent remettre en question des opinions toutes faites ou nous amener à créer des réseaux pour susciter des changements positifs. Ce constat est particulièrement évident chez les jeunes générations auxquelles Internet offre des possibilités illimitées d'explorer, d'apprendre, de se socialiser et de créer, qui contribuent directement à leur développement personnel. Le monde en ligne est leur principal espace de liberté et leur première source d'information, et ils peuvent y exercer leurs droits et libertés. Les pièges pourront être évités en adoptant des mesures de précaution et en proposant un accompagnement adapté. Pour ne pas décourager les utilisateurs (en particulier les plus jeunes), Internet ne doit pas être présenté comme un univers sombre, truffé d'écriteaux « attention, danger ! » L'objectif de favoriser un usage éclairé, créatif, efficace et confiant d'Internet grâce à un tel accompagnement est justement ce qui fait l'utilité et l'originalité du présent manuel. Si, grâce à lui, les enfants peuvent profiter de la multitude de possibilités qu'offre Internet, tout en renforçant leur capacité de résilience dans l'environnement numérique, conscients de leurs propres capacités et responsabilités, il aura atteint son but.

■ Le Conseil de l'Europe est heureux d'avoir suivi le manuel dans son évolution et remercie les nombreuses personnes qui ont participé au fil des ans à son lancement puis à sa révision. Cette source d'informations de qualité, toujours plus riche, permettra aux enfants, aux parents, aux enseignants et aux responsables politiques des 47 États membres de tirer le meilleur parti d'Internet et de préparer les générations futures à l'utiliser avec confiance et en toute sécurité



Snežana Samardžić-Marković
Directrice générale de la démocratie



Christos Giakoumopoulos
Directeur général des droits de l'homme
et de l'État de droit

Introduction

” La littératie est un pont entre la misère et l’espoir. C’est un rempart contre la pauvreté et un fondement du développement, [...] un cadre pour la démocratisation et un moyen de promotion de l’identité nationale et culturelle [...] C’est, enfin, la voie vers le progrès humain et le moyen par lequel tout homme, femme ou enfant peut s’épanouir et donner le meilleur de lui-même.

Kofi Annan, ancien Secrétaire Général des Nations Unies, janvier 1997-décembre 2006

Le présent manuel est la deuxième édition du *Manuel de maîtrise d’Internet* initialement publié en 2003. La première édition a été révisée deux fois à trois ans d’intervalle, en 2006 et 2009, afin de suivre le rythme soutenu de l’évolution du secteur des technologies en ligne. Bien que cette édition propose une structure similaire, son contenu a été entièrement actualisé et de nouvelles fiches ont été ajoutées, pour aborder également les technologies de demain.

■ Le manuel est destiné à un public très large et s’adresse aussi bien aux familles qu’aux enseignants et aux décideurs politiques. Il fournit par ailleurs des liens vers des informations et ressources plus complètes pour ceux qui souhaitent approfondir tel ou tel sujet. Il vise également à instruire les adolescents et jeunes adultes qui font partie des plus fervents utilisateurs de technologies et sont des créateurs de tendances.

■ Avant tout, le *Manuel de maîtrise de l’Internet* entend donner des informations et inviter à la réflexion sur quelques-unes des questions éthiques, sociologiques et culturelles complexes indissociables des activités liées au numérique et aux médias qui prennent aujourd’hui une place si importante dans la vie de tant de personnes à travers le monde. Le Conseil de l’Europe, qui publie ce manuel, œuvre depuis 1949 à la promotion, à la protection et au développement des droits de l’homme, de la démocratie et de l’État de droit dans ses 47 États membres.

■ La technologie s’étant rapidement immiscée dans la plupart des domaines de la vie de la plupart des gens ces cinquante dernières années, elle a également eu des répercussions sur les droits de l’homme, les devoirs et les libertés, tout en élargissant considérablement la notion de littératie, qui en est un élément essentiel. Le fait fait partie de la vaste palette d’instruments du Conseil de l’Europe visant à répondre aux nombreux défis et à saisir les nombreuses opportunités liées à Internet. On trouvera dans les fiches des références à certains de ces instruments.

■ La littératie implique de maîtriser les outils de communication modernes pour s’exprimer, mais aussi pour comprendre ; longtemps, elle s’est résumée à trois mots : lire, écrire et calculer. Aujourd’hui, du fait de la puissance des outils et plateformes numériques que nous utilisons comme moyens d’expression, mais aussi de la vitesse et de l’instantanéité de la propagation des informations, elle a acquis d’autres dimensions avec lesquelles plus d’un continue de se débattre. Les photos, vidéos, messages à nombre de caractères limités, émoticônes et podcasts sont devenus des langages à part entière grâce à des outils comme Instagram, Snapchat, Vine et PériScope. Bien souvent, l’interaction et la communication réelle sont réduites à une simple opération électronique où l’on ne voit plus l’autre. Les jeunes sont particulièrement touchés par ce phénomène : ils s’envoient des textos, twittent, jouent à des jeux électroniques et échangent des images nuit et jour dans le monde en ligne qui s’imbrique et se confond de plus en plus avec ce que les adultes appellent encore aujourd’hui le « monde réel ».

■ Les conventions sociales et culturelles sont bousculées lorsque les utilisateurs de médias sociaux ajoutent ou ôtent à leurs listes « d'amis » des personnes qui se trouvent à l'autre bout du monde et qu'elles ne rencontreront probablement jamais. De plus en plus de relations s'établissent en ligne car c'est là que se rencontrent les partenaires commerciaux et qu'ils créent des sociétés ; de la même manière, Internet devient de plus en plus souvent le premier lieu où l'on rencontre son partenaire de vie. Ces profonds changements font du sens des responsabilités un élément central de la littératie, puisqu'il nous faut acquérir une solide compréhension de nos propres droits fondamentaux et respecter ceux des autres si nous voulons éviter les écueils et contribuer positivement à la société actuelle.

■ Le *Manuel de maîtrise de l'Internet* se présente comme un recueil de fiches d'information au format similaire à la première édition, à la différence près que les fiches ont été regroupées en six chapitres thématiques pour permettre aux utilisateurs de les télécharger et de les imprimer plus facilement, chapitre par chapitre ou individuellement. On trouvera au début de chaque chapitre un aperçu de son contenu sous la forme de listes de points à vérifier, qui ont l'avantage d'être plus complètes qu'un simple index et de faciliter la consultation des fiches d'information en résumant les principaux points abordés. Le manuel entend présenter Internet sous toutes ses facettes, en commençant par les bases de son fonctionnement et du stockage de nos données, avant de poursuivre par les moyens d'obtenir des informations de qualité et de mettre en relation les personnes et les idées, pour terminer par les outils d'aide et l'avenir des technologies en ligne. Le manuel est une boîte à outils qui aidera l'utilisateur à naviguer dans l'océan de possibilités qui lui sont offertes par Internet et ce faisant, à trouver des moyens de contribuer à façonner le monde en ligne plutôt que de se laisser façonner par lui.

■ Étant présentées sur un média électronique, les fiches d'information sont rédigées de manière aussi synthétique que possible, dans un format facile à lire et permettant de retrouver rapidement les idées, mises en garde, conseils et liens utiles. Toutes commencent par faire le point sur l'état des connaissances relatives à chaque thème avant d'étudier plus en détail les possibilités d'utilisation d'un outil, d'une plateforme ou d'un service à des fins pédagogiques pour en tirer une valeur ajoutée et ouvrir d'autres débouchés. L'attention du lecteur est ensuite attirée sur certains aspects éthiques méritant une réflexion plus approfondie, mais comme il a été fait remarquer précédemment, de nouvelles interrogations peuvent surgir à tout moment dans ce domaine compte tenu de l'évolution constante des technologies. La partie « Mode d'emploi », que l'on retrouve dans la plupart des fiches, est un guide pratique qui explique étape par étape comment fonctionnent les choses ou comment on peut les faire fonctionner pour tirer le meilleur parti des technologies.

■ En bas de chaque fiche d'information, on trouvera des idées pour le travail en classe, des exemples de bonnes pratiques et des informations complémentaires, par exemple des liens vers des articles et répertoires ou d'autres applications de l'outil ou du service en question. Ces pages peuvent être considérées comme un condensé des meilleures pratiques recueillies auprès d'institutions, d'organisations et de personnes travaillant dans le domaine social, éducatif, culturel et de la protection de l'enfance à travers le monde, spécialement compilées par plusieurs experts pour les besoins du manuel. Toutes les précautions ont été prises pour que l'ensemble des recommandations soient à jour, pertinentes et fiables et qu'elles puissent être utilisées avec tous les groupes d'âge, sauf mention contraire. L'attention du lecteur est toutefois attirée sur le fait que dans le monde actuel, des milliers d'URL (Uniform Resource Locators, connues sous le nom de « liens (hypertexte/web) » ou « hyperliens ») sont créées et supprimées chaque jour. Aucun manuel relatif aux technologies en ligne ne peut garantir que toutes les informations et tous les liens qui y figurent resteront valables et continueront d'exister.

■ Le *Manuel de maîtrise de l'Internet* devrait plutôt être considéré comme une photographie de la situation à l'instant t. De nouvelles informations, idées et orientations viendront s'y ajouter pour le maintenir à jour. Les lecteurs sont invités à contribuer à ce processus en faisant parvenir leurs idées, ressources et exemples de bonnes pratiques à la Division de l'enfance du Conseil de l'Europe, children@coe.int.

1. Internet : en tout temps et en tout lieu

” « Nous sommes désormais tous connectés via Internet, comme le seraient les neurones d'un cerveau géant »

Stephen Hawking, physicien et théoricien

LISTE DE POINTS À VÉRIFIER :

1. SE CONNECTER

Avez-vous sécurisé votre connexion Internet en installant un antivirus et un pare-feu et en définissant un mot de passe pour votre routeur ?

Avez-vous établi une charte de bon usage applicable à toute personne utilisant ou ayant accès à Internet par le biais de votre réseau et de vos appareils ?

Avez-vous créé des comptes « Invité » sur les appareils utilisés par vos enfants ?

2. PRÉSENCE EN LIGNE ET « NUAGE »

Vos coordonnées sont-elles affichées sur votre site Internet ou blog ?

Prenez-vous des dispositions pour protéger votre vie privée en ligne ?

Vous assurez-vous que le contenu que vous utilisez pour votre site web ou blog est conforme à la législation sur le droit d'auteur ?

3. WEB 2.0, WEB 3.0 ET PLUS

Avant de mettre en ligne des photos et vidéos, demandez systématiquement leur accord aux personnes qui y apparaissent.

Les recommandations des Internauts sur les sites de voyage et de produits peuvent être utiles, mais êtes-vous bien sûrs qu'elles sont authentiques ?

Le contenu généré par l'utilisateur stimule la créativité et favorise la liberté d'expression, mais fait de l'amélioration d'Internet une responsabilité partagée.

4. BLOGS ET VIDÉOBLOGS

Protégez votre vie privée en utilisant un pseudonyme et ne divulguez pas certaines données personnelles.

Protégez votre blog ou vidéoblog contre le piratage informatique en paramétrant un niveau de sécurité adéquat et en sauvegardant régulièrement vos contenus.

Lorsque vous mettez du contenu en ligne sur votre blog, gardez à l'esprit son objectif et le public auquel il est destiné.

5. INTERNET EN MOBILITÉ

À quel âge les enfants peuvent-ils commencer à utiliser les appareils mobiles en toute sécurité et lesquels sont les mieux adaptés aux plus jeunes ?

Avez-vous une connaissance suffisante des techniques de géolocalisation et du Bluetooth pour pouvoir utiliser vos appareils mobiles sans difficulté et sans risque pour la sécurité ?

L'apprentissage nomade (*m-learning*) et le paiement mobile sont des applications qui modifient notre façon d'apprendre, de travailler et d'acheter. Que savez-vous de ces évolutions récentes ?

Imaginez maintenant que votre routeur soit relié par un câble à celui de votre voisin, qui serait lui-même relié à celui de la maison d'à côté, et ainsi de suite : c'est exactement ainsi que fonctionne Internet, à une plus grande échelle. Il se compose d'une multitude de routeurs connectés les uns aux autres qui vous permettent de transférer des informations (données contenues dans des courriers électroniques, images, vidéos, etc.) d'un point (votre ordinateur de bureau par exemple) à un autre (le smartphone d'un ami en vacances à l'autre bout du monde).

— Aussi étonnant que cela puisse paraître, ces informations transitent par d'immenses câbles sous-marins qui relient les continents et sont directement connectés à l'infrastructure (habituellement les lignes téléphoniques) des territoires de départ et d'arrivée.

Lorsque vous envoyez une image depuis votre ordinateur à un ami, celle-ci est découpée en minuscules morceaux de données appelés « paquets » qui sont étiquetés, un peu comme une enveloppe envoyée par la poste (origine, destination et indications sur la manière dont les données doivent être assemblées pour recomposer l'image). En lieu et place d'informations comme le numéro de la maison et le nom de la rue, les paquets de données contiennent l'adresse IP³ du lieu d'envoi et l'adresse IP du lieu de destination. Ils sont ensuite envoyés par l'intermédiaire de votre ligne téléphonique vers les installations de votre fournisseur d'accès à Internet, elles-mêmes reliées à la dorsale Internet (c'est-à-dire l'ensemble des routeurs connectés les uns aux autres dont nous avons parlé précédemment). Les paquets sont redirigés plusieurs fois par ces routeurs jusqu'à ce qu'ils arrivent à bon port (on appelle cela le nombre de « sauts »). Mais quelle est vraiment leur destination ? Contrairement à ce que l'on pourrait penser, si vous envoyez par exemple une image par courrier électronique, ce n'est pas l'ordinateur de votre ami, mais les centres de données du client de messagerie de ce dernier.

— Les centres de données sont d'immenses entrepôts remplis de routeurs et de disques durs. Votre image sera stockée sur plusieurs disques durs (pour protéger les données en cas de défaillance de l'un d'entre eux). Si votre ami utilise Gmail, par exemple, l'image que vous lui aurez envoyée pourrait être stockée physiquement dans l'un des centres de données de Google aux États-Unis, en Irlande, en Belgique, aux Pays-Bas ou ailleurs⁴. Lorsque votre ami souhaite voir la photo, son ordinateur envoie une demande qui est redirigée, en transitant par la dorsale, vers le centre de données en question, lequel transmet les données et affiche l'image sur l'écran.



GOVERNANCE D'INTERNET

— Comment Internet a-t-il été mis en place ? Qui est chargé de maintenir les infrastructures actuelles et d'en créer de nouvelles ? Qui décide des normes telles que les adresses IP ?

— Si l'idée des hyperliens et pages web interconnectées est venue de Tim Berners-Lee et Robert Cailliau, qui travaillaient tous deux au CERN en Suisse, le premier réseau interconnecté, ARPANET, a été créé aux États-Unis entre des universités⁵.

— C'est pourquoi le tout premier organisme chargé d'attribuer des « adresses » uniques, essentiellement pour autoriser les utilisateurs à se connecter au réseau, a été établi aux États-Unis : l'IANA (Internet Assigned Numbers Authority).

— Avec la croissance d'Internet, il est apparu nécessaire d'assurer une meilleure coordination de son développement, de sa maintenance, de sa stabilité et de sa sécurité. Le Département du Commerce des États-Unis a alors proposé une réforme de l'IANA qui est devenu l'ICANN⁶ (Internet Corporation for Assigned Names and Numbers) en 1998. Cet organisme a été créé officiellement, sous la forme d'une société à but non lucratif « à des fins publiques et de bienfaisance » caractérisée par une logique de gouvernance ascendante consistant à coordonner des milliers de partenaires dans le monde, notamment du secteur privé, de la société civile et des gouvernements. Il a cependant fait l'objet de nombreuses critiques et de demandes de réforme de la part de plusieurs pays en raison de ses liens avec le gouvernement des États-Unis et du risque de surreprésentation des intérêts américains.

— En réaction à ces critiques, l'ICANN s'est ouvert à beaucoup d'autres partenaires dont

3. https://fr.wikipedia.org/wiki/Adresse_IP

4. <http://www.google.com/about/datacenters/inside/locations/index.html>

5. https://fr.wikipedia.org/wiki/World_Wide_Web

6. <https://www.icann.org/fr>

111 États et un certain nombre d'observateurs, parmi lesquels les principales organisations des télécommunications et le Conseil de l'Europe. Mais il lui a été reproché le manque de participation démocratique et de consultation plus large des partenaires, ce qui a donné lieu à la création par l'Organisation des Nations Unies du Forum sur la gouvernance d'Internet en 2006.

— Le Forum sur la gouvernance d'Internet se réunit annuellement et donne à un grand nombre d'acteurs, en particulier les jeunes, la possibilité de partager leurs points de vue sur l'avenir de l'Internet.



INTÉRÊT PÉDAGOGIQUE

- Internet donne accès à une somme de nouvelles idées, ressources, possibilités d'apprentissage, informations et services.
- Il facilite le partage d'expériences et la communication entre utilisateurs par-delà les frontières, grâce notamment aux forums, au courrier électronique, aux réseaux sociaux, aux messageries instantanées et aux vidéoconférences. Par conséquent, il offre aux étudiants la possibilité de participer à des projets et de travailler avec d'autres étudiants sans déplacement coûteux.
- Internet rend les outils de recherche accessibles même à ceux qui n'ont pas l'habitude de se rendre à la bibliothèque.
- Grâce à des services et logiciels complémentaires, Internet peut ouvrir de nouvelles perspectives aux personnes ayant des besoins spéciaux.
- Savoir comment Internet est régi permet à tous les citoyens de prendre part aux grandes décisions qui seront prises quant à son avenir.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Il faut savoir qu'Internet donne souvent une fausse impression d'anonymat. Vu la manière dont il fonctionne, vous laissez toujours une trace (votre adresse IP) où que vous alliez sur le réseau.
- Comme ailleurs, on trouve sur Internet des escroqueries, de fausses informations et des contenus inadaptés aux enfants.
- Si Internet ouvre un grand nombre de nouvelles possibilités, les solutions techniques ne sont pas toujours meilleures que les outils traditionnels. Ainsi, bien que le courrier électronique ait révolutionné la communication et que la vidéoconférence puisse donner l'impression d'être « quasiment sur place », rien ne remplacera jamais un échange direct en face à face.
- La gouvernance de l'Internet peut avoir un impact considérable sur votre expérience d'utilisateur en ligne, des principes comme l'anonymat ou la neutralité du réseau étant mis dans la balance. Il se livre une bataille continuelle entre ceux qui défendent le principe d'un Internet libre et ouvert et ceux qui souhaitent le contrôler. Certaines sociétés essaient de rediriger le trafic vers leurs propres sites web, applications ou services en proposant une offre d'Internet mobile « gratuit » limitée à ces sites, applications ou services, et en facturant la consultation de toute autre page⁷. Facebook, par exemple, a créé le portail « Internet.org » qui est la page d'accueil par défaut pour tous les utilisateurs se connectant par l'intermédiaire de leur fournisseur d'accès à Internet dans plusieurs régions du monde, et en particulier dans les pays en développement⁸.
- Il faut avoir conscience que tout ce que vous partagez en ligne peut être mis en cache, stocké ou copié.



MODE D'EMPLOI

- La quasi-totalité des appareils disponibles sur le marché aujourd'hui peuvent se connecter à Internet, que ce soit par Wi-Fi, par accès Internet mobile (pour les smartphones et tablettes, par exemple) ou par un câble Ethernet (la plupart des ordinateurs étant équipés d'un port Ethernet).

7. <https://en.wikipedia.org/wiki/Zero-rating>

8. <https://fr.wikipedia.org/wiki/Internet.org>

- Pour vous connecter à Internet, deux grandes options s'offrent à vous :
 - ▶ Contacter un fournisseur d'accès à Internet (FAI), habituellement une société de téléphonie ou un câblo-opérateur, qui vous fournira un nom d'utilisateur et un mot de passe et parfois un modem/routeur pour vous connecter à Internet par le biais de votre ligne téléphonique ou de votre réseau câblé de télévision.
 - ▶ Souscrire une offre « Internet mobile » auprès de votre opérateur de téléphonie mobile. Il faut savoir que si vous choisissez cette option, la quantité de données pouvant être téléchargées/mises en ligne restent assez limitée, bien qu'elle augmente progressivement avec le déploiement des standards de télécommunication mobile 4G ou 5G (plus rapides) par un nombre toujours plus grand d'opérateurs.
- Il existe également de plus en plus de points d'accès Wi-Fi « ouverts » que vous pouvez utiliser pour vous connecter gratuitement à Internet. On les trouve dans divers lieux publics comme les bibliothèques, mais également dans des bars, restaurants et centres commerciaux. La plupart du temps, avant de vous connecter, il vous sera demandé d'effectuer l'une ou plusieurs des opérations suivantes : accepter les conditions d'utilisation, créer un compte au moyen de votre adresse de courrier électronique (attention : cette adresse pourra ensuite être utilisée pour vous envoyer de la publicité, veillez donc à créer une adresse spécifique pour cet usage) ou entrer un mot de passe pour vous connecter à Internet. Dans les bars, restaurants ou hôtels, par exemple, le Wi-Fi « ouvert » n'est souvent accessible qu'aux clients : il vous faudra alors demander le mot de passe à un employé. Lorsque vous vous connectez depuis un point d'accès sans fil public, ne partagez jamais de données confidentielles et n'effectuez pas de transactions bancaires en ligne ou d'autres opérations sensibles.
- La plupart des FAI mettront à votre disposition un routeur préconfiguré qu'il vous faudra simplement brancher sur votre ligne téléphonique/prise câble pour être connecté. Parfois, vous devrez acheter un routeur et le configurer vous-même. Pensez à vérifier auprès de votre FAI si le routeur dont vous disposez ou que vous avez l'intention d'acheter est compatible avec votre abonnement Internet.

SUGGESTIONS D'ACTIVITÉS EN CLASSE



Sous Windows 7 et versions ultérieures



1. Cliquer sur le bouton « **Démarrer** ».
2. Taper « **cmd** » dans la barre « **Rechercher** » et cliquer sur l'icône de programme qui apparaît dans le menu démarrer.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>
  
```

3. Taper « **tracert wikipedia.org** » puis appuyez sur « **Entrée** ».
4. Vous pourrez alors visualiser les « **sauts** » qui ont été faits entre votre ordinateur et le site web auquel vous souhaitez accéder et le temps mis de l'un à l'autre. Dans cet exemple, nous voyons que pour accéder à Wikipédia, nous passons tout d'abord par les routeurs de notre FAI « local » (dans notre cas, Belgacom en Belgique), puis nous traversons l'Atlantique jusqu'à un routeur situé à Washington (abrégié « was ») pour finalement arriver au lieu d'hébergement de Wikipédia. Les élèves sont bien entendu encouragés à faire cette

expérience avec d'autres sites web. Notez le temps pris pour chaque étape en millisecondes. Notice how much time each step took in milliseconds.

```
C:\Windows\system32\cmd.exe
C:\>tracert wikipedia.org
Tracing route to wikipedia.org [208.80.154.224]
over a maximum of 30 hops:
  0  12 ms   45 ms   7 ms   192.168.1.1
  1  25 ms   28 ms  175 ms  1.192-134-109.adsl-dyn.isp.belgacom.be [109.134.192.11]
  2  *        *        *      Request timed out.
  3  193 ms  39 ms   77 ms  ae-12-1000.ibrstr3.isp.belgacom.be [91.183.246.108]
  4  30 ms   43 ms   52 ms  ae2.bru21.ip4.gtt.net [141.136.102.217]
  5  126 ms  162 ms  133 ms  xe-7-3-0.was10.ip4.gtt.net [141.136.111.10]
  6  412 ms  388 ms  277 ms  xe-5-3-1.cr2-eqiad.wikimedia.org [173.241.131.218]
  7  201 ms  277 ms  185 ms  text-lb.eqiad.wikimedia.org [208.80.154.224]
Trace complete.
C:\>
```



Sous Mac OS X et versions ultérieures

1. Lancer l'Utilitaire de réseau sous Mac OS X (en tapant « utilitaire de réseau » sur Spotlight et en cliquant sur la première occurrence).
2. Cliquer sur "Traceroute".
3. Taper le nom de domaine pour lequel on souhaite exécuter la commande « traceroute », par exemple « **Wikipedia.org** » et cliquer sur « **Trace** ».
4. Vous pourrez alors visualiser le chemin emprunté de votre ordinateur au web que vous souhaitez consulter et le temps mis pour chacun des « sauts » effectués.

Matériel pour les enseignants

- Pour plus d'informations, voir la vidéo du Naked Science Scrapbook « How does the Internet work? »⁹.
- Engagez une discussion en classe sur la manière dont les technologies en ligne peuvent être bénéfiques aux personnes ayant des besoins spéciaux, en vous appuyant sur le plan d'action du Conseil de l'Europe dans ce domaine pour trouver des idées¹⁰.



BONNES PRATIQUES

- Choisissez une connexion adaptée à votre utilisation d'Internet. Si vous utilisez régulièrement des services qui nécessitent un Internet très rapide, comme la diffusion en continu de vidéos (*streaming*) haute définition, optez pour une connexion plus rapide (au moins 20 Mégabits par seconde, soit l'équivalent de l'ADSL2+). Plus particulièrement, recherchez une connexion Internet sans limitation de la quantité de données pouvant être téléchargées. Si vous n'utilisez Internet que pour vous tenir au courant de l'actualité et envoyer des courriers électroniques, un abonnement Internet de base pourra suffire¹¹.
- Éteignez toujours vos appareils (ordinateurs) ou désactivez la connexion Wi-Fi sur votre smartphone/tablette lorsque vous allez vous coucher. Les laisser connectés peut créer un risque supplémentaire pour la sécurité de vos données, voire pour votre santé (voir Fiche d'information 19 sur la sécurité).

9. <https://www.youtube.com/watch?v=oj7A2YDgIWE>

10. https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action_Plan_CoE_Easy_to_Read_13nov08_FR.pdf

11. www.cnet.com/internet-speed-test

- Il est important de savoir comment accéder à la page de configuration de votre routeur. Le plus souvent, il suffit de taper l'une des adresses IP suivantes sur votre navigateur : 192.168.1.0 ou 192.168.1.1. La plupart des pages de configuration Wi-Fi ayant des comptes administrateur « par défaut » avec des noms d'utilisateur et des mots de passe très basiques (par exemple : « admin » et « admin »), il convient de sécuriser l'accès à la page de configuration de votre routeur car celle-ci peut facilement être utilisée pour modifier vos paramètres ou accéder à votre réseau domestique.
- Asseyez-vous à côté de vos enfants chaque fois que vous le pouvez lorsqu'ils surfent sur Internet pour encourager la discussion sur leurs expériences en ligne et accroître la confiance ; lancez-vous le défi d'apprendre ensemble.
- Intéressez-vous à la gouvernance d'Internet et participez au débat public sur des principes fondamentaux comme l'anonymat, la sécurité ou la neutralité du réseau.
- Établissez une charte de bon usage¹² si d'autres personnes utilisent l'ordinateur ou le réseau dont vous êtes le responsable.



INFORMATIONS COMPLÉMENTAIRES

- The List est un annuaire mondial de FAI : <http://www.thelist.com>.
- Les sites web éducatifs European Schoolnet <http://www.eun.org>, Global SchoolNet <http://www.globalschoolnet.org/GSH/> et Education World <http://www.educationworld.com/> proposent des ressources et des projets collaboratifs.
- On trouvera des conseils pour la rédaction d'une charte de bon usage sur Education World, portail en ligne pour les enseignants et professionnels de l'éducation : http://www.educationworld.com/a_curr/curr093.shtml.
- Le portail Insafe propose des ressources et des conseils sur les moyens de se connecter et de naviguer sur Internet en toute sécurité : <https://www.betterinternetforkids.eu/>.
- Le site web officiel du Forum de la gouvernance d'Internet permet de discuter des questions de politique publique liées à Internet : <http://www.intgovforum.org/cms/>.
- On trouvera plus d'informations concernant la neutralité du réseau sur la page Wikipédia : https://fr.wikipedia.org/wiki/Neutralité_du_réseau.
- On trouvera plus d'informations concernant l'ICANN sur son site Internet : <https://www.icann.org/>.

12. http://en.wikipedia.org/wiki/Acceptable_use_policy

Présence en ligne et « nuage »



Avez-vous quelque chose à partager avec le reste du monde et vous faut-il un espace en ligne pour le faire ?

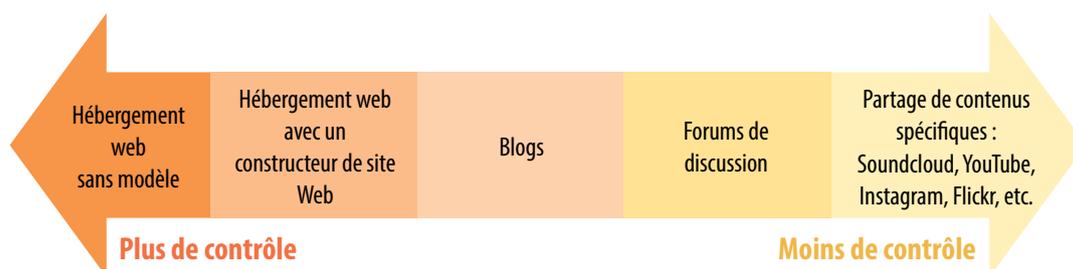
— Si les sites web ont été l'un des premiers moyens de publier du contenu en ligne, de plus en plus d'alternatives ont vu le jour ces dix dernières années. Aux débuts d'Internet, il n'était pas facile de mettre en place un site web : c'était un processus relativement coûteux qui nécessitait des compétences en matière de codage. Aujourd'hui, il ne faut même plus être un spécialiste en informatique pour créer et concevoir son propre site. Il est néanmoins conseillé de prendre le temps d'étudier toutes les options disponibles.

— En résumé, il faut savoir ce que l'on veut mettre en ligne et comment on veut le faire.

— Souhaitez-vous partager du contenu spécifique (images, vidéos, textes, etc.) ou une grande diversité de contenus ? Voulez-vous avoir l'entière maîtrise du processus créatif ou préférez-vous travailler à partir d'un modèle prédéfini que vous pourrez modifier jusqu'à un certain point ? Pourquoi avez-vous besoin de partager du contenu, et à quoi servira-t-il ? Quel est le public visé ? Le monde

entier, votre région, votre ville ou simplement des élèves et des parents ? Quelle somme d'argent êtes-vous prêt à consacrer au partage de contenus en ligne ?

— On trouvera ci-dessous une liste non exhaustive de moyens de partager du contenu, classés selon les possibilités de contrôle/personnalisation du processus.



— Si vous souhaitez bénéficier d'une liberté totale quant au contenu et à la conception, il vous faudra opter pour un hébergement web sans modèle. Cette solution a toutefois un coût et nécessite dans la plupart des cas d'acheter un nom de domaine (par exemple <www.monsiteweb.com>). Si vous ne souhaitez pas apprendre le codage, mais tout de même partager une grande diversité de contenus et disposer d'une grande souplesse sur la forme, vous pouvez opter pour un hébergement web avec un constructeur de site web ou un blog (offrant cependant un choix parfois moindre en ce qui concerne le design). Les forums de discussion sont déjà relativement spécifiques : on peut créer un forum de discussion pour une école, par exemple. Enfin, si vous souhaitez simplement partager des photos, des vidéos ou de la musique, vous pouvez choisir de créer un compte auprès d'un service spécialisé dans l'hébergement de ce type de contenus. En définitive, quel que soit votre contenu, il sera stocké sur le serveur du service d'hébergement que vous choisirez, c'est-à-dire quelque part dans le « nuage ».

— N'oubliez pas que la gratuité de bon nombre de ces services signifie souvent que vos lecteurs seront exposés à de la publicité plus ou moins intrusive (c'est-à-dire gênant la navigation, par exemple une multitude de fenêtres publicitaires, des pages web se superposant au site, un nombre excessif de bannières, etc.)



INTÉRÊT PÉDAGOGIQUE

— Établir une présence et partager des contenus en ligne présente un grand intérêt sur le plan pédagogique et contribue à l'acquisition d'un certain nombre de compétences.

- **Gestion/organisation de contenus** : que vous décidiez de construire un site web ou de créer une galerie de photos, votre contenu doit être organisé de manière simple afin que l'utilisateur puisse trouver rapidement ce qu'il recherche.
- **Conception** : votre identité en ligne sera souvent liée à un logo, une image, un choix de couleurs ou à la mise en page de votre site web, autant d'éléments qui font partie du travail de conception.
- **Compétences numériques** : il est relativement évident que le fait d'assurer une présence en ligne renforcera certaines compétences numériques comme le codage (par exemple, HTML, PHP, HTML5, JavaScript) si vous optez pour la construction d'un site web. Cela dit, même avec d'autres options, il vous faudra acquérir de nouvelles connaissances sur les moteurs de recherche et les moyens d'assurer la visibilité de votre contenu, les formats de fichiers, etc.
- **Compétences de communication/d'écriture** : à moins que vous prévoyiez de partager du contenu sans commentaires, il vous faudra soigner votre style et votre communication pour intéresser votre public.

- **Compétences en marketing** : vu le nombre de personnes en ligne, il est très difficile de se démarquer des autres. Pour vous forger une réputation et accroître votre visibilité en ligne, il vous faudra notamment apprendre à mettre en valeur ce que vous avez créé ou partagé.
- **Travail de groupe** : si votre présence en ligne entre dans le cadre d'un projet commun avec des amis/camarades de classe/élèves, cela renforcera vos compétences de travail en équipe. La gestion d'un site web n'est pas une tâche facile et le travail doit souvent être organisé et réparti entre plusieurs personnes : l'administrateur, le concepteur, le rédacteur de contenus, etc.
- **Autres avantages** : en créant un site web sur un thème spécifique, par exemple sur les mathématiques pour un projet scolaire, vous serez inévitablement amené à approfondir votre connaissance et votre compréhension du sujet.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

■ Si vous souhaitez partager du contenu vous concernant ou créer un site web personnel, vous aurez l'entière responsabilité de ce qui y est publié. Vous (et vos parents si vous êtes mineurs) pourriez vous retrouver en difficulté pour plusieurs raisons.

Motifs juridiques

■ Les limites de la « liberté d'expression » : ce droit n'est pas absolu et il existe un certain nombre de restrictions à son exercice, lesquelles doivent être prévues clairement par la loi, nécessaires dans une société démocratique (proportionnées) et poursuivre un but légitime (l'article 10.2 de la Convention européenne des droits de l'homme précise : « des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire »). Ces restrictions peuvent varier d'un État à l'autre, mais de manière générale, les actes suivants pourraient vous valoir des ennuis avec la justice :

- ▶ diffamation¹ ;
- ▶ discours de haine² ;
- ▶ partage des données personnelles d'un tiers³ ;
- ▶ stockage de données – si vous optez pour des services sur le « nuage », renseignez-vous au préalable pour savoir où seront stockées vos données ; il est de votre droit et même de votre devoir de garder le contrôle sur leur utilisation et leur accessibilité⁴ ;
- ▶ incitation au terrorisme :
 - <<https://goo.gl/cv9XDR>> ;
 - <<https://goo.gl/Tq3UDp>> ;
- ▶ propriété intellectuelle : partagez-vous du contenu qui n'est pas le vôtre ? Dans ce cas, vérifiez bien si vous êtes autorisés à le faire ou non. Le contenu commercial est protégé par la législation sur le droit d'auteur et il faut une autorisation spécifique du titulaire des droits pour l'utiliser. Certains artistes ou créateurs publient du contenu sous « licence » spécifique, souvent de type « Creative Commons ». Selon le cas, celle-ci vous autorisera peut-être à utiliser le contenu à des fins commerciales ou sans avoir à mentionner l'auteur. Si vous souhaitez utiliser du matériel protégé par le droit d'auteur, il vous faudra demander une autorisation en bonne et due forme à l'organisation ou à la personne détentrice des droits (maison de disques, studio de cinéma, etc.).

1. <https://fr.wikipedia.org/wiki/Diffamation>

2. https://fr.wikipedia.org/wiki/Discours_de_haine

3. http://www.echr.coe.int/Documents/Handbook_data_protection_FRA.pdf

4. http://ec.europa.eu/justice/data-protection/reform/index_en.htm



Motifs personnels

- Partage excessif : gardez à l'esprit que ce que vous partagerez sera potentiellement visible par toute personne connectée à Internet, où qu'elle soit dans le monde. Par exemple, publier vos photos privées de vacances, qui contiennent des données de localisation (GPS), pourrait permettre à des personnes qui vous sont étrangères de vous suivre, ou à des voleurs de savoir exactement quand vous êtes absent de votre domicile pour pouvoir vous cambrioler. Soyez stratégique dans vos choix de publication en ligne.
- Réputation en ligne : bien que vous ayez sans doute l'illusion de pouvoir rester anonyme en ligne, il existe de nombreux moyens de retrouver votre véritable identité. Les forces de l'ordre disposent des outils nécessaires pour remonter jusqu'à l'utilisateur sous certaines conditions (le plus souvent dans le cadre d'un mandat délivré par un juge). Par conséquent, soyez conscient que tout ce que vous partagez en ligne contribuera à votre réputation en ligne et hors ligne.
- Si vous partagez des idioties ou du contenu choquant ou de mauvais goût, cela peut avoir des répercussions sur votre vie sociale et professionnelle actuelle et future. Si vous avez besoin de vider votre sac, parlez-en à vos proches ou défoulez-vous sur votre oreiller plutôt que d'envoyer un tweet rageur au monde entier car cela pourrait se retourner contre vous et vous le faire regretter pour le restant de vos jours. Vous pouvez consulter le site [Web we want⁵](http://www.webwewant.eu/fr/) pour en savoir plus sur la protection de votre réputation en ligne.

■ Si vous souhaitez partager d'autres types de contenus (provenant de votre établissement scolaire, par exemple) ou créer un site web officiel pour le compte de votre école, un certain nombre d'autres points sont à prendre en considération :

- Les politiques de l'établissement scolaire en matière de sécurité sur Internet et de bon usage d'Internet doivent être clairement définies avant de créer un site web officiel ou de faire participer des élèves à des concours de création de sites web.
- La maquette et les modalités d'utilisation des photos doivent être conformes à la politique de l'école en matière de sécurité sur Internet.
- Pour des questions de sécurité et de protection de la vie privée, de nombreux établissements scolaires ne mentionnent aucun nom, ou uniquement les prénoms des personnes apparaissant sur les photos qu'ils publient. C'est un élément à prendre en compte lorsque l'on crée un site Internet. Quelle est la politique de votre établissement dans ce domaine ?
- Il est judicieux de contrôler tous les liens vers des sites web extérieurs pour vérifier l'intégrité des informations publiées et s'assurer du respect par ces sites de la politique de l'établissement en matière de sécurité sur Internet.
- En ce qui concerne l'accès à Internet, votre établissement devra définir sa politique : préfère-t-il filtrer les accès à Internet (à moins que la loi ne l'y oblige, auquel cas il n'aura pas le choix) ou enseigner aux élèves à utiliser Internet avec sagesse et discernement ? De nombreuses écoles considèrent qu'il est plus efficace d'associer ces deux techniques. De même, lorsque l'on confie à des élèves la tâche de créer un site web, il ne faut pas oublier que des utilisateurs du monde entier pourront le consulter. Ce sera en quelque sorte un instrument de relations publiques pour votre établissement. Il serait donc sage que les enseignants supervisent le travail des élèves et les guident tout au long de la phase de création.
- Les enseignants, et dans certains cas les parents, sont responsables en dernier ressort des productions des élèves. Par conséquent, ils devraient avoir le droit de refuser une page web ou d'en faire retirer une du site de l'école ou d'un projet. Pour pouvoir superviser convenablement le travail des élèves, les enseignants devraient toujours avoir accès aux mots de passe⁶, sites web⁷, etc.

5. <http://www.webwewant.eu/fr/>

6. https://fr.wikipedia.org/wiki/Mot_de_passe

7. https://fr.wikipedia.org/wiki/Site_web



MODE D'EMPLOI

- À moins que vous préfériez opter pour un service professionnel payant d'hébergement web ou avoir votre propre nom de domaine, il n'est pas très difficile de se lancer dans la publication de contenus en ligne.
- La plupart des services que vous utiliserez, que ce soit des constructeurs de site web, des blogs ou des vidéoblogs (voir Fiche d'information 4) comportent des tutoriels qui vous aideront à démarrer.
- Un certain nombre de compétences restent toutefois nécessaires pour créer un site web en partant de zéro. Fort heureusement, il existe aujourd'hui des millions de façons d'apprendre le codage, dont les plus connues sont Codeacademy⁸ et W3schools⁹. Cela dit, plutôt que de vous arrêter à celles-ci, prenez toujours le temps d'effectuer des recherches en ligne pour trouver d'autres informations dans votre langue ou adaptées à vos besoins.
- Si vous choisissez un service d'hébergement web professionnel, il faudra également fournir d'autres informations que votre adresse de courrier électronique, par exemple votre nom, votre adresse, votre numéro de téléphone et des informations de paiement, par exemple un numéro de carte de crédit. Il est donc préférable que les enfants et les jeunes demandent de l'aide et des conseils à un adulte (enseignant, parent) avant de se lancer dans ce type d'entreprise.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

Construire la présence en ligne de votre établissement

Utilisé correctement, un site, blog, vidéoblog ou autre outil similaire constitue un moyen formidable de réunir les très nombreuses facettes d'une communauté scolaire. Il peut favoriser un sentiment de cohésion et être un précieux outil de communication pour rendre l'information facilement accessible à tous. Voici quelques suggestions pour le contenu du site.

- Les enseignants peuvent fournir les plans de cours ou un aperçu des réalisations des élèves sur une période donnée.
- Les administrateurs peuvent publier les emplois du temps et annonces diverses.
- Les enfants et les jeunes peuvent publier leur production artistique, des poèmes, des récits, des rapports et d'autres travaux.
- Les parents d'élèves peuvent utiliser le site pour annoncer des activités, fêtes et autres événements parents-professeurs.
- La communauté au sens large peut utiliser le site pour annoncer un match de football ou diffuser des informations sur les sorties scolaires, l'action de la police, les travaux routiers, etc.

Si la diversité des contenus peut enrichir un site web, blog ou vidéoblog, trop de contributeurs peuvent également rendre complexe la maintenance web. Il est important qu'une petite équipe soit chargée de la collecte et de la mise en forme du contenu. Cette tâche pourra être confiée à un enseignant, à un administrateur ou à toute autre personne choisie pour être le coordinateur des technologies de l'information et de la communication (TIC).



BONNES PRATIQUES

- Gardez une trace de tous vos comptes. Créez des dossiers contenant les adresses dont vous vous servez pour vous inscrire aux différents services que vous utilisez et classez vos courriers électroniques de manière à pouvoir retrouver les informations importantes comme votre nom d'utilisateur.

8. www.codeacademy.com
9. www.w3schools.com/

- Utilisez toujours votre adresse de courrier électronique plutôt que votre compte de réseaux sociaux pour créer un compte sur des sites web, blogs ou vidéoblogs. S'il peut sembler pratique de s'enregistrer à ces services par l'intermédiaire des comptes Facebook, Google+ ou autres, lorsque vous le faites, vous les autorisez à accéder à une grande partie de vos données. Par ailleurs, bien que certains réseaux sociaux donnent l'impression qu'ils dureront éternellement, s'ils cessaient d'exister (ils peuvent en effet devenir obsolètes s'ils ne rencontrent pas l'adhésion du public), vous pourriez vous retrouver dans l'incapacité de vous connecter au compte en question.
- Le partage de contenus en ligne via un site web, blog ou vidéoblog est certes une occasion privilégiée de faire connaître vos points de vue, mais il ne doit pas vous faire oublier l'importance de protéger votre vie privée en utilisant un pseudonyme ou en ne divulguant pas un certain nombre d'informations personnelles.
- Commencez modestement, prenez votre temps pour apprendre et expérimenter avant de mettre du contenu en ligne ou de le présenter en classe. Il peut être utile de visiter d'autres sites web, blogs ou vidéoblogs pour trouver de l'inspiration.
- Affichez toujours les coordonnées de votre établissement (adresse et numéro de téléphone, par exemple) sur son site web, blog ou vidéoblog.
- Veillez à ce que votre contenu web soit adapté à l'utilisateur et aux différents appareils. Aujourd'hui, de plus en plus de gens accèdent à du contenu web via leurs téléphones portables et cela nécessite souvent un design adapté. Il est également souhaitable de rendre votre contenu web accessible aux personnes handicapées. On trouvera des ressources sur le site : <http://www.w3.org/WAI/gettingstarted/Overview.html>.
- Chaque fois que vous le pouvez, mettez en ligne du contenu multilingue pour que les non-francophones puissent également en bénéficier.



INFORMATIONS COMPLÉMENTAIRES

- Cet article sur les tendances numériques donne plus d'informations sur les constructeurs de sites web : <http://web.archive.org/web/20160622040107/http://www.digitaltrends.com/computing/bestwebsite-build-websites-free/>.
- Article Wikipédia sur la gestion de la réputation en ligne : https://en.wikipedia.org/wiki/Online_presence_management.
- Les fiches d'information de la Commission européenne relatives au nouveau Règlement général sur la protection des données incluent le « droit à l'oubli » : http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf.

- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.

Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile.

Article 29 – L'éducation doit favoriser l'épanouissement de la personnalité de chaque enfant et le développement de ses talents dans toute la mesure de leurs potentialités. Elle doit inculquer à l'enfant le respect de ses parents, de sa propre culture et de celle des autres.

Article 31 – L'enfant a le droit de se reposer et de se livrer au jeu et à un vaste ensemble d'autres activités.

Web 2.0, Web 3.0 et plus



Le Web 2.0 nous permet non seulement de télécharger et de consommer du contenu, mais également d'en publier en ligne et d'en créer. Le terme « Web 2.0 » désigne ce qui est perçu comme une « deuxième génération » de services web privilégiant le contenu généré par l'utilisateur, la facilité d'emploi et l'interopérabilité. On y inclut les sites de réseautage social (voir Fiche d'information 8), les wikis, les outils de communication et les folksonomies qui facilitent tous les démarches collaboratives en ligne et les échanges entre utilisateurs. Il ne s'agit pas d'une simple mise à jour technique de plus, mais bien d'une suite de changements qui s'appuient sur les fonctions interactives du « Web 1.0 » pour utiliser le réseau comme une plateforme permettant aux utilisateurs de faire fonctionner les applications logicielles grâce à un simple navigateur.

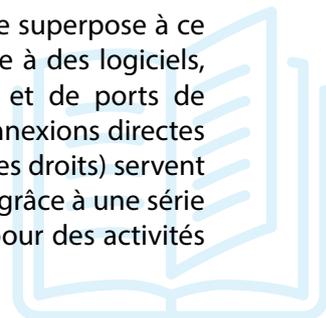
— Sur un site Web 2.0, les utilisateurs peuvent être propriétaires des données et exercer un contrôle sur celles-ci grâce à une « architecture participative » qui les encourage à apporter une valeur ajoutée aux applications tandis qu'ils les utilisent. Il en résulte d'immenses avantages par rapport aux sites traditionnels qui limitent le rôle des visiteurs à la consultation et dont le contenu n'est modifiable que par leur propriétaire. Les sites du Web 2.0 présentent souvent une interface conviviale reposant sur des médias multiples ou « riches », autrement dit des technologies de pointe comme la diffusion en

continu de vidéos, les applets (petites applications téléchargées) qui interagissent instantanément avec l'utilisateur et les contenus qui changent lorsque l'on passe le curseur dessus.

WEB 3.0 ET PLUS

Le Web 3.0 (voire Web 4.0, 5.0, etc.) est un terme plus largement discuté. Certains spécialistes le décrivent comme l'évolution et l'extension du Web 2.0, tandis que d'autres y voient une sorte d'« intelligence connectée » qui relie les données, les concepts, les applications et les individus et qui, de l'avis de nombre d'entre eux, finira elle-même par générer des données. Certains lui préfèrent le terme de « web sémantique », que d'autres utilisent plutôt pour désigner l'une des multiples technologies et tendances convergentes qui définiront la prochaine grande évolution du Web.

Il existe également d'autres types de réseaux. Le darknet est un réseau qui se superpose à ce que nous appelons le World Wide Web, et auquel l'on ne peut accéder que grâce à des logiciels, configurations ou autorisations spécifiques, souvent au moyen de protocoles et de ports de communication particuliers. Les réseaux d'ami à ami (friend-to-friend ou F2F – connexions directes entre personnes qui se connaissent) et pair à pair (entre utilisateurs ayant les mêmes droits) servent habituellement au partage de fichiers. Enfin, les réseaux tels que Tor fonctionnent grâce à une série de connexions rendues anonymes et peuvent donc être utilisés plus facilement pour des activités illégales.



CONSÉQUENCES POUR LES ÉTABLISSEMENTS SCOLAIRES

Les outils du Web 2.0 stimulent la créativité, la collaboration et la communication et peuvent révolutionner l'enseignement. Ils favorisent de nouveaux modèles pédagogiques comme les classes inversées où les élèves font à la maison un certain nombre d'activités traditionnellement réservées au travail en classe¹. Nombre d'entre eux étant gratuits, ils contribuent à réduire les dépenses en logiciels et incitent au développement de nouveaux modèles de licences pour les établissements scolaires.

Les différences entre le Web 1.0, 2.0 et 3.0 sont nombreuses, comme le montre le tableau ci-dessous.

Web 1.0	Web 2.0	Web 3.0
Basé sur des applications	Basé sur le web	Applications multi-appareils/dynamiques
Isolé	Collaboratif	Diffuse du contenu personnalisé
Licence ou achat	Gratuit	Média multilicence
Créateur unique	Création collaborative	Interaction entre les créateurs et les appareils
Code propriétaire	Code source ouvert (Open Source)	Construit de manière collaborative, exécutable
Contenu soumis à droit d'auteur	Contenu partagé	Contenu généré par l'utilisateur et par machine

Quatre des technologies les plus utilisées du Web 2.0 sont les réseaux sociaux (voir Fiche d'information 8), la messagerie, la création et le visionnage de vidéos et de films (par le podcast, les MP4, etc.) et les wikis, bien qu'il en existe d'autres.

Le Podcasting² Le podcasting, né avec le lancement de l'iPod (le lecteur de médias portable d'Apple lancé en 2001), vient des mots anglais « iPod » et « broadcast ». À l'origine, c'était un moyen de partager des fichiers audio par Internet pour une lecture en différé sur des appareils mobiles ou

1. https://fr.wikipedia.org/wiki/Classe_invers%C3%A9

2. <http://computer.howstuffworks.com/internet/basics/podcasting.htm>

des ordinateurs, dans un format connu sous le nom de MP3 (fichier numérique MPEG avec couche audio). Aujourd'hui, la plupart des appareils mobiles permettent d'enregistrer des vidéos et le MP3 a laissé la place au MP4, format multimédia qui stocke à la fois de l'audio et de la vidéo. Grâce aux podcasts et aux vidéos MP4, il est plus facile pour les enseignants et les élèves de faire entrer le monde extérieur dans les salles de classe, de vivre ensemble des événements et de partager des expériences.

— **Le partage de vidéos** est devenu extrêmement populaire depuis le lancement de YouTube en 2005 et se retrouve également sur de nombreuses plateformes de médias sociaux. Teachertube³ est un site basé sur YouTube⁴ qui cible plus particulièrement les enseignants et les contenus à vocation pédagogique ; il peut également être utilisé par les établissements scolaires et les associations pour créer leurs propres chaînes de partage de vidéos. Les sites de partage de vidéos⁵ proposent en général des fonctionnalités de recherche et permettent aux utilisateurs de publier des vidéos, de les commenter, d'y ajouter des étiquettes (tags) et de les visionner. Il existe de nombreuses communautés de production et de partage de vidéos sur des centres d'intérêt communs. Plus récemment, on a vu apparaître des sites qui permettent aux utilisateurs de mettre leurs clips vidéo en ligne et d'y ajouter du son, des sous-titres, etc. Jumpcut⁶ en est un exemple.

— **Les wikis** sont des pages web qui permettent aux lecteurs d'interagir et de travailler en collaboration, car elles peuvent être modifiées ou complétées par chacun. Le wiki est un magnifique outil du Web 2.0 pour le travail rédactionnel en groupes à l'école. Google docs⁷, par exemple, permet aux utilisateurs de travailler de manière collaborative sur des textes, diaporamas et tableaux. Un autre exemple bien connu de wiki est Wikipédia, encyclopédie collaborative qui compte désormais plus d'articles à jour que l'Encyclopaedia Britannica.

— **Le partage de signets** permet aux utilisateurs de partager leurs liens préférés sur Internet. Jusqu'à présent, chaque utilisateur avait sa propre liste de sites web favoris dans son navigateur Internet. Grâce au partage de signets, il peut aujourd'hui la publier de manière à ce qu'elle puisse être utilisée par tous. Le contenu peut être classé à l'aide d'étiquettes (tags) qui facilitent la recherche et l'utilisation. Le site et l'application Delicious⁸, par exemple, sont des outils de partage de signets qui montrent aux utilisateurs combien d'autres personnes ont enregistré un site donné dans leurs signets.

— **Le partage de photos** est un outil populaire qui permet aux Internauts de partager des photos avec les membres de leur famille et leurs amis. Sur le site Flickr⁹, par exemple, les utilisateurs peuvent charger des photos puis inviter les autres personnes à les visionner une par une ou sous forme de diaporama. Des notes et des étiquettes (tags) peuvent être ajoutées à chaque photo et tous les utilisateurs peuvent laisser des commentaires.

— **Des logiciels d'édition et de retouche de photos** sont maintenant disponibles en ligne et permettent aux utilisateurs d'améliorer leurs photos. Parmi ces applications de plus en plus appréciées du public, on peut citer :

- Picasa (Google) <<http://picasa.google.com>>
- iPhoto (Apple) <www.apple.com/iphoto>
- Photo Story (Microsoft) <<http://microsoft-photo-story.en.softonic.com>>.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Les outils du web permettent à n'importe qui de publier ou de modifier des informations sur Internet, et elles ne sont pas toujours correctes ou conformes aux faits. D'où l'importance de multiplier les occasions pour les jeunes apprenants d'acquérir les compétences nécessaires dans le domaine des médias pour juger de la validité et de l'orientation des sites et du contenu.

3. www.teachertube.com

4. <https://support.google.com/youtube/search?q=teachers+channel>

5. <http://computer.howstuffworks.com/internet/basics/video-sharing.htm>

6. www.jumpcut.com

7. <https://www.google.com/docs/about/>

8. <http://del.icio.us.com>

9. www.flickr.com/

- Les enseignants devraient abandonner la vision simpliste selon laquelle tout contenu faux est nécessairement mauvais : il peut être tout simplement le prolongement d'un jeu de rôle en ligne ou présenter un intérêt pédagogique (par exemple : faux profils de personnages célèbres de l'histoire sur des sites de réseautage social).
- Les outils et applications web offrent des possibilités infinies de publication d'informations sur soi-même et sur les autres. Les utilisateurs devraient néanmoins être vigilants quant au risque de divulgation d'informations et d'atteinte à la vie privée. La règle d'or est de ne rien publier qui ne soit pas destiné à ce que le monde entier le sache (voir Fiche d'information 8 sur les réseaux sociaux).
- Il faut du temps et des efforts pour intégrer les technologies au processus d'apprentissage ; par conséquent, avant de vous lancer dans cette entreprise, assurez-vous que l'utilisation des outils du Web 2.0 et 3.0 présentera un intérêt pour vos apprenants.
- Les outils du Web 2.0 ne se valent pas tous et ne reposent pas tous sur la même philosophie ou le même modèle économique. Tandis qu'un site web comme Wikipédia adopte une approche non commerciale, indépendante, collaborative et basée sur le volontariat, de nombreux réseaux sociaux, comme Facebook, ont un but commercial.
- Le contenu qui alimente Wikipédia sera utilisé au bénéfice de la collectivité tandis que celui qui alimente Facebook sera utilisé, entre autres, pour vous montrer des publicités personnalisées.
- L'évaluation de produits et de services est devenue courante grâce aux capacités du Web 2.0/3.0. Cela dit, il convient de garder un regard critique sur les sites concernés car même sur les plus populaires, les notations ne sont pas toujours fiables ; les recommandations rémunérées sont de plus en plus fréquentes.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- **Utilisation d'Internet** : l'activité principale en ligne pour 86% des Internautes est la socialisation, suivie de la recherche d'informations (près de 50%) et des activités professionnelles et commerciales (25% environ)¹⁰. Examinez les statistiques sur les usages d'Internet avec vos élèves/enfants. Invitez-les à comparer leur usage d'Internet avec celui d'autres jeunes dans leur pays et ailleurs dans le monde, ainsi qu'avec l'usage qui en était fait il y a une dizaine d'années. Quelles conséquences cela pourrait-il avoir ?
- **Vidéo** : les élèves peuvent créer leurs propres vidéos pour partager plus largement leurs points de vue et opinions sur un sujet donné. Faites-les travailler en équipes, préparez un scénario et demandez-leur de créer une vidéo avec leur téléphone portable. Cela leur donnera la possibilité de débattre de sujets tels que le droit d'auteur (Fiche d'information 14), l'obtention de l'accord de la personne filmée/photographiée (ou l'accord de ses parents si c'est un mineur) avant de diffuser les images sur Internet, etc. Ils pourront partager leur vidéo sur le site web de la classe ou de l'école, ou utiliser une chaîne dédiée sur YouTube¹¹ pour s'adresser à des millions d'Internautes. Certains établissements scolaires utilisent aujourd'hui la vidéo pour enregistrer des cours et donner aux absents la possibilité de rattraper ceux auxquels ils n'ont pas assisté.
- **Wikis** : trouvez les wikis les plus adaptés à votre environnement éducatif (voir informations complémentaires) puis organisez un travail collectif pour vos élèves. Vous pourrez ainsi suivre activement le travail de chaque élève et garder une trace de tous les changements apportés. Les wikis sont parfaits pour permettre aux élèves de travailler à de véritables projets collaboratifs entre plusieurs établissements, même de pays différents.

10. <http://www.pewglobal.org/2015/03/19/2-online-activities-in-emerging-and-developing-nations/>.

11. www.youtube.com

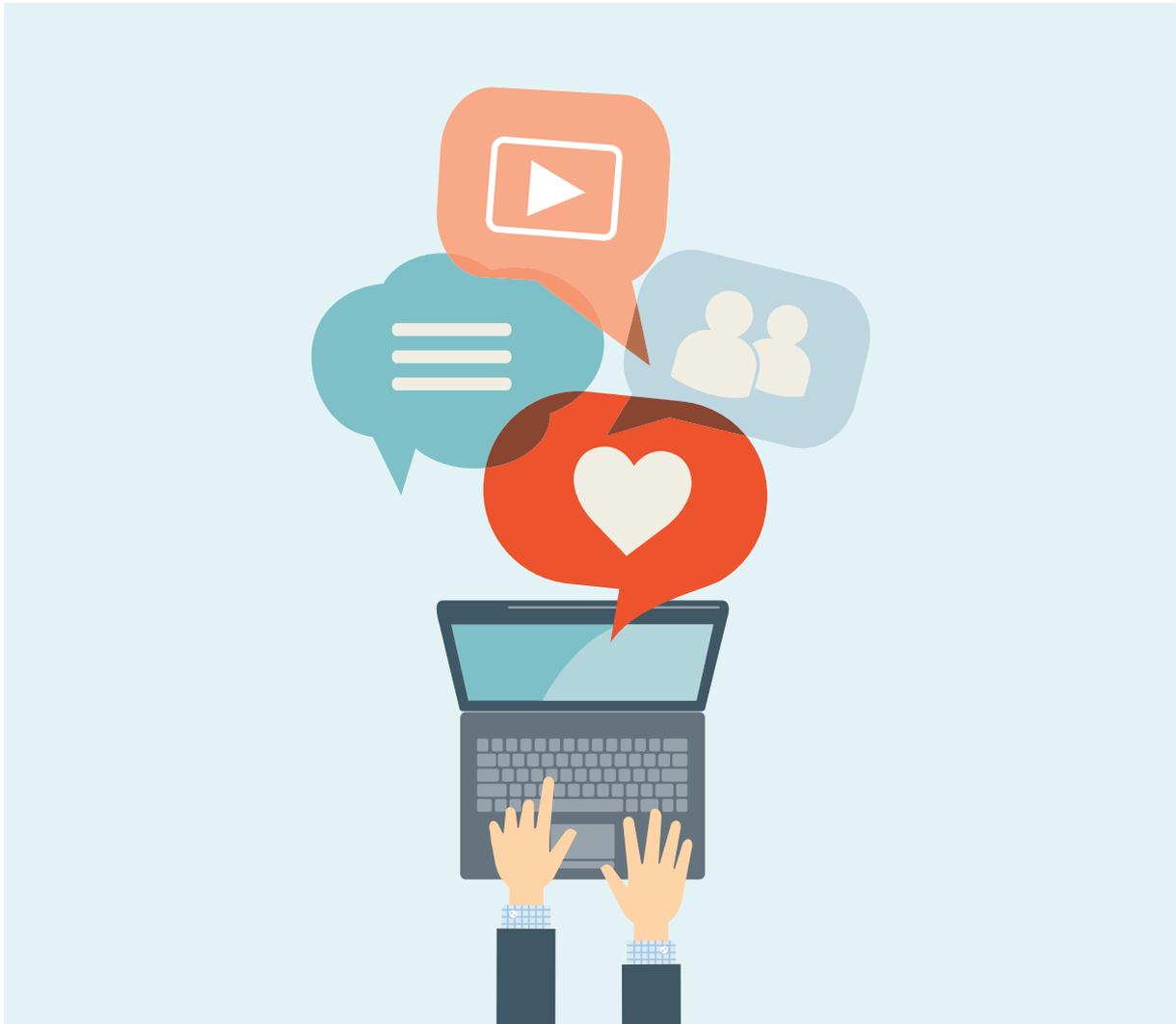
- **Partage de signets** : définissez un projet de recherche spécifique et répartissez les tâches entre les apprenants ou groupes d'apprenants. Vous pouvez utiliser un moteur de recherche pour trouver un outil de partage de signets adapté à vos besoins. Chaque groupe pourra ainsi établir une collection de liens utiles. L'un des avantages de ce système est que les apprenants n'ont plus à se connecter toujours au même ordinateur pour poursuivre un travail, leurs favoris étant accessibles à tout moment depuis n'importe quel poste.



INFORMATIONS COMPLÉMENTAIRES

- Ces deux wikis peuvent être utilisés dans un cadre éducatif : <http://mediawiki.com> et <http://www.pbworks.com>.
- Les enseignants de plusieurs centaines de milliers d'établissements scolaires européens travaillent aujourd'hui en collaboration dans un environnement d'apprentissage sécurisé avec des classes d'autres pays par l'intermédiaire du réseau eTwinning de la Commission européenne, à l'adresse : www.etwinning.net/en/pub/index.htm.
- On trouvera des informations sur l'utilisation des outils du Web 2.0 en toute sécurité à la maison et à l'école sur le site : www.betterinternetforkids.eu/.
- Bien que YouTube Kids propose moins de fonctionnalités que YouTube.com pour ce qui est du visionnage et du partage de vidéos, il fonctionne dans un environnement sécurisé spécialement adapté aux jeunes enfants et propose des conseils aux parents, aux enseignants et aux autres personnes qui s'occupent d'enfants : <https://kids.youtube.com/>.
- On trouvera des informations sur les outils du Web 2.0 destinés à un usage en classe et des téléchargements gratuits à l'adresse : <http://web.archive.org/web/20160413121845/http://www.solutionwatch.com/512/back-to-school-with-the-class-of-web-20-part-1/>.
- On trouvera des applications utiles du Web 2.0 pour l'école primaire à l'adresse : <http://web.archive.org/web/20150914224206/http://langwitches.org/blog/2007/12/22/best-web-20-applications-for-elementary-school/>.

Blogs et vidéoblogs



C'est dans les années 1990 que les carnets de bord en ligne ont évolué pour devenir le blog que nous connaissons aujourd'hui. Le terme « blog¹ » est une contraction de « weblog » et désigne tout journal en ligne créé et publié par des individus ou des groupes. Il a été ajouté au dictionnaire Oxford en 2003. Bien qu'un certain nombre d'hommes politiques et de célébrités aient également créé leurs propres pages, les blogueurs restent dans la plupart des cas des Internautes lambda qui affichent leurs opinions et parlent de leur quotidien.

— Les blogs et vidéoblogs (en abrégé « vlogs ») sont également devenus des plateformes de transformation sociale : les blogueurs et vidéoblogueurs mettent en avant les difficultés qu'ils rencontrent dans leur vie, contribuant ainsi à informer le public sur des questions telles que le métier de parent ou la vie d'une personne autiste, ou à forger une conscience politique sur diverses questions.

— Du fait de la popularité des blogs, de nombreux sites web proposant des logiciels d'aide à la création et à la publication de contenus ont été créés. Chaque article d'un blog peut être commenté, ce qui donne lieu à des discussions et contribue à l'éclosion de nouvelles idées.

— Les blogs sont hébergés par des services spécifiques ou des services classiques d'hébergement web. Aujourd'hui, les tarifs d'hébergement sont jugés raisonnables.

1. <https://fr.wikipedia.org/wiki/Blog>



Mobiblogs

Les blogs mobiles, ou mobiblogs², sont une méthode de publication sur un site web ou un blog au moyen d'un téléphone mobile ou autre appareil portable. Ils sont apparus avec le développement des fonctionnalités de courrier électronique sur les téléphones portables (voir Fiche d'information 5 Internet en mobilité).



Vidéoblogs

Un vidéoblog est la même chose qu'un blog à ceci près que les messages se présentent en format vidéo. Ils sont devenus populaires sur YouTube, mais on peut aujourd'hui en trouver sur Vine, Instagram, Facebook et même Pinterest.



RSS feeds

La syndication de contenu RSS³ (pour « Rich Site Summary ») s'applique désormais aussi aux blogs. Ceux qui souhaitent que leur contenu puisse être publié sur d'autres sites web peuvent le rendre accessible en utilisant le langage XML⁴ (pour « Extensible Markup Language », en français « langage de balisage extensible »).

Le XML est proche du HTML. Il permet aux lecteurs de « s'abonner » à un contenu et de recevoir automatiquement les mises à jour du blog sans avoir à s'y connecter. On parle aussi de fil RSS ou flux XML



Intérêt pédagogique des blogs et vidéoblogs

- ▶ Les blogs et vidéoblogs donnent à leurs créateurs des moyens d'expression. Ils peuvent parler de ce qui les intéresse, partager leurs réflexions et faire connaître à leur public les questions qui revêtent de l'importance à leurs yeux. Ils peuvent évoquer leur quotidien ou leurs expériences et illustrer des points de vue sur un média facilement accessible à tous.
- ▶ Les blogueurs et vidéoblogueurs peuvent en même temps être des « mobiblogueurs » s'ils utilisent leurs smartphones pour rédiger, modifier et mettre en ligne du contenu.
- ▶ Les smartphones étant courants, un public plus divers et souvent plus jeune peut bloguer et vidéobloguer sans avoir à acheter du matériel informatique onéreux.
- ▶ Les blogs et vidéoblogs sont largement utilisés par les journalistes, les chercheurs et les militants comme moyens et sources d'information et d'expression.
- ▶ Les blogs et vidéoblogs traitant du handicap et des besoins spéciaux se multiplient : leur but est de sensibiliser à ces questions et d'ouvrir le débat



Blogs dans le milieu scolaire

Les blogs sont un moyen d'impliquer les élèves dans leurs apprentissages et leur offrent une tribune pour exprimer leurs idées et leur ressenti ; ils peuvent servir d'outil pédagogique innovant pour le débat et le travail collaboratif. Les élèves d'un cours de littérature moderne ont ainsi utilisé un blog pour étudier le roman *The secret life of bees*. L'auteur a rédigé une introduction au cours et les élèves ainsi que leurs parents ont été invités à consigner par écrit chaque jour leurs impressions sur le travail de lecture qui leur était demandé. L'auteur les a ensuite commentées (voir <<http://techtraining.dpsk12.org/ilt/Bees/SLOBees.pdf>>).

Les experts distinguent trois étapes dans la création d'un blog : on commence par définir le public visé, puis l'objet du blog et enfin sa portée. Ce processus est décrit sur le site web <<https://macln.wordpress.com/2011/01/12/three-step-processfor-blogging/>>. Les blogueurs doivent en permanence rassembler, filtrer et mettre en ligne du matériel. En cherchant les informations qu'il commentera ensuite, l'élève se familiarise avec différentes théories et idées et acquiert les

2. <https://fr.wikipedia.org/wiki/Moblog>

3. <https://fr.wikipedia.org/wiki/RSS>

4. https://fr.wikipedia.org/wiki/Extensible_Markup_Language

compétences requises pour analyser le contenu de manière critique et discerner le vrai du faux.

— Dans l'enseignement, la technologie peut être source de motivation. Les blogs plaisent aux élèves car ils leur permettent de laisser libre cours à leur créativité et de s'exprimer. Cet intérêt peut être exploité pour enseigner des matières très diverses.

— Les blogs donnent à chaque élève la possibilité de participer à des discussions qui le confrontent à une multitude de points de vue différents.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Rappelez aux élèves qu'il est déconseillé de divulguer dans les espaces publics d'Internet des informations personnelles qu'ils ne donneraient pas dans une discussion « hors ligne ». Ce problème concerne plus particulièrement les blogs qui sont souvent très personnels.
- Même un blog anonyme n'est pas totalement anonyme et la suppression d'un blog ne signifie pas toujours que son contenu ne sera plus visible.
- Pensez à votre sécurité hors ligne et posez-vous la question de savoir s'il serait facile pour quelqu'un de vous retrouver à partir des informations que vous avez fournies.
- Réfléchissez aux idées que vous allez exprimer et à la personnalité que vous allez afficher en tant que blogueur ou vidéoblogueur. Pourraient-elles offenser ou choquer certaines personnes, par exemple votre établissement scolaire ou votre futur employeur ?
- Les blogs et vidéoblogs peuvent également être utilisés pour diffuser des messages haineux et discriminatoires ou pour mettre en avant du contenu extrême, radical ou choquant.



MODE D'EMPLOI

— Si vous disposez des compétences techniques nécessaires, vous pouvez créer votre blog vous-même. La plupart des gens utilisent des sites qui mettent à disposition des outils de création et de publication de contenus sous forme de blogs. School Blogs à l'adresse <<http://www.schoolblogs.net/wpress/>>, Blogger (voir ci-après) et Wordpress sont des hébergeurs courants qui proposent des services gratuits. Ils donnent des instructions simples, étape par étape, qui vous aident à créer un compte, à donner un nom à votre blog et à choisir un modèle.

— Une fois que votre blog est opérationnel, vous rédigez et mettez en forme vos articles à partir d'une page web centrale. L'interface classique est au format « tel écran, tel écrit » (WYSIWYG⁵) et très facile d'utilisation. Les visiteurs de votre blog peuvent laisser des remarques en cliquant sur le lien « commentaires » à la fin de chaque article.

— Vous pouvez opter pour une modération des commentaires avant leur affichage sur votre page web.

— N'hésitez pas à enrichir vos commentaires avec des liens et des images. Les boutons correspondant à ces fonctionnalités sont généralement présents dans la barre d'outils située au-dessus de la zone dans laquelle vous saisissez votre texte.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Invitez les élèves à travailler en binômes pour un entretien sur un sujet donné, l'un jouant le rôle de blogueur-journaliste et l'autre celui de la personne interrogée. Le blogueur rédige ensuite une note de blog que l'élève interviewé devra approuver.
- Recherchez les principaux blogs et vidéoblogs consacrés au handicap, aux besoins spéciaux, au changement social ou à la sensibilisation de l'opinion. Invitez les élèves à discuter de la

5. « What you see is what you get » : https://fr.wikipedia.org/wiki/What_you_see_is_what_you_get

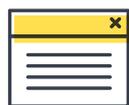
manière dont ils peuvent apporter leur contribution à ces derniers en laissant un commentaire ou en proposant un article de blog.

- Invitez ensuite les élèves à débattre de la méthode la plus adaptée pour transmettre leur message : blog, vidéoblog, série de tweets, vidéos Vine ou Périoscope. Les possibilités sont infinies. Si les élèves choisissent Twitter, Vine, Périoscope ou toute autre application, rappelez leur de ne pas oublier d'ajouter à leur publication des liens vers leur blog.
- Demandez aux élèves d'établir une liste de 5 à 10 sujets qui les intéressent. Effectuez ensuite quelques recherches pour voir s'il existe des blogs sur ces thèmes.
- Quels sont les sujets abordés par les jeunes ou étudiants blogueurs qui enregistrent les audiences les plus élevées : l'environnement, la politique, la mode, la musique, la technologie ?



BONNES PRATIQUES

- Bien que le blog soit un excellent moyen d'exprimer vos idées, il peut être souhaitable de protéger votre vie privée en utilisant un pseudonyme et en vous abstenant de communiquer certaines informations à caractère personnel. Les enfants et les jeunes doivent être particulièrement vigilants quant à la divulgation de ce type de données dans un blog.
- Respectez la législation relative aux droits d'auteur et n'utilisez pas les maquettes de blogs ou photos d'autres personnes sans leur accord. Il existe de nombreux sites web qui vous autorisent à utiliser leurs photos gratuitement, avec ou sans mention de crédits photographiques.
- Créez votre propre blog pour vous familiariser avec cette pratique avant de la présenter en classe. Visitez d'autres blogs pour trouver des idées et de l'inspiration. Le site web School Blogs⁶ compte plus de 4 000 membres et donne aux utilisateurs la possibilité de lancer leur propre blog scolaire.
- Prenez du temps pour expliquer le concept du blogage à vos élèves, et la finalité des blogs. Donnez des exemples de bons et de mauvais blogs, puis quelques règles strictes concernant, par exemple, la longueur et la fréquence des notes, les thèmes abordés, le nombre d'hyperliens, de photos, etc. Demandez aux élèves de tenir un blog, de parler de leurs expériences et de commenter les blogs des autres.



INFORMATIONS COMPLÉMENTAIRES

- Blogger est un site qui propose des outils pour la création de blogs et mobiblogs : www.blogger.com/start.
- On trouvera des informations à l'intention des blogueurs sur les aspects juridiques et éthiques du blog à l'adresse : <http://weblogs.about.com/od/bloggingethics/tp/Blogging-Best-Practices.htm>.
- L'Electronic Frontiers Foundation (EFF) propose un guide juridique pour les blogueurs : <http://www.eff.org/bloggers/lg/>.
- Weblogg-ed – ce site suit les tendances en matière de blogs dans le domaine de l'éducation : www.weblogg-ed.com/.
- « Blogging and RSS – the 'what's it?' and 'how to' of powerful new Web tools for educators » : <http://web.archive.org/web/20160413030845/http://www.infotoday.com/MMSchools/jan04/richardson.shtml>.
- « The educated blogger: using weblogs to promote literacy in the classroom » : <http://firstmonday.org/ojs/index.php/fm/article/view/1156/1076>.

6. <http://www.schoolblogs.net/>

- On trouvera des outils pour accompagner les élèves de l'enseignement primaire et secondaire dans la rédaction d'articles de blog à l'adresse : [<www.readwritethink.org/student_mat/index.asp>](http://www.readwritethink.org/student_mat/index.asp).
- On trouvera des outils pour l'utilisation des blogs par les enseignants à l'adresse [<http://www.socialstudiescentral.com/>](http://www.socialstudiescentral.com/).
- Darren Rowse a été l'un des premiers à pouvoir vivre de son activité de blogueur. Il donne des conseils et des ressources sur son site web : [<www.problogger.net/>](http://www.problogger.net/).
- Parmi les sites web proposant des photos gratuites destinées à être utilisées sur des blogs, on peut citer [<www.pixabay.com>](http://www.pixabay.com), [<www.flickr.com/creativecommons/>](http://www.flickr.com/creativecommons/) et [<www.freedigitalphotos.net>](http://www.freedigitalphotos.net).
- « Learning together to be safe », boîte à outils pour les écoles élaborée par le Département britannique pour les enfants, les écoles et les familles, fournit des ressources aux enseignants sur des questions telles que l'extrémisme et la radicalisation : [<www.preventforschools.org/download/file/mmu-learning-together-to-besafe.pdf>](http://www.preventforschools.org/download/file/mmu-learning-together-to-besafe.pdf).
- Articles pertinents du Conseil de l'Europe, et notamment de la Convention européenne des droits de l'homme [<www.echr.coe.int/Documents/Convention_FRA.pdf>](http://www.echr.coe.int/Documents/Convention_FRA.pdf) :

Article 8 – Droit au respect de la vie privée et familiale.

Article 10 – Liberté d'expression.

- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.

Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile.

Article 29 – L'éducation doit favoriser l'épanouissement de la personnalité de chaque enfant et le développement de ses talents dans toute la mesure de leurs potentialités. Elle doit inculquer à l'enfant le respect de ses parents, de sa propre culture et de celle des autres.

Internet en mobilité



L'utilisation d'Internet en mobilité, c'est-à-dire sur un ordinateur ou un autre appareil portable au moyen d'une connexion mobile ou sans fil, est en progression car les utilisateurs profitent de ces nouveaux moyens de se connecter lorsqu'ils sont loin de chez eux ou de leur lieu de travail.

En 2012, 36 % des personnes âgées de 16 à 74 ans dans les 28 pays de l'UE utilisaient un appareil mobile pour se connecter à Internet. Deux ans plus tard, ce chiffre avait atteint 51 %. Des études¹ montrent que les appareils portables les plus communément utilisés pour se connecter à Internet sont les téléphones portables ou smartphones, les ordinateurs portables, les notebooks, netbooks et tablettes.

Le téléphone portable n'a pas attiré beaucoup d'acheteurs lorsqu'il est apparu sur le marché en 1983. En 1995, on comptait cinq abonnements à un téléphone portable pour 100 habitants dans l'Union européenne. D'après Eurostat, ce chiffre était passé à 80 pour 100 habitants dans l'Union des 25 en 2003.

1. http://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/fr

■ Dix ans plus tard, le nombre d'abonnements à un smartphone était de 400 millions, soit près de 40 % du total des téléphones portables. Ericsson prévoit que d'ici fin 2020, le nombre de smartphones en Europe atteindra les 800 millions².

■ Les frontières entre la technologie mobile et l'informatique à usage personnel s'estompent peu à peu car la plupart des téléphones portables sont équipés de navigateurs Internet et de fonctionnalités de courrier électronique tandis qu'un nombre croissant d'ordinateurs sont équipés de la technologie sans fil.



TECHNOLOGIE MOBILE

■ C'est la technologie utilisée pour les communications cellulaires : certains y voient même l'avenir de l'informatique³.

SMS

■ Les services de minimessages (SMS) sont une fonctionnalité des systèmes de téléphonie, du Web ou des appareils de communication mobile qui permet de transmettre de courts messages textuels⁴.

MMS

■ Les services de messages multimédia (MMS) sont une fonctionnalité qui permet aux utilisateurs d'envoyer des messages comportant du contenu multimédia depuis et vers les téléphones portables⁵.

Apprentissage mobile

■ L'apprentissage mobile ou nomade désigne toute forme d'apprentissage faisant appel aux technologies mobiles telles que les téléphones et ordinateurs portables ou les assistants numériques personnels⁶.

Géolocalisation

■ La géolocalisation est la capacité à déterminer la position géographique réelle d'un objet comme un téléphone portable ou un terminal informatique connecté à Internet.

■ Les utilisateurs de technologies mobiles doivent comprendre le fonctionnement du système de géolocalisation de leurs appareils mobiles et savoir comment régler les paramètres de confidentialité de ces derniers (pour plus de précisions sur les paramètres de confidentialité, voir Fiche d'information 9).

Applications

■ Une application (mobile) est un programme informatique spécialement conçu pour fonctionner sur un appareil portable comme un smartphone, une tablette, une montre connectée et dans certains cas, un vêtement ou autre objet personnel connecté⁷. Pour plus d'informations sur les vêtements connectés, voir la fiche d'information 23.

■ Le nombre d'applications a augmenté de manière directement proportionnelle au nombre d'utilisateurs de téléphones portables. Selon les estimations, c'est une économie qui génère plus de 10 milliards d'euros de recettes par an au sein de l'Union européenne⁸.

■ Il existe une grande diversité d'applications sur le marché. Certaines sont gratuites, d'autres payantes. Cela dit, il est recommandé de bien lire les avis des utilisateurs sur les applications avant de les télécharger ou de les acheter car les applications gratuites peuvent se révéler coûteuses du fait des fonctionnalités d'achat intégrées à celles-ci (voir Fiche d'information 13 sur les achats en ligne).

2. <http://web.archive.org/web/20150324081657/http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-europe.pdf>

3. https://en.wikipedia.org/wiki/Mobile_technology

4. https://fr.wikipedia.org/wiki/Short_Message_Service

5. https://fr.wikipedia.org/wiki/Multimedia_Messaging_Service

6. https://fr.wikipedia.org/wiki/Apprentissage_mobile

7. https://fr.wikipedia.org/wiki/Application_mobile

8. <http://web.archive.org/web/20160617033122/http://www.visionmobile.com/product/the-european-app-economy/>

Mobicash

■ Avec l'augmentation du nombre d'utilisateurs de téléphones portables, les établissements financiers ont mis en place une plateforme financière mobile unique, qui propose des services de traitement des transactions et de paiement mobile sans numéraire.

■ Les services de paiement mobile du prestataire Orange (« Orange money »), par exemple, sont disponibles dans 13 pays : le Botswana, le Cameroun, la Côte d'Ivoire, l'Égypte (sous le nom Mobicash), la Guinée, la Jordanie, le Kenya, Madagascar, le Mali, l'île Maurice, le Niger, le Sénégal et l'Ouganda⁹.

■ Le Royaume-Uni estime que les consommateurs britanniques dépenseront près de 30,5 milliards de livres en achats depuis leurs appareils portables en 2021¹⁰.



COMPRENDRE LES ENJEUX : UN IMPÉRATIF

- Il est préoccupant de constater que les enfants reçoivent des téléphones mobiles ou des tablettes de plus en plus tôt, car aucune étude n'a été menée à long terme pour évaluer les problèmes de développement qui pourraient découler d'une exposition trop précoce à ces appareils.
- Le risque pour les enfants d'effectuer des achats en ligne sans en comprendre les incidences est préoccupant.
- Les résultats des études sur les dangers d'une exposition prolongée au rayonnement, même minime, sont peu concluants.
- Si l'utilisation de l'ordinateur est encore souvent réglementée à la maison, de nombreux parents considèrent que l'utilisation du téléphone portable est privée. Enhardis par cette nouvelle liberté, les enfants pourraient connaître des ennuis financiers s'ils dépensent de l'argent pour des offres promotionnelles ou des accessoires comme les sonneries.
- Les téléphones mobiles peuvent être utilisés comme appareils de surveillance grâce à leurs fonctionnalités de géolocalisation. La question de l'équilibre entre sécurité et liberté fait aujourd'hui débat.
- La technologie Bluetooth¹¹ pose des problèmes de sécurité tels que le piratage et l'envoi ou la réception de messages non sollicités.
- Les mobiblogs¹² sont des blogs (journaux intimes publiés sur Internet) que l'on alimente par l'intermédiaire de son téléphone mobile. Ils facilitent la publication d'informations et de photos par les jeunes mais risquent de mettre en danger leur propre sécurité et celle des autres.
- Le phénomène d'intimidation au moyen de la technologie mobile est de plus en plus préoccupant et ne se limite pas aux smartphones et tablettes, car il existe aujourd'hui des montres connectées sur lesquelles les applications des réseaux sociaux sont préinstallées.
- La fonction « appareil photo » des téléphones portables et l'accès facile à Internet depuis ces appareils peuvent être une menace pour la vie privée : on note chez les jeunes une tendance préoccupante à prendre et à publier en ligne des photos compromettantes (par exemple, d'autres jeunes dans les vestiaires des gymnases ou dans des situations embarrassantes, d'enseignants en classe, etc.), parfois retouchées.
- Coût des téléphones portables : les enfants n'ont souvent pas conscience du coût élevé de certains services comme le vote en ligne, les SMS surtaxés non sollicités, ou encore les achats intégrés aux applications.
- Les téléphones portables peuvent distraire et poser un risque pour les conducteurs et même pour les piétons, comme cela a été vu récemment. Tant de gens marchent en écrivant qu'il existe même

9. <https://goo.gl/4LQveU>

10. <https://goo.gl/8a7Dx7>

11. <https://fr.wikipedia.org/wiki/Bluetooth>

12. <https://fr.wikipedia.org/wiki/Moblog>

désormais des applications, disponibles sur Apple¹³ ou Android¹⁴, qui vous permettent de voir le sol lorsque vous envoyez un message et ne regardez pas où vous mettez les pieds.

- Les virus¹⁵ infectent les téléphones portables depuis qu'ils sont devenus des objets de la vie courante, en 2004. F-Secure estime qu'il existe des centaines de virus pour mobiles, toujours plus nombreux et divers. Les menaces les plus récentes sont présentées dans l'onglet « threat description »¹⁶.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- L'Internet nomade n'est pas sans risques car de nombreuses personnes ne pensent pas à régler leurs paramètres de confidentialité à un niveau adéquat. La facilité d'utilisation et la multiplication du nombre d'appareils par utilisateur augmentent la probabilité d'intrusion.
- De nombreux utilisateurs profitent de la connectivité sans fil gratuite dans les cafés, restaurants et autres lieux accessibles au public et communiquent des informations personnelles et financières dans ces environnements.
- Internet étant présent partout, tout le temps, il n'y a pas de période de latence qui permet de réfléchir aux informations que l'on envoie ou que l'on publie sur la toile ou aux achats et autres activités que l'on effectue en ligne. Vu le grand nombre d'applications qui permettent de diffuser des événements en direct, votre enfant pourrait très bien se retrouver à diffuser une scène gênante ou violente qui se déroulerait devant ses yeux sans avoir le temps de se demander si l'enregistrement ou la mise en ligne de ce contenu serait une bonne chose ou non.
- Compte tenu de la facilité avec laquelle même de très jeunes enfants peuvent effectuer des achats par l'intermédiaire d'appareils portables, les spécialistes mettent en garde contre une « virtualisation » de l'argent qui aurait tendance à faire oublier aux enfants la valeur réelle de celui-ci.



MODE D'EMPLOI

— Les téléphones portables sont des produits grand public et il est facile et relativement peu coûteux d'en acquérir un. Lorsque vous achetez un appareil mobile, vous pouvez opter pour une solution prépayée vous donnant un crédit de communication ou souscrire un abonnement mensuel auprès d'un opérateur de téléphonie pour bénéficier des services.

— Les appareils mobiles comme les smartphones, tablettes, liseuses numériques et consoles de jeux portables ne nécessitent qu'une connexion Wi-Fi pour permettre un accès au monde en ligne



SUGGESTIONS D'ACTIVITÉS EN CLASSE

— Les téléphones portables étant extrêmement populaires chez les jeunes, les enseignants peuvent motiver leurs élèves en intégrant l'utilisation de SMS et d'autres fonctionnalités dans les activités pédagogiques. La portabilité des appareils de poche est un atout pour les enseignants lorsqu'ils sont en déplacement et pour les élèves lorsqu'ils travaillent en groupe ou sur le terrain. L'utilisation d'appareils mobiles dans le cadre scolaire et extrascolaire responsabiliserait les élèves vis-à-vis de leur travail. Par ailleurs, ils seraient moins susceptibles de perdre leurs notes et d'oublier leurs devoirs.

13. <https://itunes.apple.com/fr/app/type-n-walk/id331043123?mt=8>

14. <https://play.google.com/store/apps/details?id=com.biztech.typewhilewalk&hl=en>

15. https://fr.wikipedia.org/wiki/Virus_informatique ; https://en.wikipedia.org/wiki/Mobile_virus_and_worms ; https://fr.wikipedia.org/wiki/Ver_informatique

16. https://www.f-secure.com/en/web/labs_global/threat-descriptions

- En voyage d'études, invitez les élèves à enregistrer leurs impressions sur un appareil mobile et à compléter leurs articles à l'aide de photos et de vidéos.
- Invitez les élèves à utiliser plusieurs applications pour présenter leur travail à la maison, par exemple Vine pour de courtes vidéos, Périoscope pour des reportages sur le terrain, ou Twitter et Facebook pour des bulletins d'information.
- Demandez aux élèves de recenser les risques et les difficultés de l'utilisation des smartphones et appareils mobiles en classe. Un cours 100% technologies est-il possible selon eux? Pourquoi ?



BONNES PRATIQUES

- Préférez un téléphone portable à faible rayonnement¹⁷, c'est-à-dire présentant un DAS (débit d'absorption spécifique) « tête » inférieur à 0,56 W/kg et un DAS « corps » inférieur à 0,57 W/kg, ainsi que des oreillettes, les meilleures étant équipées d'un filtre de fréquences.
- Encouragez les jeunes à limiter leur utilisation du téléphone portable et de la tablette. Ne l'interdisez cependant pas. L'utilisation du téléphone portable et des différents services de messagerie est courante chez les adolescents et dans de nombreux cercles, ils sont essentiels pour établir des liens avec les autres.
- Désactivez le Bluetooth s'il ne sert pas, afin d'éviter les problèmes de sécurité.
- Comme pour le courrier électronique, n'acceptez que des données provenant de sources fiables. Prémunissez-vous contre le spam par SMS en ne donnant votre numéro de téléphone portable qu'à des personnes que vous connaissez bien.
- Avant de publier des images, assurez-vous qu'elles ne portent pas atteinte aux droits d'autrui tels qu'ils sont prévus par la loi.
- Parlez à vos enfants des échanges de contenus préjudiciables et soulignez qu'ils pourraient être contraires aux lois nationales de protection de l'enfance.
- Soyez discrets dans votre utilisation du téléphone et de la tablette. Les personnes qui vous entourent n'ont pas forcément envie d'entendre votre conversation.
- Si vous êtes importunés par des appels ou des SMS non sollicités, contactez votre opérateur de téléphonie mobile ou la ligne d'assistance Insafe de votre pays¹⁸.
- De nombreux téléphones portables ont une option de filtrage : utilisez une liste noire pour bloquer les numéros indésirables ou une liste blanche pour n'accepter que certains numéros prédéfinis (seuls ceux du répertoire, par exemple). Il est également possible de télécharger des filtres de contrôle parental sur Internet (logiciels gratuits) ou d'en acheter auprès de votre opérateur de téléphonie mobile.
- N'oubliez pas que les téléphones portables ne sont pas les seuls appareils de communication : les tablettes et les montres connectées comportent également des fonctionnalités de messagerie et d'appel.
- Pour les enfants les plus jeunes, ou les adolescents qui ne savent pas encore gérer leur budget de manière responsable, choisissez une formule « prépayée » plutôt qu'un abonnement mensuel pour éviter les mauvaises surprises. Discutez avec eux de leur consommation et veillez à ce qu'ils comprennent la valeur réelle de l'argent.
- N'oubliez pas de configurer le smartphone de votre enfant à l'achat. La plupart des appareils sont équipés de toutes les fonctionnalités (appareil photo, GPS, communication en champ proche (CCP), Bluetooth, etc.) et sont configurés par défaut pour des adultes. N'hésitez pas à rechercher des guides en ligne pour savoir comment paramétrer le téléphone de votre

17. <http://www.phonerated.com/top-rated-best-overall-low-sar-phones-global>

18. http://www.saferinternet.org/ww/en/pub/insafe/focus/national_helpines.htm

enfant. Il est notamment recommandé de lui créer un compte spécifique, protégé par un mot de passe, de désactiver les achats intégrés aux applications, l'installation de nouvelles applications (pour les plus jeunes), la géolocalisation et l'utilisation du GPS, et d'installer un logiciel de contrôle parental.

- Sachez que le mot de passe que vous saisissez pour effectuer un achat en ligne sur un appareil mobile peut rester actif encore pendant 15 minutes après la transaction et rendre possible un autre achat ¹⁹.



INFORMATIONS COMPLÉMENTAIRES

- Rapport du GSMA pour mieux comprendre l'économie du mobile : http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.
- Infographies présentant le paysage social, numérique et mobile en Europe en 2014 : <http://web.archive.org/web/20151211195326/http://wearesocial.net/blog/2014/02/socialdigital-mobile-europe-2014/>.
- S212, site britannique indépendant d'évaluation des téléphones mobiles et autres appareils portables : <http://www.s21.com/mobile-phones.htm>.
- Rapport publié par l'UNESCO sur « l'avenir de l'apprentissage mobile : implications pour la planification et la formulation des politiques » : <http://unesdoc.unesco.org/images/0021/002196/219637E.pdf>.
- « Children and mobile phones, an agenda for action », publication en ligne de Childnet International : http://www.childnet.com/ufiles/CMPAAA_A4.pdf.
- Le British Board of Film Classification a succédé à l'Independent Mobile Classification Body (IMCB) pour fournir le cadre indépendant à la base du code de pratique des opérateurs mobiles : <http://www.bbfc.co.uk/what-classification/mobile-content>.
- Pour en savoir plus sur le fonctionnement du Bluetooth et les moyens de le protéger : <http://web.archive.org/web/20160407133222/http://electronics.howstuffworks.com/bluetooth4.htm>.
- L'opérateur de téléphonie mobile Vodafone a rédigé un guide à l'intention des parents : <https://www.vodafone.com/content/parents/howto-guides.html>.

19. <http://www.creditcards.com/credit-card-news/whos-responsible-kids-unauthorized-charges-1279.php>

2. Internet – Mise en relation des personnes et des idées

” « Finalement, tout est lié – les gens, les idées, les objets. La qualité du lien est la clé de la qualité en tant que telle ».

Charles Eames, designer du début du XXe siècle

LISTE DE POINTS À VÉRIFIER :

6. COURRIER ÉLECTRONIQUE ET COMMUNICATION

Avez-vous créé plusieurs comptes de messagerie électronique et défini des mots de passe différents pour chacun d'entre eux ?

Votre mot de passe est-il assez fiable (plus de 8 caractères et associant lettres, chiffres et symboles) ?

Indiquez-vous clairement l'objet de vos courriers électroniques à l'aide de mots-clés pertinents dans la ligne prévue à cet effet ?

Avez-vous prévu une authentification à deux facteurs sur vos comptes de courrier électronique (question de sécurité subsidiaire et/ou numéro de téléphone portable) ?

7. SALONS DE DISCUSSION (DIALOGUE EN LIGNE OU CHAT) ET MESSAGERIE INSTANTANÉE

Vos coordonnées figurent-elles dans votre site web ou blog ?

Avez-vous pris des mesures pour protéger votre vie privée en ligne ?

Vous êtes-vous assuré que le contenu que vous utilisez pour votre site web/blog respecte la législation relative au droit d'auteur ?

8. RÉSEAUX SOCIAUX ET PARTAGE SOCIAL

Nous n'avons qu'une réputation : réfléchissez-vous systématiquement avant de publier quelque chose en ligne ?

Quand avez-vous mis à jour pour la dernière fois vos paramètres de confidentialité sur les sites que vous utilisez ?

La démocratie repose sur la participation du plus grand nombre possible de citoyens au débat public : avez-vous essayé de faire entendre votre voix par le biais des sites de réseautage social qui le permettent ?

9. PROTECTION DE LA VIE PRIVÉE ET PARAMÈTRES DE CONFIDENTIALITÉ

Avant de publier une photo sur les réseaux sociaux, vous demandez-vous s'il est vraiment nécessaire de le faire et d'identifier les personnes qui y apparaissent ?

Lisez-vous les conditions générales d'utilisation des applications mobiles pour comprendre ce qui est « à vous » et ce qui est « à eux » dans tout ce que vous partagez ?

Lorsque vous installez une application, êtes-vous sûrs de savoir exactement à quelles informations privées elles auront accès ? Cet accès est-il véritablement nécessaire au bon fonctionnement de l'application ?

Savez-vous quel est l'impact du Règlement général de l'Union européenne sur la protection de vos données ?

Courrier électronique et communication



Le courrier électronique¹, (e-mail) est un outil qui permet d'envoyer des messages entre plusieurs ordinateurs connectés à un réseau comme Internet. Ce terme désigne également le message lui-même (abrégé « courriel »). Il ne faut en général que quelques secondes pour transférer un courrier électronique. Le destinataire peut en prendre connaissance et y répondre quand il le souhaite. D'une utilisation souple et efficace, le courrier électronique a radicalement changé la manière dont nous travaillons et communiquons. Des milliards de messages sont envoyés chaque jour.

— Une adresse de messagerie électronique se compose de deux parties : un nom local et un nom de domaine, séparés par le signe « @ ». Le nom local est souvent, mais pas toujours, le nom de l'utilisateur, tandis que le nom de domaine correspond à l'organisation, à la société ou au fournisseur d'accès Internet de celui-ci. Le nom de domaine peut également désigner le type d'organisation et/ou le pays. Par exemple, name@ox.ac.uk est l'adresse d'une personne qui travaille ou étudie à l'Université d'Oxford.

1. https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique

— Les comptes de courrier électronique restent au cœur de l'expérience utilisateur car ils sont souvent demandés pour pouvoir s'inscrire à des sites et participer en ligne. Par conséquent, bien qu'il existe aujourd'hui de nombreux autres moyens de communication dont certains peuvent être préférés aux emails (réseaux sociaux, messagerie instantanée, etc.), les adresses électroniques sont devenues un aspect essentiel de l'identité en ligne des Internaute et leur servent souvent d'identifiant pour se connecter à l'ensemble des services en ligne qu'ils utilisent.



INTÉRÊT PÉDAGOGIQUE

— Les adresses de courrier électronique étant souvent demandées en ligne, apprendre à bien gérer un compte de courrier électronique a des vertus pédagogiques, comme apprendre à trier du courrier physique en séparant le contenu personnel du contenu administratif important pour pouvoir le retrouver facilement.

— Le courrier électronique est également un outil précieux dans les projets interculturels entre élèves de pays différents. Il peut être utilisé pour l'amélioration de leurs connaissances en langues et le partage d'informations sur leurs cultures respectives.

— Certains élèves plus réservés s'expriment mieux par le courrier électronique que dans une discussion en classe face à d'autres élèves



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Votre adresse email étant la porte d'entrée à tous vos comptes en ligne, le piratage de votre compte de courrier électronique peut avoir des conséquences très graves.
- La plupart des clients de messagerie (programmes informatiques utilisés pour accéder au courrier électronique² d'un utilisateur et le gérer) que l'on trouve en ligne sont gratuits, mais nombre d'entre eux utilisent des algorithmes pour analyser le contenu de vos messages et afficher de la publicité ciblée sur la page d'accueil de votre messagerie web.
- Il est difficile d'exprimer des émotions dans un courrier électronique. C'est pourquoi il faut toujours veiller à rédiger vos messages avec soin pour vous assurer qu'ils ne seront pas mal compris. Les « émoticônes »³, petites icônes expressives dont font partie les smileys, peuvent vous aider à préciser vos intentions, et en particulier à exprimer l'ironie ou l'humour. Utilisez-les toutefois avec parcimonie pour ne pas détourner l'attention du destinataire de votre message.
- Un pourcentage important des courriers électroniques reçus sont des messages non sollicités et sont en général des spams indésirables⁴ (voir Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité). Heureusement, les filtres antispam sont de plus en plus efficaces pour distinguer ce type de messages des courriers électroniques normaux.
- Veillez à ne pas contribuer vous-même à la diffusion de ces messages indésirables en transférant à tout va des courriers électroniques que vous trouvez « amusants » ou « intéressants » à l'ensemble de vos contacts. Si vous le faites trop souvent, les filtres antispam risquent d'identifier votre adresse de courrier électronique comme un proxy de spam et de la bloquer, empêchant ainsi tout contact avec quelqu'un d'autre.
- Certains courriers transférés sont faux ou frauduleux, par exemple, ceux qui prétendent qu'une société ou organisation s'est engagée à verser une somme d'argent donnée pour une cause humanitaire (souvent, un enfant malade ayant besoin d'une intervention chirurgicale) à chaque transfert du message.

2. https://fr.wikipedia.org/wiki/Client_de_messagerie

3. <https://fr.wikipedia.org/wiki/%C3%89motic%C3%B4ne>

4. https://en.wikipedia.org/wiki/Email_spam

- Il est très facile de masquer un nom pour tromper le destinataire. Il suffit par exemple de le modifier dans les paramètres ou de créer une adresse électronique anonyme de type *elvispresley@hotmail.com* dans une messagerie Internet. Même si vous reconnaissez l'adresse électronique comme étant celle d'un de vos contacts, vérifiez également la ligne « objet » du message car il est possible que l'ordinateur de l'expéditeur soit devenu une « machine zombie »⁵ détournée par un pirate ou infectée par un virus.
- Un lien peut sembler vous rediriger vers un site web alors qu'il vous conduit en fait à un autre. Cette technique est particulièrement courante dans les attaques d'hameçonnage (*phishing*)⁶.



BONNES PRATIQUES

- Créez plusieurs comptes de courrier électronique à des fins différentes (inscription sur des sites de réseaux sociaux, achat de produits en ligne, etc.). Conservez-en un que vous garderez aussi privé que possible en ne publiant pas son adresse sur le Web et en ne l'utilisant que pour les services importants que vous et vos amis utilisez. Réservez-en un autre pour vous inscrire à des services que vous pourriez n'utiliser qu'une fois, ou que vous n'utilisez que rarement.
- Veillez à rédiger des messages aussi concis que possible. Essayez d'éviter les paragraphes trop volumineux. Vérifiez l'orthographe.
- Pensez à bien indiquer le but de votre message à l'aide de mots-clés pertinents dans la ligne « objet ». Cela permet au destinataire d'une part, de voir qu'il s'agit d'un message authentique et d'autre part, de le retrouver plus facilement par la suite.
- Créez des mots de passe sécurisés pour vos comptes de courrier électronique (plus de 8 caractères, associant lettres, chiffres et symboles) et utilisez des mots de passe différents pour chaque compte.
- Restez raisonnable quant au volume de courrier électronique que vous envoyez et faites preuve d'intelligence et de stratégie dans le choix de vos outils de communication. Une conférence téléphonique ou une discussion sur un forum privé seront peut-être plus adaptées à des échanges privés avec un grand nombre de personnes qu'une masse de courriels.
- Abstenez-vous de vérifier votre messagerie électronique toutes les dix minutes. De nombreuses personnes se laissent interrompre en permanence par les courriels.
- De manière générale, ne transmettez jamais des informations sensibles comme vos coordonnées bancaires par courrier électronique. Vous n'aurez à le faire qu'en de rares occasions, par exemple pour réserver une chambre d'hôtel. En cas de doute, agissez avec précaution, vérifiez la réputation en ligne du service que vous souhaitez utiliser et la marche à suivre pour supprimer la carte ou annuler la transaction et préférez des services de paiement comme PayPal aux services moins sécurisés comme les services de transfert direct d'argent (par exemple Western Union). Cela dit, n'envoyez jamais par courriel des informations confidentielles telles que les identifiants et mots de passe de vos comptes en ligne. Les services en ligne ne vous les demanderont jamais. Si vous recevez un courrier électronique sollicitant ces données, il s'agit d'une tentative d'hameçonnage.
- Des stratégies de hameçonnage sont de plus en plus sournoises font leur apparition, dont certaines consistent à vous envoyer de faux courriels de notification qui imitent parfaitement les messages que vous recevez des services que vous utilisez (par exemple, les sites de réseautage social) et vous dirigent vers un faux site web vous demandant vos données de connexion. Pensez à vérifier systématiquement l'adresse de courrier électronique de l'expéditeur du message et l'adresse du site web donné en lien au cas où quelque chose vous paraîtrait suspect.

5. https://fr.wikipedia.org/wiki/Machine_zombie

6. <https://fr.wikipedia.org/wiki/Hame%C3%A7onnage>

- Conservez une saine méfiance par rapport au courrier électronique que vous recevez. N'ouvrez pas un message dont la source ne vous semble pas fiable.
- Soyez particulièrement attentifs aux pièces jointes. Si vous n'attendiez pas une pièce jointe de l'expéditeur du message ou si elle ne vous semble pas fiable pour toute autre raison, supprimez-la sans l'ouvrir. Même les pièces jointes reçues d'expéditeurs connus et dignes de confiance devraient d'abord être enregistrées puis analysées au moyen d'un antivirus avant d'être ouvertes.
- Faites usage de toutes les fonctionnalités de sécurité proposées par votre client de messagerie. De manière générale, il vous propose de fournir une deuxième adresse de courrier électronique au cas où votre compte serait victime de piratage et de plus en plus, de donner également votre numéro de téléphone portable pour des vérifications de sécurité plus poussées dans des cas exceptionnels. Configurez correctement les paramètres de sécurité de votre compte de manière à ce que vous puissiez plus facilement le récupérer s'il venait à être piraté.
- Consultez la Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité pour des conseils supplémentaires concernant le courrier électronique.



MODE D'EMPLOI

- Pour consulter vos courriers électroniques, vous pouvez utiliser l'application « officielle » de votre service de courrier électronique sur votre smartphone, votre tablette ou votre ordinateur fonctionnant sous Windows 8 ou version ultérieure (par exemple l'application Gmail, Outlook ou Yahoo!), aller directement sur son site web (en utilisant un service de messagerie web) ou utiliser un client de messagerie, application externe qui télécharge les courriers électroniques depuis votre service de courrier électronique et vous permet de les gérer et de les organiser. L'avantage de cette dernière solution est qu'elle permet de regrouper et de consulter en un même endroit tous vos courriels, téléchargés depuis plusieurs services différents. Les clients de messagerie les plus courants sont Thunderbird et Outlook. Le plus souvent, ils sont utilisés pour les courriels professionnels.
- Pour plus d'informations sur la mise en place d'un filtre antispam, voir la Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Demandez à vos élèves les plus âgés qui disposent d'une adresse e-mail, de se connecter à leur service de courrier électronique et d'aller dans les paramètres de sécurité pour sécuriser leur compte en ajoutant une question de sécurité, une deuxième adresse email ou un numéro de téléphone portable.
- Voici les procédures à suivre pour sécuriser votre compte de courrier électronique sur Gmail, Yahoo! et Outlook.
 - ▶ <<https://support.google.com/accounts/answer/46526?hl=fr>>
 - ▶ <<https://support.microsoft.com/fr-fr/help/12410/microsoft-account-help-protect-account>>
 - ▶ <<https://fr.aide.yahoo.com/kb/account/Sécurisez-votre-compte-Yahoo-sln2080.html>>
- Pourquoi insister sur ces trois grands en particulier, alors qu'il existe de nombreux autres services de courrier électronique ? Pour la raison qu'ils sont, du moins pour Gmail et Outlook/Hotmail, liés à de nombreux autres services. Ainsi, un compte Google est quasiment indispensable lorsque l'on possède un smartphone fonctionnant sous Android et le compte Outlook est souvent relié au système d'exploitation Windows. Cela signifie qu'indépendamment de vos préférences, vous pourriez être « contraint » de créer un compte de courrier électronique

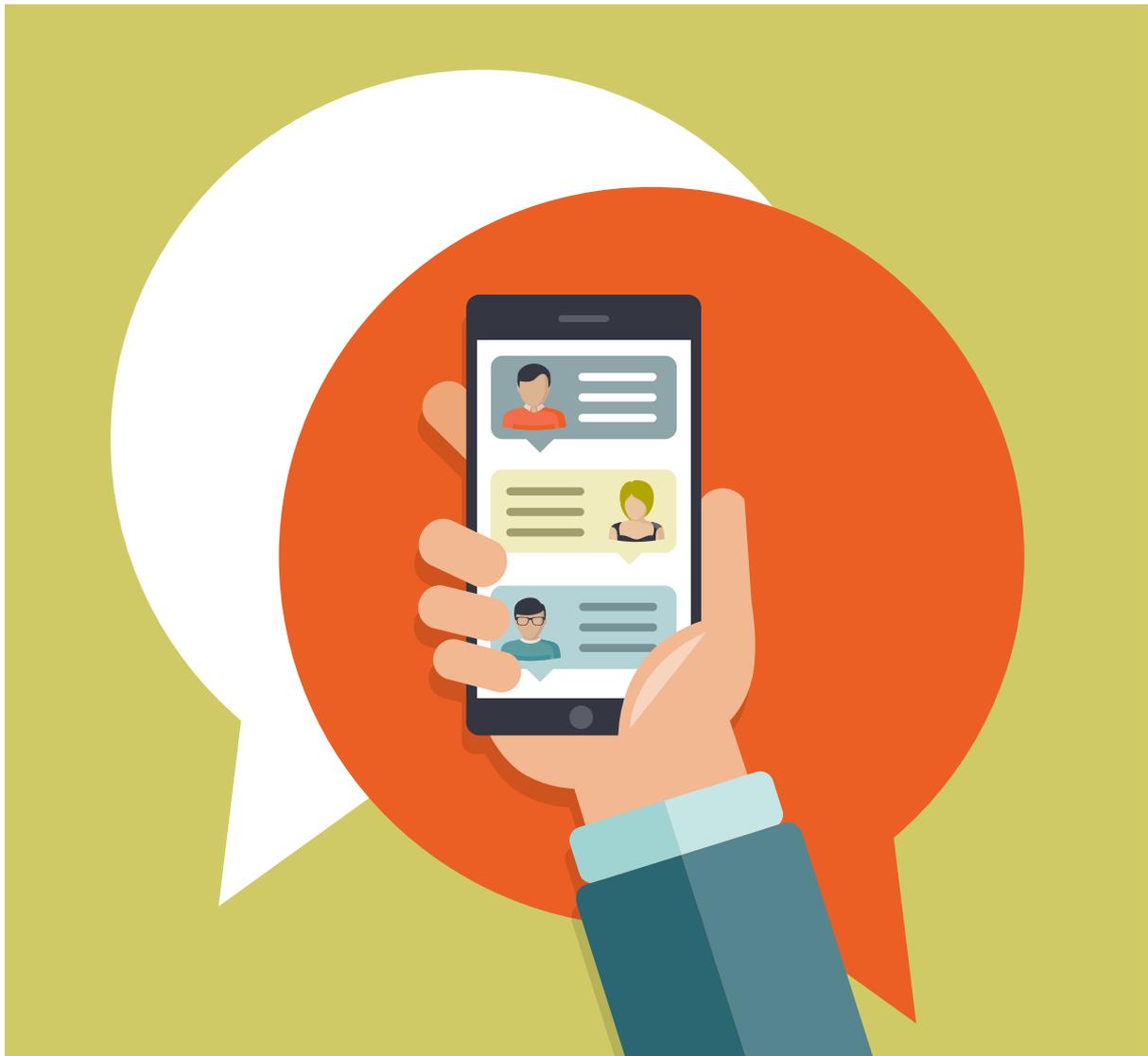
sur l'un de ces services. Vous êtes bien entendu libre d'utiliser des clients de messagerie proposant des paramètres de confidentialité plus stricts comme Web.de ou Protonmail.com. En général, les fournisseurs d'accès à Internet proposent eux aussi un service de courrier électronique. D'autres solutions peuvent également être trouvées en ligne.

- Invitez vos élèves à travailler par groupes de trois ou plus et demandez-leur d'imaginer des mots de passe fiables pour un compte de courrier électronique factice. Précisez bien qu'il s'agit d'en trouver de nouveaux et non de divulguer leurs mots de passe personnels ! Après 10 minutes de recherche d'idées, demandez aux équipes de présenter leur mot de passe en précisant pourquoi elles pensent qu'il est sécurisé. Aidez-les à définir les caractéristiques d'un mot de passe sûr (plus de 8 caractères, associant chiffres, lettres et symboles) et les défauts habituels des mots de passe peu robustes (mots se trouvant dans un dictionnaire, ayant un lien direct avec vous comme votre nom de famille, le nom de votre chien, etc.)

INFORMATIONS COMPLÉMENTAIRES

- Des exemples bien connus de clients de messagerie sont Microsoft Outlook <<https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook>> et Mozilla Thunderbird <<http://www.mozilla.org/projects/thunderbird/>>.
- Truth or Fiction est un site web permettant aux Internaute de vérifier la véracité des courriers électroniques couramment transférés : <<http://www.truthorfiction.com/>>. Un autre site similaire : <<http://m.snopes.com/whats-new/>>.
- Trois des principaux sites de messagerie web sont Outlook <<https://office.live.com/start/Outlook.aspx>>, Yahoo! <<https://mail.yahoo.com>> et Gmail de Google <<http://www.gmail.com>>. Vous pouvez également chercher vous-mêmes d'autres prestataires de courrier électronique, dans votre pays.
- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :
Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.
Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile.

Salons de discussion (dialogue en ligne ou *chat*) et messagerie instantanée



■ « Dialogue en ligne » (chat) est un terme générique qui désigne une communication interactive sur un canal de discussion spécifique. Les utilisateurs peuvent échanger avec des groupes de personnes sur des salons de discussion (*chatroom*)¹ ou tenir des conversations privées avec des amis au moyen de services de messagerie instantanée².

■ Le chat est un moyen de communication très informel, analogue aux conversations en face à face entre deux ou plusieurs personnes. Les discussions se font généralement à l'écrit mais peuvent être enrichies par du *streaming* audio ou vidéo³ grâce à l'utilisation de casques ou de webcams. Cette forme de communication est instantanée et diffère donc du courrier électronique qui ne requiert pas la présence simultanée du destinataire et de l'expéditeur.

1. https://fr.wikipedia.org/wiki/Salon_de_discussion

2. https://fr.wikipedia.org/wiki/Messagerie_instantan%C3%A9e

3. <https://fr.wikipedia.org/wiki/Streaming>

Différences entre *chat* et messagerie instantanée

■ Ces termes sont utilisés de manière interchangeable ; cela dit, si un utilisateur peut dialoguer en ligne au moyen de services de messagerie instantanée, l'envoi d'un message instantané n'est pas un *chat*. Après avoir été très à la mode, le *chat* semble avoir perdu du terrain au profit de la messagerie instantanée et des autres types de messageries. De nombreuses entreprises voient ces applications d'un mauvais œil car le fait que les employés soient constamment interrompus par des messages lorsqu'ils travaillent a tendance à faire baisser leur productivité.

Quels sont les autres types de médias de messagerie ?

■ Les applications de messagerie comme WhatsApp, Kik, Viber, Telegram ou iMessage sont de plus en plus utilisées par les propriétaires de smartphones. Les applications à auto-effacement telles que Snapchat et Wickr rencontrent également un grand succès. Ces outils sont généralement gratuits et semblent offrir davantage « d'intimité » que ceux de plus grandes plateformes comme Facebook, Twitter ou LinkedIn.

■ Du fait de l'accès rapide à ces applications sur smartphones, les utilisateurs ont tendance à filmer, commenter, prendre des photos et les envoyer avant même de réfléchir aux conséquences que cela pourrait avoir. C'est pourquoi elles ont été citées dans l'augmentation des cas de harcèlement et d'intimidation en ligne.

■ Le développement de la messagerie instantanée et des autres types de médias de messagerie se poursuivra incontestablement avec l'entrée des smartphones sur de nouveaux marchés. Facebook a ainsi fait l'acquisition de WhatsApp, la société japonaise Rakuten a racheté Viber et de nombreux autres acteurs du secteur ont investi dans des applications de ce type. Le message est on ne peut plus clair : les médias de messagerie ont encore de beaux jours devant eux.

Importance de la compréhension du chat et de la messagerie instantanée

■ Le *chat* et la messagerie instantanée sont des passe-temps très prisés qui transforment la manière dont les jeunes communiquent entre eux. Ils trouvent des applications utiles lorsqu'ils permettent aux élèves d'échanger des idées et de parler de leurs devoirs et d'autres projets scolaires, mais ils sont malheureusement aussi le cadre de manœuvres de harcèlement ou de cyberintimidation (voir Fiche d'information 21 sur l'intimidation et le harcèlement).

■ Les enseignants sous-estiment souvent l'importance du *chat* dans la vie des élèves et peuvent laisser passer l'occasion de s'en servir comme outil pédagogique. Pourtant, les possibilités d'utilisation ne manquent pas ; en voici quelques exemples :

- séances de remue-méninges et discussions en temps réel sur des problèmes
- jeux de rôle et simulations
- échange d'opinions et débats, discussions en petits groupes
- tutorat et conseils
- recherches en groupe
- création d'une communauté en ligne.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Le chat peut facilement provoquer des malentendus car les signaux sociaux, les gestes et la communication non verbale ne peuvent être transmis à l'écrit. Il est demandé à chacun d'agir avec autant de courtoisie que dans les situations de la vie réelle et de prendre l'habitude de respecter les règles de la netiquette⁴. L'humour et les émotions peuvent également s'exprimer en utilisant des émoticônes⁵, combinaisons de symboles tournés à 90° pour représenter des visages. La plupart des jeunes utilisent des abréviations ou des acronymes : on trouvera les plus courants, regroupés dans un dictionnaire, à l'adresse <<http://www.netlingo.com/acronyms.php>>.

4. <https://fr.wikipedia.org/wiki/N%C3%A9tiquette>

5. <https://fr.wikipedia.org/wiki/%C3%89mot%C3%B4ne>

- Lorsque vous dialoguez en ligne avec des inconnus sur le Web, gardez toujours à l'esprit que les personnes ne sont pas toujours ce qu'elles prétendent être. Les salons de discussion fermés des logiciels de groupe⁶ qui sont utilisés en milieu scolaire et permettent la tenue de conférences sont plus sûrs car l'accès est limité à un groupe d'utilisateurs bien défini.
- Le temps passé à dialoguer en ligne ou à envoyer des messages instantanés a considérablement augmenté, les adolescents envoyant chaque jour des centaines de messages sous différentes formes (textes, messages instantanés, dialogue en ligne, courriels, etc.). Bien que l'ergonomie des claviers et souris d'ordinateurs se soit largement améliorée, de nouveaux syndromes comme la tendinite du pouce ont fait leur apparition chez les jeunes. Les smartphones sont des appareils relativement récents et l'envoi de messages ou la rédaction de longs courriels peuvent donner lieu à une utilisation excessive du pouce. Limiter le *chat* et l'envoi de textos n'est donc pas qu'une question d'équilibre de vie, mais également de santé.
- Il ne faut pas oublier que malgré leur apparente gratuité, les applications de messagerie instantanée sont gérées par des sociétés qui doivent, d'une manière ou d'une autre, couvrir leurs charges d'exploitation. Nombre d'entre elles optent donc pour une stratégie consistant à créer une base d'utilisateurs grâce à une application gratuite, pour la revendre à une autre société dès qu'elle atteint une certaine taille. Tel a été le cas de Whatsapp qui a été racheté par Facebook. D'autres applications, comme Snapchat, constituent d'abord leur base d'utilisateurs avant de commencer à introduire de la publicité. Soyez toujours conscient du modèle économique du service de messagerie instantanée que vous utilisez et faites des choix éclairés, en tenant compte des avantages et des inconvénients de chacun (vie privée moins protégée, contrôle de vos données, exposition à la publicité, cotisation annuelle/mensuelle, etc.).
- Les échanges de fichiers entre utilisateurs par le biais de la messagerie et du chat sont courants mais il existe toujours un risque que ces fichiers contiennent des logiciels malveillants. Assurez-vous que tous les fichiers ont été analysés par un antivirus avant de les partager et vérifiez toute pièce que vous recevez avant de l'ouvrir (voir Fiche d'information 19 sur la sécurité).
- Il y a eu beaucoup de publicité négative quant aux risques que courraient les jeunes qui utilisent des salons de discussion en ligne. Quelques affaires criminelles très médiatisées ont fait craindre aux parents et aux enseignants que des pédophiles puissent, par ce biais, entrer en contact avec les enfants, notamment sur les jeux en ligne (voir Fiche d'information 6 sur les jeux). Bien que ces dangers existent, il est important de les relativiser. Une grande majorité d'utilisateurs des salons de discussions se présentent tels qu'ils sont dans la réalité et la plupart des communications par chat sont sans danger. Plutôt que de faire peur ou d'interdire l'utilisation du chat, les adultes devraient autonomiser les jeunes et les inviter à respecter les quelques règles de sécurité suivantes :
 - ▶ Choisir un espace de discussion adapté à son âge et suivi par un modérateur en direct, auquel on signalera tout incident ;
 - ▶ Choisir un nom d'utilisateur ne révélant pas si l'on est un garçon ou une fille et ne jamais donner d'informations personnelles, ni publier de photos de soi-même (voir Fiche d'information 9 sur la protection de la vie privée).
 - ▶ Avant de retrouver dans la vie réelle un ami d'un salon de discussion, en parler d'abord à ses parents et se faire accompagner par un adulte de confiance. Donner toujours rendez-vous dans un lieu public, par exemple un parc, lors de la première rencontre physique avec quelqu'un que l'on aura appris à connaître en ligne.
 - ▶ Confier à un adulte tout ce qui aurait pu les mettre mal à l'aise lors d'une session de chat. En cas de problème dans un salon de discussion ou ailleurs sur Internet, il reste toujours la possibilité d'en parler à des conseillers expérimentés du service national d'assistance⁷.
 - ▶ Pour discuter en ligne avec des personnes connues, préférer la messagerie instantanée (par exemple MSN, Skype) aux salons de discussion pour pouvoir contrôler sa liste de contact.

6. <https://fr.wikipedia.org/wiki/Groupware>

7. www.betterinternetforkids.eu/web/portal/practice/helplines



MODE D'EMPLOI

- Il existe différents types de programmes de chat gratuits sur le Web. Vous les trouverez en tapant « chat » dans n'importe quel moteur de recherche⁸. Nombre d'entre eux, comme Yahoo Chat⁹, ICQ¹⁰ et AOL Chat, proposent un accès à divers salons avec des groupes de discussion en temps réel. Bien souvent, il faut commencer par télécharger une petite application pour activer le *chat* et s'enregistrer auprès du modérateur avant de pouvoir se connecter et participer librement aux discussions.
- Les applications de messagerie instantanée¹¹, qui permettent aux utilisateurs d'avoir des conversations privées avec des interlocuteurs qu'ils ont sélectionnés, rencontrent aujourd'hui un plus grand succès que les salons de discussion. On trouvera ces applications en tapant « messagerie instantanée » sur un moteur de recherche. Les utilisateurs téléchargent une application de messagerie instantanée puis établissent une liste de personnes avec lesquelles elles souhaitent discuter. La communication ayant lieu entre utilisateurs d'un même groupe restreint, la messagerie instantanée est souvent considérée comme plus « sûre » que les échanges dans les salons de discussion.

Comment utiliser un salon de discussion ?

- Ouvrez le programme de chat que vous avez choisi d'utiliser.
- Fournissez un nom d'utilisateur et un mot de passe, si nécessaire.
- Choisissez le salon de discussion qui vous convient, modéré par une personne physique. Il en existe sur différents thèmes et centres d'intérêt, par exemple l'automobile ou d'autres sujets d'étude, mais aussi pour les enseignants, etc.
- Une fois connecté, vous verrez les conversations des participants défiler sur l'écran de texte principal.
- Saisissez votre message puis appuyez sur « entrée » ou cliquez sur « envoyer » pour que votre message soit visible par les autres utilisateurs du salon de discussion.
- Si vous souhaitez envoyer un message à une personne en particulier, sélectionnez-la dans la liste de participants que vous trouverez dans la fenêtre.
- De nombreux salons de discussion peuvent également être utilisés pour la transmission de fichiers de pair à pair¹² ou l'échange de fichiers trop volumineux pour être envoyés par courrier électronique¹³.
- Vérifiez toujours vos paramètres pour ne pas ajouter par inadvertance des utilisateurs non souhaités à votre espace de discussion.

Comment utiliser la messagerie instantanée ?

- Ouvrez votre application de messagerie instantanée¹⁴.
- Consultez votre liste de contacts pour savoir qui est en ligne et disponible pour discuter.
- Vous pouvez ajouter un nouveau contact en saisissant son adresse de courrier électronique pour lui envoyer un message l'invitant à se joindre à votre groupe. S'il accepte votre invitation, il sera enregistré dans votre liste. Vous pourrez ainsi discuter avec lui en temps réel lorsque vous serez tous les deux en ligne.
- Cliquez sur le nom d'utilisateur de la personne choisie pour lui envoyer un message et ouvrez un dialogue pour entrer en communication avec elle.
- Saisissez votre message et appuyez sur « entrée » ou cliquez sur « envoyer » pour que votre message soit visible par les autres utilisateurs de la messagerie instantanée.
- Il est préférable de ne pas engager la discussion avec des utilisateurs inconnus ou de répondre à un courrier électronique ou à un message instantané provenant de personnes que vous ne connaissez pas.

8. https://fr.wikipedia.org/wiki/Moteur_de_recherche

9. <http://chat.yahoo.com>

10. <http://www.icq.com/>

11. <http://lifestream.aol.com>

12. https://fr.wikipedia.org/wiki/Pair_%C3%A0_pair

13. https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique

14. https://fr.wikipedia.org/wiki/Messagerie_instantan%C3%A9e

- Vérifiez toujours vos paramètres pour ne pas ajouter par inadvertance des utilisateurs non souhaités à votre messagerie instantanée.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Choisissez un sujet et invitez les élèves à se poser mutuellement des questions et à échanger des informations dans un salon de discussion.
- Choisissez un sujet d'étude. Rassemblez quelques éléments pour aider les élèves dans leur travail de préparation au cours. Confiez-leur des tâches à réaliser en binômes ou en petits groupes. Cette phase sera organisée sur le modèle d'un groupe de recherche (le chat fonctionne le mieux lorsque les interactions ont lieu au sein de petits groupes de 2 à 6 élèves).
- À la fin du projet, les élèves préparent des présentations adaptées à une session de discussion. Le dialogue en ligne commence par des présentations en petits groupes des différents sujets d'étude. Tous les participants résument ensuite ce qu'ils ont appris lors du cours.
- Les sessions de dialogue en ligne étant analogues aux conversations qui ont lieu dans la vie réelle, elles offrent aux élèves de véritables possibilités d'interaction et peuvent donc être utiles dans l'apprentissage des langues étrangères. L'enseignant peut encourager les élèves à participer à la discussion, de préférence à l'aide de courts messages. L'interactivité peut être renforcée en attribuant des rôles aux élèves ; l'un peut être un innovateur, l'autre un critique. Le reste de la classe peut suivre les discussions et réagir.
- Environment Online (ENO)¹⁵ est un projet international d'éducation à l'environnement sur le web. Au début du cours, les élèves découvrent leurs sujets sur les pages web du projet. Ils recueillent ensuite des données environnementales scientifiques et empiriques, mesurent divers phénomènes ou prennent des photographies.
- Pendant chaque session à thème, des cours virtuels sont organisés sous la forme de dialogues en ligne en temps réel, interactifs et synchrones¹⁶, de questionnaires électroniques et de forums¹⁷. Avant et après les cours, les élèves échangent des idées, suivent l'évolution de leurs travaux par *chat* et réfléchissent à ce qu'ils ont appris.



BONNES PRATIQUES

— Le langage utilisé dans les salons de discussion est familier, fractionné et associatif. Les participants à un *chat* doivent être rapides et vifs d'esprit pour passer d'un sujet, voire d'une discussion à une autre. Le rôle de l'enseignant est d'assurer la qualité du contenu et une participation équilibrée de tous les intervenants. Plus les élèves sont jeunes, plus il est important que l'échange soit dirigé et modéré par l'enseignant.

- Suivez activement la discussion pendant toute la session.
- Convenez au préalable de la date et de l'heure de la session : tous doivent être présents au même moment.
- Respectez les règles de la netiquette : restez courtois comme si vous étiez face à face.
- N'oubliez pas qu'un message écrit négligemment peut être blessant même si ce n'était pas votre intention.
- Les messages courts sont préférables. Ne monopolisez pas une session de discussion en temps réel en copiant-collant des pans entiers de texte rédigés à l'avance que les autres seront obligés de lire et auxquels il leur faudra répondre.

15. <http://www.enoprogramme.org>

16. <http://www.netlingo.com/word/real-time-chat.php>

17. [https://fr.wikipedia.org/wiki/Forum_\(informatique\)](https://fr.wikipedia.org/wiki/Forum_(informatique))

- Le style du chat est proche du monologue intérieur. Lisez attentivement les messages des autres pour comprendre ce qu'ils veulent dire. Cela implique de savoir lire entre les lignes.
- Ne communiquez jamais votre identifiant ni votre mot de passe. Ne divulguez pas d'informations privées lors des sessions de chat ou de messagerie instantanée. Des captures d'écran de vos informations (ou commentaires) peuvent être faites et partagées avec des tiers.



INFORMATIONS COMPLÉMENTAIRES

- On trouvera quelques idées pour les enseignants à l'adresse : http://www.educationworld.com/a_tech/chat-room-get-new-life-in-classrooms.shtml.
- tChat est un salon de discussion en français : <http://www.tchat-orange.fr/index.php>.
- On trouvera des informations sur le chat comme outil social à l'adresse : <http://www.openp2p.com/lpt/a/3071>.
- Voir Wikipédia pour une liste des émoticônes de base : <https://fr.wikipedia.org/wiki/Émoticône>.
- Le Pew Research Center a étudié la messagerie mobile et les médias sociaux : <http://web.archive.org/web/20160703022409/http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/>.
- « What is snapchat and why do kids love it and parents fear it? » : <http://web.archive.org/web/20160619055301/http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/#65fc2b447875>.
- Au Danemark, Cyberhus utilise les discussions de groupe pour aider les adolescents vulnérables à se sentir mieux et renforcer leur participation à la société : <http://cfdp.dk/2015-cyberhus-chat-counselling-last-year/>.

Réseaux sociaux et partage social



Un service ou site de réseautage social¹ est une plateforme utilisée pour réunir des personnes qui ont des centres d'intérêts ou des activités en commun. Ce système basé sur le web offre aux utilisateurs divers moyens d'entrer en contact, comme le dialogue en ligne, la messagerie instantanée, le courrier électronique, la vidéo, le *chat* vocal, le partage de fichiers, les blogs, les groupes de discussion, etc.

— Les réseaux sociaux s'organisent autour des profils personnels des utilisateurs, qui contiennent des informations essentielles les concernant, ainsi que leurs centres d'intérêt, leurs cercles d'amis, etc. Les sites de réseautage social rassemblent des communautés de personnes qui ont des activités et des centres d'intérêt en commun ou qui souhaitent découvrir ceux d'autres personnes. Ils proposent à leurs utilisateurs plusieurs types de logiciels² à cette fin.

— Les sites de réseautage social permettent aux utilisateurs d'établir des contacts entre eux (généralement en se basant sur les pages sur lesquelles chaque membre du réseau se présente) et proposent des systèmes de recommandation basés sur des relations de confiance pour mettre

1. https://fr.wikipedia.org/wiki/R%C3%A9seautage_social

2. https://fr.wikipedia.org/wiki/Logiciel_social

en rapport les utilisateurs. Certains sites comportent des répertoires de catégories spécifiques d'utilisateurs (par exemple d'anciens camarades de classe).

■ Le partage social permet aux utilisateurs de partager du contenu d'un site web sur un site ou une application de réseautage social³.

■ Parmi les sites et applications de réseautage social les plus populaires, on peut citer : Twitter, Facebook, LinkedIn, Google+, Snapchat, Tumblr, Pinterest, Vine et Whatsapp.

■ En Europe, on trouve : Badoo, Bebo, V Kontakte ou VK (Russie), Delphi, Draugiem.lv (Lettonie), iWiW (Hongrie), Nasza-Klasa (Pologne), Soup (Autriche), Glocals en Suisse, Skyrock, The Sphere, StudiVZ (Allemagne), Tagged, Tuenti (principalement en Espagne) et bien d'autres.

■ Les réseaux sociaux peuvent également servir à des échanges sur les droits de l'homme et les libertés fondamentales et fournir des informations intéressantes au grand public.

■ La plupart des réseaux sociaux sont généralistes, mais il existe également d'autres communautés plus spécifiques :

- communautés de transactions, qui visent à faciliter l'achat et la vente, la location de biens ou de chambres, etc. ;
- communautés d'intérêts, généralement axées sur un sujet en particulier, par exemple le cinéma, la santé, etc. ;
- communautés portant sur des environnements imaginaires et des jeux, comme « World of Warcraft » et « Second Life » ;
- communautés de promotion et de défense des droits de l'homme ou du consommateur ;
- communautés d'aide et de conseil sur le handicap, les besoins spéciaux ou d'autres difficultés ;
- La plupart des réseaux sociaux proposent également des fonctionnalités simples de gestion de la confidentialité des données à caractère personnel (voir Fiche d'information 9 sur les paramètres de confidentialité). Ces outils permettent aux utilisateurs de restreindre l'accès à certaines parties de leur profil à leurs seuls amis ou aux membres disposant de certaines autorisations. Ils permettent également aux membres de restreindre l'accès par recherches aléatoires et la possibilité pour d'autres membres d'associer des tags à leurs contenus.



INTÉRÊT PÉDAGOGIQUE

- Le réseautage social et le partage social sont des moyens peu coûteux et rapides de partager du contenu et des informations personnelles et commerciales.
- Le réseautage social permet également aux individus de rester en contact ou de reprendre contact avec des membres de leur famille et des amis qu'ils auraient pu perdre de vue ou qui vivent loin d'eux.
- Les sites de réseaux sociaux permettent l'organisation d'événements : si certains sont anodins, comme un salon de la bijouterie ou une fête d'enfants, d'autres peuvent faire du tort, comme une rave party ou une manifestation à caractère raciste/xénophobe/homophobe ou visant à défendre d'autres causes extrêmes et à dénigrer.
- De nombreux secteurs ont pris conscience de l'importance des réseaux sociaux dans la valorisation des marques, et visent à obtenir des recommandations (et in fine, des ventes) par ce biais.
- Compte tenu de la facilité avec laquelle ils peuvent partager du contenu via les sites web et les applications sur smartphones, de nombreux jeunes ont tendance à publier tout et n'importe quoi, sans grand discernement.
- Un usage responsable des réseaux sociaux est essentiel car les employeurs potentiels, les lycées ou universités, voire la famille et les amis, peuvent avoir accès à ces informations.
- Cet usage responsable peut d'ailleurs être considéré comme un moyen peu coûteux de promouvoir

3. www.oxforddictionaries.com/definition/english/social-sharing

ses projets ou réalisations (par exemple un jeune qui lance une campagne pour des services fournis à la collectivité), de créer un contenu viral pour le bien commun, ou d'obtenir une reconnaissance (par exemple publication d'informations sur un prix ou un diplôme récemment décerné).

- Les sites de réseautage social peuvent être utilisés pour diffuser des informations fausses ou basées sur des préjugés, ce qui requiert une vigilance particulière de la part des utilisateurs quant au choix de leurs « amis » et un travail de vérification de la fiabilité des contenus.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

■ Les gens se disent souvent libérés de leurs inhibitions sur les réseaux sociaux. Ils se sentent quelquefois invincibles, ce qui les pousse à faire des commentaires et des réponses qu'ils ne se permettraient pas dans une relation normale. À cela s'ajoute le fait que l'on peut facilement exagérer les émotions dans le monde virtuel ou dire des choses que l'on tairait si l'on avait notre interlocuteur directement en face de nous.

■ Les sites de réseaux sociaux permettent aux utilisateurs de déposer des commentaires sur les profils d'autres personnes. Il convient de bien réfléchir au type et à la nature de ces commentaires.

■ Au Royaume-Uni, Get Safe Online⁴, a recensé un certain nombre de risques liés à l'utilisation des sites de réseaux sociaux, et notamment :

- la divulgation d'informations privées par l'utilisateur lui-même ou par ses amis/contacts ;
- les manœuvres d'intimidation ;
- le cyberharcèlement ;
- l'accès à des contenus inadaptés pour l'âge ;
- les sollicitations d'enfants à des fins sexuelles et la violence à l'égard d'enfants ;
- la confrontation avec des commentaires de nature violente, sexuelle, extrémiste ou raciste, des activités choquantes et des attitudes haineuses ;
- les personnes qui en harcèlent d'autres ou tentent de les persuader de changer de convictions ou d'idéologies, ou d'adopter des points de vue extrémistes ;
- les poursuites ou récriminations pour avoir publié des commentaires offensants ou inappropriés ;
- les courriels d'hameçonnage semblant provenir de sites de réseaux sociaux mais incitant l'Internaute à se rendre sur des sites frauduleux ou au contenu inapproprié ;
- les messages d'amis, d'autres personnes et de sociétés incitant l'Internaute à cliquer sur un lien vers un site frauduleux ou au contenu inapproprié ;
- le piratage et le détournement de compte ou de page ;
- les virus ou logiciels espions dans les pièces jointes aux messages ou dans des photographies ;
- la publication de messages par l'Internaute lui-même ou par un membre de sa famille indiquant qu'il n'est pas chez lui ou qu'il part en vacances, faisant ainsi savoir à tous que sa maison est vide et laissant le champ libre aux cambrioleurs ; s'il venait ensuite à porter plainte auprès de sa compagnie d'assurance après avoir été victime d'un cambriolage en son absence, ce type de publications pourrait constituer un motif de rejet de sa demande d'indemnisation⁵.

■ Il existe d'autres risques encore :

- l'exposition à du contenu commercial et l'exploitation des données privées à des fins commerciales ;

4. <https://www.getsafeonline.org/social-networking/social-networking-sites/>
5. www.getsafeonline.org/social-networking/social-networking-sites/

- une réputation ternie à jamais, ce qui pourrait entraîner des difficultés à trouver un emploi ou d'autres types de discrimination comme l'exclusion financière (incapacité à obtenir un prêt ou une assurance, etc.) ;
- l'exposition à du contenu non pluraliste allant uniquement dans le sens de ses propres convictions/connaissances/opinions et pouvant de ce fait limiter le cheminement et l'évolution personnels ;
- l'exposition à une pression sociale extrême exigeant une apparence parfaite, une existence heureuse et tout sauf banale et la publication en flux ininterrompu de choses agréables ou spectaculaires

■ Comme pour toutes les autres technologies en ligne, il ne sert à rien d'interdire aux jeunes l'accès aux réseaux sociaux. Au contraire, il faut leur donner les clés d'un comportement sûr en ligne, leur apprendre à faire preuve de discernement et les encourager à respecter les restrictions liées à l'âge, à ne pas divulguer leurs informations personnelles et à se comporter en individus responsables lorsqu'ils diffusent du contenu.

■ Tout adulte responsable cherchera à se former aux dangers et aux bonnes pratiques en matière d'utilisation des sites de réseaux sociaux plutôt que d'en empêcher l'utilisation. Ces choses se font naturellement dans le monde matériel, alors pourquoi pas dans le monde en ligne ?

■ Il convient d'encourager les jeunes à faire part de leurs expériences sur Internet à des adultes de confiance, par exemple leurs parents ou leurs enseignants. Comme toujours en matière de sécurité sur Internet, l'implication active des parents et des enseignants sur les questions ayant trait à la vie en ligne des jeunes est le facteur qui a l'impact le plus positif sur le comportement de ces derniers en ligne.

■ Cela permettra également aux parents de découvrir les côtés plaisants des sites de réseaux sociaux.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Demandez aux élèves de réfléchir au type d'informations qu'ils jugeraient acceptable de publier sur un profil en ligne. Une fois qu'ils auront établi une liste, demandez-leur de créer un profil sur papier. Consentiraient-ils à ce que ce profil soit diffusé à tous les parents d'élèves de l'école ? Dans la plupart des cas, ils ne le voudraient pas ; c'est donc l'occasion de leur rappeler que toute personne peut consulter leur profil sur un site de réseaux sociaux à moins qu'ils ne l'aient paramétré de manière à ce qu'il reste privé. Il est important d'établir ce lien entre le monde réel et le monde virtuel pour aider les jeunes à bien mesurer les conséquences potentielles de la publication d'informations en ligne.
- En classe, consultez deux ou trois sites de réseaux sociaux et demandez aux élèves de signaler tout comportement à risque qu'ils pourraient constater. Qu'est-ce qui expose les utilisateurs à un danger ? Invitez ensuite les élèves à faire le point sur leurs propres activités en ligne à la lumière de ces éléments.
- Dans le cadre d'un travail en groupe, demandez à vos élèves d'établir leurs propres listes de points à prendre en considération lorsqu'ils publient des contenus en ligne sur un site de réseaux sociaux. Comparez les listes et faites-en une synthèse que les élèves pourront imprimer et afficher à côté de leur ordinateur.
- Demandez à vos élèves d'apporter des photos numériques qu'ils souhaiteraient publier sur un site de réseaux sociaux. Par petits groupes, faites-les analyser chacune des photos pour déterminer quelles sont les informations à caractère personnel que l'on peut en déduire. Attribuez une « note de sécurité » à chaque photo sur une échelle de 1 à 5, 5 correspondant à une photo qui ne dévoile rien de la vie privée de l'utilisateur.

- Voir la Fiche d'information 3 intitulée « Web 2.0 , 3.0 et plus » pour d'autres suggestions d'utilisation des réseaux sociaux en classe.
- Préparez du matériel adapté pour vos enfants ou vos élèves afin d'engager une discussion sur le contenu extrémiste et la manière dont il peut influencer sur les comportements. Cherchez ensemble des moyens de lutter contre l'extrémisme. Le plan d'action du Conseil de l'Europe contre l'extrémisme violent et la radicalisation pourra vous être utile pour informer les élèves et faire émerger des idées⁶.
- Examinez le Règlement général sur la protection des données avec vos élèves et les raisons pour lesquelles l'Union européenne pourrait souhaiter interdire l'accès aux réseaux sociaux aux enfants en dessous d'un certain âge⁷. Quelle devrait être cette limite d'âge ?



BONNES PRATIQUES

- Toute personne peut avoir accès aux informations personnelles que vous mettez en ligne – la règle d'or consiste à partir du principe que tout est public à moins de s'assurer du contraire. Par conséquent, il ne faudrait jamais rien dire sur un site de réseautage social que l'on ne souhaiterait pas rendre public dans le monde matériel. Le fait de choisir un profil « privé » ne signifie pas toujours que seuls vos amis peuvent le voir. Dans certains cas, cela signifie simplement que tout le monde peut consulter ce que vous publiez dans le profil, mais que seuls les « amis » peuvent y ajouter des commentaires ou envoyer des messages instantanés. Sachez également que si vous rejoignez de grands groupes ou réseaux (par exemple nationaux, ou à l'échelle d'une ville), l'accès à votre profil risque d'être ouvert à un grand nombre de personnes.
- Suivez votre instinct – quelque chose qui a l'air « louche » risque fort de l'être ! Si vous trouvez quelque chose en ligne qui ne vous plaît pas ou vous met mal à l'aise, éteignez votre ordinateur et parlez-en à un ami en qui vous avez confiance.
- Soyez vigilant avec vos données personnelles, le problème étant que dès lors que vous publiez ce genre d'informations sur Internet, vous ne pouvez plus contrôler qui les consulte ou comment elles seront exploitées. Un simple clic suffit pour copier des images ou des photos et les partager avec des milliers d'autres personnes. Les photos étant numériques, elles peuvent même être modifiées ou falsifiées. Certains nouveaux logiciels de recherche parviennent même à identifier les personnes qui apparaissent sur une photo même si aucun nom n'y est associé. Les jeunes doivent donc tous apprendre à ne diffuser que des images qu'ils n'auraient aucun mal à montrer à tout le monde, y compris leurs parents et enseignants.
- Sur Internet, les gens ne sont pas toujours ce qu'ils prétendent être. Le fait que certains sites web affirment mettre en relation des élèves d'une même école ne veut rien dire. Les informations fournies par les utilisateurs lors de leur inscription ne sont pas vérifiées. Toute personne peut créer un profil d'utilisateur qui ne correspond pas à son identité. De la même manière, n'importe qui peut, quel que soit son âge réel ou prétendu, s'inscrire dans autant de communautés scolaires qu'il le souhaite.
- Conservez un certain équilibre de vie : si les médias sociaux sont devenus une obsession et que vous ne pouvez plus vivre sans vérifier/mettre à jour votre profil, publier des photos et compter les « j'aime », vous devriez peut-être envisager de vous couper temporairement des réseaux sociaux ou au minimum de garder un œil sur le temps consacré à ces derniers.
- Lisez les conseils fournis par la plupart des prestataires de services de réseaux sociaux pour une utilisation sûre de leurs sites.
- Réfléchissez bien avant de mettre en ligne un contenu – n'oubliez pas qu'une fois que vous l'aurez publié, vous risquez de ne plus pouvoir le supprimer entièrement de l'Internet.

6. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3576

7. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf

- La plus grande prudence s'impose en ce qui concerne la publication d'images. Même si vous n'y associez pas votre nom, elles pourraient tout de même permettre de vous identifier. Par ailleurs, elles peuvent rester accessibles dans les caches web longtemps après leur retrait.
- Protégez vos données personnelles, et en particulier celles qui pourraient permettre de vous identifier ou de vous localiser.
- Ne publiez jamais rien qui puisse être offensant, diffamatoire ou dégradant vis-à-vis d'autres personnes.
- N'oubliez pas que votre profil peut être configuré en « public » ou « privé ». Choisissez la solution qui vous paraît la plus adaptée après mûre réflexion.
- Utilisez les paramètres de confidentialité proposés par les sites de réseaux sociaux. Réfléchissez bien avant de rendre votre profil visible à tous.
- N'oubliez pas que si l'option « public » est activée, votre compte peut être vu par tout le monde. Et même dans le cas contraire, il peut être vu par toute personne faisant partie des réseaux dont vous êtes membre. Il est judicieux de vérifier régulièrement vos paramètres car il peut arriver que les sites de réseaux sociaux modifient leurs politiques.
- Si vous rencontrez des problèmes en ligne, tels que des campagnes de haine, des manœuvres d'intimidation ou des messages ciblés à contenu raciste, xénophobe, homophobe ou extrême, demandez toujours de l'aide à une personne de confiance, même si vous pensez qu'elle pourrait ne pas comprendre ou approuver.
- Ne donnez jamais vos coordonnées sur votre profil.
- N'oubliez pas que les contenus que vous publiez en ligne peuvent être utilisés à des fins très diverses et notamment pour vous envoyer de la publicité personnalisée, mais aussi pour mesurer votre aptitude à l'emploi ou pour des motifs politiques.
- Vérifiez vos paramètres lorsque vous utilisez différents appareils pour vous rendre sur les sites de réseaux sociaux car ils pourraient vous demander un accès aux informations de votre smartphone, tablette ou ordinateur.



INFORMATIONS COMPLÉMENTAIRES

- Pour plus d'informations sur les réseaux sociaux, voir « The world's 21 most important social media sites and apps in 2015 » : <http://web.archive.org/web/20160423200413/http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015>.
- Quelques conseils pour utiliser les réseaux sociaux en toute sécurité : http://web.archive.org/web/20120602054510/http://www.getsafeonline.org/nqcontent.cfm?a_id=1459.
- On trouvera des informations sur divers sujets liés à l'utilisation des sites de réseautage social et des conseils relatifs à la sécurité sur ces sites à l'adresse : www.privacyrights.org/social-networking-privacy.
- Il existe un rapport du Social Science Research Network sur l'usage des réseaux sociaux par les adolescents : http://web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.
- Le PEW Research Center a publié une étude sur les adolescents, la technologie et les amitiés à l'adresse : <http://web.archive.org/web/20160710143035/http://www.pewinternet.org/2015/08/06/teenstechnology-and-friendships/>.
- Documents pertinents du Conseil de l'Europe : Recommandation CM/Rec(2012)4 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux : <https://wcd.coe.int/ViewDoc.jsp?id=1929453>.

Protection de la vie privée et paramètres de confidentialité



On entend par protection de la vie privée le degré de contrôle qu'a une personne sur l'accès à ses données à caractère personnel et l'utilisation qui en est faite. La plupart des Internautes et des utilisateurs de services de courrier électronique supposent que leurs données personnelles ne seront pas utilisées sans leur autorisation et que les échanges d'informations sont privés et sécurisés. La réalité est bien différente.

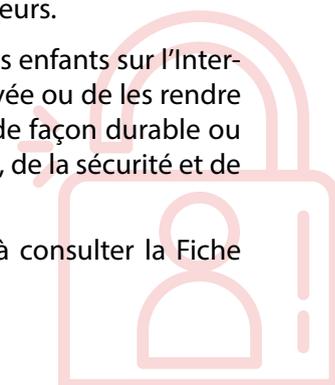
— À chaque fois que vous consultez un site web, publiez du contenu sur un média social ou envoyez un courrier électronique, vous laissez des informations vous concernant. Celles-ci peuvent inclure votre adresse physique et adresse IP, vos numéros de téléphone et de carte de crédit, votre profil de consommateur et même bien plus.

— N'oubliez pas qu'il peut être difficile de garder la mainmise sur vos données une fois qu'elles sont sur le réseau, et que cela peut avoir des conséquences durables.

■ Le commerce électronique, et notamment les achats en ligne et la publicité, étant devenu une manière courante de faire des affaires, une attention particulière devrait être portée à la protection des données sensibles, des communications et des préférences des consommateurs.

■ Il convient de veiller à ce qu'aucun historique des contenus générés par des enfants sur l'Internet, susceptible de porter atteinte à leur dignité, à leur sécurité et à leur vie privée ou de les rendre vulnérables, maintenant ou à un stade ultérieur de leur vie, ne soit accessible de façon durable ou permanente (Déclaration du Comité des Ministres sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur Internet, adoptée le 20 février 2008)¹.

■ La protection de la vie privée est étroitement liée à la sécurité ; veuillez à consulter la Fiche d'information 19 sur la sécurité.



PROTECTION DE LA VIE PRIVÉE SUR INTERNET

- La protection de la vie privée sur Internet (ou en ligne) est un terme générique qui désigne l'ensemble des éléments, techniques et technologies mis en œuvre pour protéger les données sensibles, les communications privées et les préférences des utilisateurs².
- Elle est mise en jeu chaque fois qu'un utilisateur se rend en ligne au moyen d'un ordinateur, d'une tablette, d'un smartphone, d'une console de jeux ou d'un autre appareil équipé d'une connexion sans fil (Wi-Fi).
- La protection de la vie privée sur Internet ne renvoie pas uniquement à la manière dont on maintient la confidentialité de ses données à caractère personnel en ligne, mais également à la facilité avec laquelle les pirates peuvent accéder à ces informations.
- Le Règlement général sur la protection des données permet aux utilisateurs d'avoir un plus grand contrôle sur leurs données et améliore la protection de leur vie privée en ligne. Ses grands principes sont les suivants :
 - ▶ nouvelle définition du consentement de l'utilisateur : le consentement ne peut plus être considéré comme ayant été donné librement si l'utilisateur doit donner son consentement au traitement de données au-delà de ce qui est strictement nécessaire à l'exécution d'une prestation de service ;
 - ▶ plus de transparence dans l'information des utilisateurs sur la manière dont leurs données sont traitées, grâce à l'utilisation de pictogrammes/icônes et d'un langage simple, pour pouvoir comparer plus facilement les services et choisir ceux qui respectent le mieux leur vie privée ;
 - ▶ le droit des utilisateurs à la portabilité des données, autrement dit le droit de recevoir les données à caractère personnel les concernant qu'ils ont fournies aux services qu'ils utilisent, dans un format structuré : cette disposition renforce considérablement le contrôle des données par l'utilisateur et le principe de la propriété des données ;
 - ▶ une protection renforcée pour les enfants – tout jeune âgé de 13 (minimum) à 16 ans (maximum) bénéficiera d'une protection supplémentaire, par exemple l'exigence d'un consentement des titulaires de l'autorité parentale au traitement des données et une protection contre le traitement des données à des fins publicitaires ;
 - ▶ des amendes d'un montant supérieur (jusqu'à 4 % du chiffre d'affaires d'une société) en cas de manquement à ces règles.
- Les conséquences du piratage et de la divulgation d'un mot de passe peuvent être très graves et aller jusqu'au vol d'identité et aux transactions illégales en ligne.

1. [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl\(20.02.2008\)&Language=lanFrench&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl(20.02.2008)&Language=lanFrench&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true)

2. <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>

Paramètres de confidentialité

■ Les paramètres de confidentialité sont les outils qui permettent aux utilisateurs de restreindre l'accès à leurs informations et de choisir lesquelles peuvent être vues par les autres.

■ Sur la plupart des réseaux sociaux, ils sont réglés par défaut : on peut les personnaliser selon ses propres exigences. Il convient par ailleurs de les revérifier à chaque nouvelle mise à jour annoncée par la plateforme de réseaux sociaux.

■ Il convient de revérifier régulièrement les paramètres de confidentialité sur tous vos appareils dotés d'une connexion sans fil, en n'oubliant pas les paramètres de géolocalisation car vos coordonnées géographiques ou celles de votre appareil sont des éléments importants de votre vie privée (voir Fiche d'information 5 Internet en mobilité).

Géolocalisation

■ La géolocalisation³ consiste à déterminer la position d'un objet – radar, téléphone portable ou ordinateur connecté à Internet, par exemple.

■ Les applications de géolocalisation indiquent aux utilisateurs où vous vous trouvez et peuvent calculer la distance entre votre position et des lieux du monde réel. Elles ont inventé de nouveaux modèles économiques.

■ La géolocalisation peut constituer une menace pour la vie privée car elle permet de savoir où vous vous trouvez ; la géolocalisation d'un enfant peut compromettre sa sécurité.

Cookies

■ Un cookie⁴ est un fichier texte déposé dans votre ordinateur lorsque vous consultez un site web. Il n'est pas dangereux pour votre ordinateur mais peut donner accès à des informations sur vos habitudes et vos centres d'intérêt. Il personnalise votre environnement de navigation sur Internet. Par exemple, si vous vous enregistrez sur un site web, celui-ci pourra vous accueillir en affichant votre nom à la connexion suivante.

■ Il est important de déterminer le degré de confidentialité que vous souhaitez maintenir quant à votre comportement en ligne. Les cookies peuvent être utilisés pour repérer vos habitudes et vos contacts et porter atteinte à votre vie privée. Ils facilitent également un ciblage comportemental par les publicitaires⁵.

■ Vous pouvez utiliser un logiciel anti-espion⁶ pour contrôler les données transmises par votre ordinateur et supprimer les cookies indésirables.

■ Aujourd'hui, tous les sites web établis dans l'UE ou qui sont destinés à des ressortissants de l'UE doivent respecter la législation relative aux cookies (Directive UE 2009/136/CE) qui donne aux individus le droit de refuser l'utilisation de cookies compromettant la confidentialité de leurs données en ligne.

Protection des données

■ La protection des données à caractère personnel est régie par la Convention du Conseil de l'Europe pour la protection des individus à l'égard du traitement automatisé des données à caractère personnel.

■ Toute personne a le droit de savoir quelles sont les données dont dispose une entreprise la concernant. Elle doit également pouvoir demander à les modifier si elles ne sont pas exactes et donner son consentement quant à la manière dont elles seront utilisées.

■ Des recommandations de bonne pratique en matière de protection des données à caractère personnel sont contenues dans le Règlement général sur la protection des données⁷.

3. <https://fr.wikipedia.org/wiki/Géolocalisation>

4. [https://fr.wikipedia.org/wiki/Cookie_\(informatique\)](https://fr.wikipedia.org/wiki/Cookie_(informatique))

5. https://fr.wikipedia.org/wiki/Ciblage_comportemental

6. https://fr.wikipedia.org/wiki/Logiciel_espion

7. http://ec.europa.eu/justice/data-protection/reform/index_fr.htm

■ Lisez attentivement les politiques de confidentialité des sites web et applications qui vous demandent de fournir des informations à caractère privé⁸. Il s'agit d'un contrat entre vous et le contrôleur des données⁹, qui doit préciser où et pendant combien de temps vos données seront stockées, et comment obtenir leur suppression.

■ Protégez votre ordinateur et vos logiciels de messagerie par un mot de passe¹⁰. Lorsque vous faites l'acquisition d'un nouvel appareil ou logiciel, ou que vous vous abonnez auprès d'un fournisseur d'accès à Internet, vous recevrez probablement un identifiant et un mot de passe par défaut. Remplacez-les rapidement par un identifiant et un mot de passe plus sécurisés.

■ Il vaut mieux chiffrer¹¹ toutes les informations sensibles envoyées par Internet. Heureusement, cette pratique est devenue la norme pour la plupart des transactions de commerce électronique¹² mais il convient tout de même de vérifier que la page que vous consultez est sécurisée avant de transmettre vos données de carte de crédit ou vos numéros de compte bancaire.

■ Il est possible de protéger différentes parties de votre ordinateur par des mots de passe. Créez-en pour les dossiers qui contiennent des documents de valeur comme les projets confidentiels, travaux de recherche, créations originales, etc.

Droit à l'oubli

■ Le droit à l'oubli est un aspect important de tout débat sur la protection de la vie privée car il permet aux individus de reprendre le contrôle sur la confidentialité de leurs données à caractère personnel.

■ Dans l'Union européenne, toute personne peut demander à ce que certains résultats soient retirés de l'index d'un moteur de recherche de manière à ce qu'ils n'apparaissent pas lorsque quelqu'un effectue une recherche avec son nom pour mot-clé. Cela dit, il y a des limites à cette possibilité, qui devra toujours être mise en balance avec les droits fondamentaux d'autres personnes, comme la liberté d'expression. En tout état de cause, l'information restera accessible sur le site web où elle figure ; elle sera simplement plus difficile à retrouver.

■ Pour exercer le droit à l'oubli et demander la suppression de son nom d'un moteur de recherche, la personne doit remplir un formulaire sur le site web de celui-ci¹³.

■ N'oubliez pas qu'il est toujours préférable de ne pas divulguer d'informations privées car une fois qu'elles sont sur Internet, il devient quasiment impossible de les effacer totalement.

Importance de parler de la protection de la vie privée en classe ou à la maison

■ La protection de la vie privée, dans ses aspects techniques et sociaux, et les risques de divulguer soi-même des informations à caractère personnel sont intéressants au plan pédagogique car ils soulèvent un grand nombre d'interrogations. Les questions techniques peuvent être abordées dans les cours d'informatique mais devraient également être intégrées dans des programmes de préparation à la vie quotidienne.

■ La notion de « profilage » est un autre aspect important qu'il faut aborder dans la formation aux questions de protection de la vie privée. Elle désigne la mise en commun d'éléments d'information disparates sur une personne pour en déduire une image beaucoup plus détaillée. Par exemple, en comparant un profil « anonyme » sur un réseau social (c'est-à-dire une personne qui se cache derrière un pseudonyme) et un profil complet, correspondant à la même personne, sur un autre site, on peut trouver la véritable identité de celle-ci.

■ Il faut se méfier de l'idée selon laquelle il n'y aurait violation de la vie privée qu'en cas de divulgation d'informations personnelles « classiques ». Les nouvelles techniques de marketing, qui établissent des distinctions entre les personnes selon leurs caractéristiques comportementales (ce que l'on appelle le ciblage comportemental) peuvent également porter atteinte à la vie privée.

8. <https://en.wikipedia.org/wiki/Disclaimer>

9. <https://goo.gl/XEkvjh>

10. https://fr.wikipedia.org/wiki/Mot_de_passe

11. <http://www.netlingo.com/right.cfm?term=default>

12. <https://fr.wikipedia.org/wiki/Chiffrement>

13. https://fr.wikipedia.org/wiki/Commerce_électronique

■ La vie privée est de plus en plus menacée par la vitesse et la facilité avec laquelle les enfants et les jeunes peuvent publier ou diffuser en direct des images numériques sur Internet grâce aux applications web et aux appareils photo et fonctions MMS des téléphones portables. Une règle simple : ne jamais publier quelque chose que vous ne souhaiteriez pas que vos enseignants ou vos parents voient.

■ Chacun devrait apprendre à utiliser Internet en toute sécurité, c'est-à-dire savoir se protéger, communiquer de manière efficace et se montrer responsable vis-à-vis des autres.

■ La question de la protection de la vie privée en ligne rejoint naturellement la dimension citoyenne de tout programme d'enseignement. Elle fait écho aux grandes questions de société qui se posent dans la plupart des cultures aujourd'hui. À cet égard, l'examen des motivations des pirates informatiques¹⁴, des « casseurs de protections » (crackers) et des militants pour le respect de la vie privée offre de riches possibilités de discussion sur l'utilité des principes démocratiques.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Le respect de la vie privée en ligne fait partie des questions éthiques et juridiques les plus complexes liées à Internet.
- Chacun a droit au respect de sa vie privée et doit être protégé contre les actes de malveillance.
- Les risques pour la vie privée sur Internet incluent l'hameçonnage ou *phishing* (piratage sur Internet en vue du vol de données sécurisées concernant l'utilisateur), le dévoiement ou *pharming* (piratage sur Internet en vue de rediriger le visiteur d'un site web légitime vers l'adresse IP d'un site frauduleux), les logiciels espions (application hors ligne qui obtient les données sans l'accord de l'utilisateur) et les logiciels malveillants (application utilisée pour nuire à l'utilisateur en ligne et hors ligne au moyen de chevaux de Troie, de virus et de logiciels espions)¹⁵.
- La textopornographie (ou « *sexting* »), qui désigne l'envoi de contenu, de messages contenant des photos (souvent des selfies) ou de vidéos suggestives et à caractère sexuel, par téléphone, ordinateur, webcam ou autre appareil ou la publication de messages à caractère sexuel en ligne, peut avoir des conséquences graves sur le plan juridique, mais aussi pour la réputation de la personne concernée, les messages, photos ou vidéos en question pouvant être diffusés sur des sites de médias sociaux ou utilisés sur des sites et dans des vidéos pornographiques.
- Nous sommes responsables de toutes les décisions que nous prenons concernant nos droits et à ceux d'autrui, par exemple en matière de droit d'auteur¹⁶ et de propriété intellectuelle¹⁷.
- La liberté d'expression est un droit ; cela dit, dans la pratique, elle pose de nombreuses questions auxquelles il n'y a jamais de réponse simple. Qu'est-ce qui est acceptable et qu'est-ce qui ne l'est pas ? Comment appliquer la réglementation sans porter atteinte aux droits de celui qui s'exprime ?



MODE D'EMPLOI

■ Le réglage des paramètres de confidentialité est l'un des meilleurs moyens de protéger votre vie privée sur tous vos équipements dotés d'un accès sans fil à Internet.

■ En fonction de votre navigateur, effectuez une recherche rapide dans les paramètres de confidentialité pour trouver comment :

14. https://fr.wikipedia.org/wiki/Droit_à_l'oubli

15. <http://fr.wikipedia.org/wiki/Hacker>

16. <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>

17. <https://fr.wikipedia.org/wiki/Copyright>

- bloquer les publicités et le suivi
- bloquer les cookies tiers
- empêcher les sites web d'accéder à votre position géographique.

— N'oubliez pas de vérifier les paramètres de confidentialité sur vos smartphones, tablettes et consoles de jeu. Les appareils photo de dernière génération présentent également des fonctionnalités de géolocalisation à contrôler.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Invitez les élèves à effectuer une recherche sur Google avec leur nom pour mot-clé, en y incluant les images et vidéos. Créez avec eux une alerte Google relative à leur nom afin qu'ils soient avertis lorsque celui-ci apparaît en ligne.
- Établissez avec votre classe un socle de connaissances de base sur le respect de la vie privée. Définissez les concepts techniques et sociaux et recensez les idées reçues à ce sujet en vue d'une discussion. Des questions simples, par exemple « qu'est-ce que le respect de la vie privée ? » et « le respect de la vie privée est-il nécessaire ? » susciteront probablement un vif débat.
- Cherchez des sites traitant de la protection de la vie privée sur Internet et utilisez des programmes traceroute¹⁸ pour localiser les adresses physiques de ces sites et mettre en évidence les diverses questions de localisation territoriale qui conditionnent la légalité sur Internet. Examinez les autres questions (d'ordre culturel, politique et historique) qui se posent au regard des résultats obtenus. Par exemple, choisissez un serveur de courriel anonyme¹⁹ ou un service proxy anonyme, lancez le programme et cherchez pourquoi ces services sont hébergés dans les pays qui apparaissent sur la liste.
- Le jeu de rôles Play Decide sur la protection des données et de la vie privée²⁰ est un moyen ludique d'étudier l'incidence de la législation sur le respect de la vie privée, les droits d'auteur et la liberté d'expression et d'information dans divers pays ou pour différents groupes culturels ou tranches d'âge.
- Enseignez aux élèves comment créer des mots de passe sécurisés²¹.
- Parcourez et comparez avec vos élèves les profils d'utilisateurs sur quelques-uns des sites de réseaux sociaux les plus connus (voir Fiche d'information 8 sur les réseaux sociaux). Quelles informations personnelles les utilisateurs divulguent-ils par inadvertance ? Établissez une liste de points à prendre en considération pour créer un profil d'utilisateur sûr.



BONNES PRATIQUES

- Deux règles d'or :
 - ▶ ne divulguez aucune information personnelle à une personne que vous ne connaissez pas ou en qui vous n'avez pas confiance ;
 - ▶ n'utilisez pas les informations personnelles ou les photos d'autres personnes sans leur consentement.
- Effectuez régulièrement²² des sauvegardes de votre système selon un plan prédéfini.
- Mettez à jour les paramètres de sécurité de votre système et faites des recherches sur les autres outils qui permettront de faire respecter vos préférences en ligne à l'adresse <<http://www.epic.org/privacy/tools.html>>.

18. <https://fr.wikipedia.org/wiki/Traceroute>

19. https://fr.wikipedia.org/wiki/Serveur_de_courriel_anonyme

20. <http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf>

21. https://fr.wikipedia.org/wiki/Mot_de_passe

22. [https://fr.wikipedia.org/wiki/Sauvegarde_\(informatique\)](https://fr.wikipedia.org/wiki/Sauvegarde_(informatique))

- Les logiciels antivirus²³ et pare-feu²⁴ sont absolument indispensables. Vous pourrez également installer d'autres outils comme les bloqueurs de fenêtres intempestives²⁵ et de logiciels espions²⁶. Analysez régulièrement votre système.
- Utilisez des mots de passe fiables²⁷ pour protéger votre PC, vos courriels et vos connexions Internet. Un mot de passe solide se compose de chiffres, de lettres et de caractères spéciaux.
- Avant de communiquer des données personnelles, assurez-vous que le symbole du cadenas, signe que votre transaction s'effectue grâce à une connexion sécurisée, est bien présent dans la barre d'outils. Avant toute transaction en ligne, vérifiez que l'URL commence bien par « https », le « s » signifiant ici « sécurisé » et permettant d'authentifier le site web et le serveur web associé, ce qui protège contre des attaques de tiers.
- Évitez d'effectuer des achats en ligne sur des sites peu fiables et de divulguer des données personnelles sur des sites Internet au niveau de sécurité faible.
- Pensez à vérifier vos droits : il se peut que vous soyez plus protégé que vous ne le pensez. Les utilisateurs sont toujours le maillon faible de la protection des données et de la vie privée.



INFORMATIONS COMPLÉMENTAIRES

- Pour en savoir plus sur la loi relative aux cookies et la Directive de l'UE, voir : <http://www.cookie-law.org/the-cookie-law/>.
- Il existe une fiche d'information de la Commission européenne sur le droit à l'oubli : http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
- Il existe également une fiche d'information de la Commission européenne sur la protection des données : http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf et d'autres informations sur les réformes connexes http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
- Le Electronic Privacy Information Center (EPIC) fournit une liste d'outils et d'articles sur le respect de la vie privée : <http://www.epic.org/privacy/tools.html>.
- Découvrez ce que votre ordinateur transmet sur Internet en utilisant BrowserSpy : <http://gemal.dk/browserspy/>.
- Soucieux de vos libertés civiles ? Les discussions suivantes sur le respect de la vie privée pourraient occuper votre classe pendant quelque temps : Electronic Frontier Foundation <http://www.eff.org/>, Epic.org <http://www.epic.org>, Privacy International <http://www.privacyinternational.org/> et Privacy.net <http://www.privacy.net/>.
- TuCows à l'adresse <http://www.tucows.com/> est un site web qui donne accès à plus de 40 000 programmes gratuits ou partagés. Il propose des téléchargements rapides, locaux et sécurisés, sans virus ni logiciels espions.
- Zone Alarm, à l'adresse <http://www.zonelabs.com/store/content/home.jsp> est l'un des pare-feu les plus connus. Il vous permet de paramétrer les contrôles d'accès pour différents programmes qui transmettent des informations par Internet.
- CryptoHeaven est une offre de chiffrement qui propose une messagerie, un système de partage de fichiers et un salon de discussion sécurisés avec chiffrement symétrique et asymétrique : <http://www.cryptoheaven.com/>.
- Les pages d'aide de Facebook donnent des informations sur les paramètres de confidentialité : <https://www.facebook.com/help/193677450678703>.

23. https://fr.wikipedia.org/wiki/Logiciel_antivirus

24. [https://fr.wikipedia.org/wiki/Pare-feu_\(informatique\)](https://fr.wikipedia.org/wiki/Pare-feu_(informatique))

25. http://fr.wikipedia.org/wiki/Pop_up

26. https://fr.wikipedia.org/wiki/Logiciel_espion

27. https://fr.wikipedia.org/wiki/Mot_de_passe

- On trouvera à l'adresse des statistiques sur les connaissances des enfants et des jeunes en ce qui concerne la protection de la vie privée en ligne et des paramètres de confidentialité à l'adresse : <<http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/do-millennials-understand-online-privacy>>.
- Pour des statistiques sur la jeunesse en Europe aujourd'hui, voir : <http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world>.
- Pour plus d'informations sur les droits numériques européens, voir : <<http://www.edri.org>>.
- Documents pertinents du Conseil de l'Europe :
 - ▶ Convention pour la protection des individus à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) : <<http://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680078b37%3E>>.
 - ▶ Déclaration du Comité des Ministres sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur Internet : <[https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl\(20.02.2008\)&Language=lanFrench&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl(20.02.2008)&Language=lanFrench&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true)>.
 - ▶ La page suivante du Conseil de l'Europe contient des informations sur les travaux du Conseil de l'Europe dans le domaine de la protection des données et de la vie privée : <<http://www.coe.int/en/web/internetusers-rights/privacy-and-data-protection>> ainsi que sur les droits et responsabilités de chacun en ligne.

3. Internet – Participation à la société du savoir

” « Le savoir est le pouvoir. L'information est libératrice. L'éducation est à la base du progrès, dans chaque société, au sein de chaque famille ».

Kofi Annan, ancien Secrétaire Général des Nations Unies, janvier 1997-décembre 2006

LISTE DE POINTS À VÉRIFIER:

10. RECHERCHE D'INFORMATIONS

Lisez-vous les avertissements lorsque vous consultez un site web ?

Comment être sûr que l'information que vous trouvez est factuelle et objective ?

Consultez-vous plusieurs sites web différents pour vérifier des faits ?

11. TROUVER DES INFORMATIONS DE QUALITÉ SUR LE WEB

Avant de télécharger des fichiers, vérifiez-vous que votre logiciel antivirus est actif ?

Un même événement peut être présenté sous des angles différents : si vous suivez l'actualité sur Internet

Supprimez régulièrement vos cookies pour éviter d'être « profilé » par des moteurs de recherche.

12. APPRENTISSAGE À DISTANCE ET FORMATIONS EN LIGNE OUVERTES A TOUS (MOOC)

Choisissez la méthode d'apprentissage à distance qui vous convient et qui vous aidera le mieux à atteindre vos objectifs (synchrone, asynchrone, calendrier libre, apprentissage à distance mixte).

Avant d'opter pour un cours à distance en particulier, voyez ce qu'en disent les autres élèves et les enseignants.

Prenez toutes les précautions qui s'imposent pour protéger votre équipement et vos logiciels contre le piratage, les virus et les autres menaces.

13. ACHATS EN LIGNE

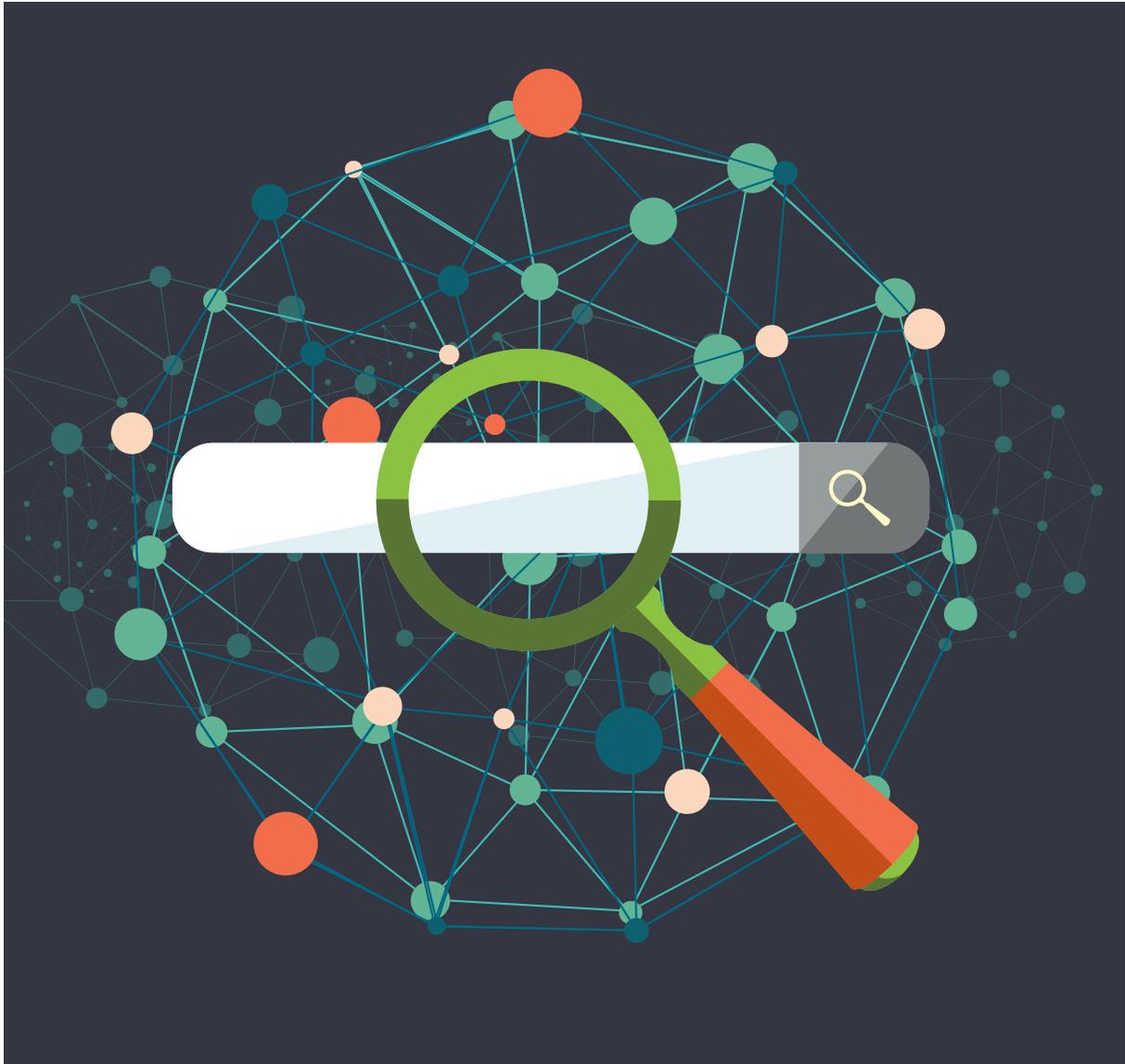
N'effectuez pas d'achats en ligne au moyen de connexions Internet non sécurisées.

Lisez et approuvez les informations qui vous sont données sur le produit ou le service que vous achetez.

Désactivez les achats intégrés aux applications sur votre smartphone ou votre tablette.

Ne croyez pas toutes les recommandations d'utilisateurs que vous lisez : certaines personnes sont rémunérées pour cela.

Recherche d'informations



Aux tous débuts d'Internet, il n'y avait pas de moteurs de recherche. Essayez d'imaginer un monde sans ces outils : on trouvait les adresses des sites web sur des documents papier ou dans des magazines et on les saisisait dans le navigateur. Avec un peu de chance, le site web en question comportait des liens vers d'autres sites et en cliquant d'un lien à un autre, l'utilisateur pouvait « explorer » le World Wide Web. Progressivement, des portails ou répertoires Internet¹ ont été créés sur le modèle de l'annuaire, se présentant comme une vaste liste de sites web classés par catégories. Certains de ces répertoires existent encore aujourd'hui, comme Yahoo! et MSN.

— Parmi les autres types de portails, on trouve :

- les portails présentant du contenu « officiel » comme le site web de l'Organisation des Nations Unies ou du Conseil de l'Europe ;

1. https://fr.wikipedia.org/wiki/Portail_web

- les portails spécialisés dans certains types de contenus ou de services comme Booking.com pour les hôtels ou Amazon.com pour les achats en ligne ;
- les portails présentant du contenu généré par l'utilisateur, qui sont très divers – on peut considérer que les réseaux sociaux, comme Facebook, en font aussi partie.

Les moteurs de recherche ont ensuite été créés et ont révolutionné notre manière de rechercher du contenu sur Internet. Intéressons-nous à leur fonctionnement : aujourd'hui, ils s'appuient sur des robots d'indexation (ou collecteurs)² et des algorithmes très complexes qui analysent le contenu des sites, le classent dans des index³ et décident quels sites web extraire de leur base en fonction des mots-clés que vous saisissez dans le cadre de recherche.

La manière dont l'algorithme est construit est extrêmement importante car la plupart des personnes s'arrêtent aux premières pages des résultats de recherche. Google est le moteur de recherche le plus utilisé aujourd'hui et il doit son succès à son algorithme qui utilise une méthode originale de détermination de l'importance d'un site web, basée sur le nombre de liens retour⁴ qu'il contient, c'est-à-dire grosso modo le nombre de sites web externes qui incluent des liens vers ce site. Par exemple, si le site web wikipedia.org est référencé sur un grand nombre d'autres sites web, il sera mieux classé.

Les algorithmes sont constamment ajustés pour améliorer la précision des résultats. Google prévoit par exemple d'ajouter au sien un élément qui calcule le degré de fiabilité d'un site web en vérifiant la concordance de son contenu avec des faits stockés dans la base de connaissances de Google. Par ailleurs, les algorithmes peuvent également être modifiés à des fins commerciales, comme nous le verrons ultérieurement.

Voir à ce sujet l'animation créée par Google sur le fonctionnement de son moteur de recherche : <https://www.google.com/insidesearch/howsearchworks/thestory/>.



INTÉRÊT PÉDAGOGIQUE

Apprendre à utiliser un moteur de recherche est probablement la première des compétences à développer pour pouvoir naviguer de manière responsable sur Internet et acquérir des compétences transversales comme la pensée critique (en cherchant et en comparant différentes sources en ligne). Une fois que l'on a compris comment se servir d'un moteur de recherche, on peut trouver des informations de qualité pour acquérir des milliers d'autres compétences ou améliorer ses connaissances sur une infinité de sujets, y compris les comportements responsables sur Internet !

On peut aussi améliorer ses compétences numériques en cherchant des solutions aux problèmes que l'on rencontre avec ses appareils ou simplement se renseigner sur leur fonctionnement. Un moteur de recherche permettra aussi, par exemple, de trouver le présent manuel de maîtrise d'Internet.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Certains portails peuvent nécessiter un abonnement ou un enregistrement, qui peuvent être payants. Avant de vous inscrire (même pour des services « gratuits »), veuillez à bien prendre connaissance des conditions générales de fonctionnement et de la politique de confidentialité du site (voir <http://www.netlingo.com/right.cfm?term=privacy%20policy>).
- Les sites web utilisent divers moyens, y compris le référencement payant, pour améliorer leur classement dans les résultats des moteurs de recherche. Certains, comme Google, signalent clairement les annonces sponsorisées, mais beaucoup d'autres ne le font pas.
- Les algorithmes eux-mêmes ne sont jamais neutres et font l'objet de controverses et de critiques⁵. On sait par exemple que Google augmentait la visibilité de ses propres services

2. https://fr.wikipedia.org/wiki/Robot_d'indexation
 3. <https://fr.wikipedia.org/wiki/Référencement>
 4. https://fr.wikipedia.org/wiki/Lien_retour
 5. https://fr.wikipedia.org/wiki/Critiques_de_Google

comme Google Shopping, Google+ ou YouTube au détriment de ses concurrents (Amazon, Facebook, Dailymotion, etc.). Les moteurs de recherche peuvent également être manipulés pour des motifs politiques. La règle d'or en la matière est de ne jamais croire qu'un résultat de recherche est représentatif de la « vérité » du simple fait qu'il figure parmi les premiers sur la liste, ou que les sites web apparaissant plus loin dans le classement sont moins importants ou pertinents.

- Tous ces éléments soulignent la nécessité de conserver une pluralité de portails et de moteurs de recherche capables d'explorer le web et de trouver des résultats plus diversifiés, mais aussi de maintenir une saine concurrence entre eux, de nature à améliorer la précision et la neutralité des recherches. En tant qu'utilisateur, vous jouez un rôle important dans la constitution de l'environnement en ligne : n'oubliez pas d'utiliser d'autres outils de recherche comme Yahoo!, Bing, Qwant, IXquick ou DuckDuckGo. En faisant appel à des moteurs de recherche moins connus, vous contribuez à leur existence et au maintien de la diversité de l'offre⁶.
- N'oubliez pas que votre position déterminée par géolocalisation⁷ et les cookies des recherches précédentes influenceront sur vos résultats de recherche. Bien que l'utilisation de vos données de géolocalisation par le moteur de recherche soit inévitable⁸ vous pouvez tout de même, en supprimant régulièrement vos cookies (voir Fiche d'information sur la vie privée et sa protection) et dans une moindre mesure, en effaçant votre historique de navigation, limiter les annonces ciblées liées à vos précédentes recherches (par exemple : destination de voyage). Vous vous assurerez ainsi d'être suffisamment informé sur les questions sociales et politiques importantes, en ne vous limitant pas à votre propre perception des choses⁹. Vous pouvez aussi désactiver complètement les cookies dans les paramètres de votre navigateur Internet mais sachez que cela peut nuire au bon fonctionnement de certains sites web.
- Enfin, n'oubliez pas que les résultats de recherche que vous obtiendrez dépendront en grande partie de ce que vous cherchez. Par exemple, si vous cherchez du contenu très violent, vous en trouverez très certainement, mais peut-être bien au-delà de ce à quoi vous vous attendiez. La résilience aux contenus choquants ou dérangeants est une capacité qui se construit petit à petit, tout au long de la vie. N'allez pas trop vite en besogne.



MODE D'EMPLOI

Les moteurs de recherche étant les principaux points d'accès à l'information, il est essentiel de bien comprendre leur fonctionnement. Vous limiter aux résultats de recherche de la première page pourrait vous donner une vision extrêmement tronquée de ce qui est important et ce qui ne l'est pas. Les principales fonctionnalités de recherche avancée à garder à l'esprit sont :

- Les guillemets : il s'agit probablement de l'une des fonctionnalités de recherche avancée les plus utiles et les plus connues. Si vous souhaitez qu'un moteur de recherche retrouve une expression exacte, placez-la entre guillemets.
- Le signe moins « - » : il sert à exclure certains termes d'une recherche. Par exemple, si vous recherchez « twilight », les premiers résultats concerneront la série du même nom. Mais si vous tapez « twilight - vampire », vous obtiendrez la définition du mot « twilight ». Cet opérateur logique est donc très utile pour éviter toute confusion, lorsque le mot que l'on recherche est trop souvent associé à un autre.
- Les options de recherche : on peut ajouter une option spécifique à la recherche en utilisant des mots-clés. Par exemple, si vous tapez « définir : oiseau », le moteur de recherche cherchera la définition d'« oiseau » plutôt que le mot en général. Si vous tapez « site : wikipedia.org apple », Google ne cherchera que sur le site « Wikipédia ». Cette fonctionnalité est très pratique lorsque l'on

6. https://fr.wikipedia.org/wiki/Moteur_de_recherche

7. <http://www.advancedwebranking.com/blog/geo-location/>

8. <http://www.allaboutcookies.org/cookies/cookie-profiling.html>

9. <http://www.pcadvisor.co.uk/how-to/internet/how-delete-cookies-web-browsing-history-3218163/>

effectue une recherche sur des portails, comme nous le verrons plus tard. Il existe bien d'autres options de recherche, que vous pourrez retrouver en cliquant sur le lien fourni dans le paragraphe suivant.

- Les recherches spécialisées : la plupart des moteurs de recherche, y compris IXquick, Qwant, DuckDuckGo, Google, Yahoo! et Bing, ont des options de recherche spécialisée, comme la recherche de contenu multimédia (images, vidéos, etc.), de publications universitaires, de livres, de cartes, etc. Familiarisez-vous avec ces possibilités de recherche spécialisées car elles ont leurs propres options avancées. Il est possible, par exemple, de filtrer des images par taille, couleur, type de fichier et même par droit d'auteur et type de licence.
- Les outils de recherche : très utiles ; ils apparaissent directement en dessous de la barre de recherche une fois que vous avez tapé un premier mot-clé dans le cadre de recherche. On peut filtrer les résultats par pays et par période. Cette fonctionnalité est très intéressante si l'on cherche des informations dans l'actualité, car on peut restreindre la recherche aux nouvelles les plus récentes ou à celles publiées exactement un an plus tôt, par exemple.
- La recherche avancée¹⁰ : on y accède en cliquant sur « paramètres » en haut à droite. Elle regroupe toutes les fonctionnalités précitées dans une interface conviviale : par conséquent, utilisez-la si vous ne maîtrisez pas complètement l'utilisation des opérateurs ou des termes de recherche spécifiques.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Fixez un objectif de recherche sur un sujet donné et formez des équipes ; certaines utiliseront des portails/moteurs de recherche et d'autres quelques-unes des techniques de recherche d'information citées précédemment. Demandez-leur de comparer leurs résultats respectifs ainsi que la facilité d'accès et la qualité de l'information.
- Choisissez un sujet d'étude, par exemple l'image de l'enfant dans la peinture au XVIIIe siècle ou la dynamique de l'écosystème d'une espèce marine. Fournissez à la classe les adresses URL de portails¹¹ qui les guideront vers des liens en rapport avec la leçon. Comme il y aura sans doute trop de liens à examiner, formez des équipes qui se partageront le travail pour en couvrir le plus possible, puis demandez à chaque équipe de présenter ses résultats. Ils seront certainement différents, ce qui permettra d'affiner les connaissances acquises par les élèves.
- Prévenir ou guérir : demandez aux élèves d'effectuer une recherche sur leur propre nom pour voir s'ils trouvent des informations non souhaitées les concernant. Comment éviter que ces informations soient accessibles à tous ? Comment les règlements sur la protection des données peuvent-ils les aider à obtenir la suppression de ces contenus indésirables ?



BONNES PRATIQUES

- Conservez une bonne dose de scepticisme quant aux informations que vous trouvez sur le web. Internet est un formidable espace de liberté pour exprimer des opinions et des idées. Exercez un regard critique sur les ressources trouvées et multipliez les sources pour ne pas propager des mythes ou vous laisser abuser par des affirmations mensongères.
- Évitez de tomber dans le plagiat en copiant des travaux déjà réalisés. Il est important de mentionner, dans la mesure du possible, l'auteur et la source du matériel que vous citez ou utilisez ; ce faisant :
 - ▶ vous leur apportez la reconnaissance qui leur est due ;
 - ▶ vous vous protégez des accusations de plagiat ;

10. https://www.google.com/advanced_search?hl=fr ; [https://fr.wikipedia.org/wiki/Google_\(moteur_de_recherche\)](https://fr.wikipedia.org/wiki/Google_(moteur_de_recherche))

11. https://fr.wikipedia.org/wiki/Uniform_Resource_Locator

- ▶ vous permettez aux autres utilisateurs de se faire leur propre jugement sur la crédibilité du matériel en question.
- ▶ n'oubliez pas la question des droits d'auteur si vous utilisez du matériel trouvé sur Internet (voir ci-après le paragraphe « mode d'emploi » et la Fiche d'information 14 sur la vidéo, la musique et les images sur Internet).
- Prenez le temps de gérer/nettoyer vos cookies et votre historique de navigation. Vous pouvez désactiver les cookies complètement pour plus de confidentialité, mais sachez que cela pourrait nuire au bon fonctionnement de certains sites web.
- Variez les termes et les moteurs de recherche et utilisez les techniques de recherche avancée pour optimiser les résultats et avoir accès à une grande diversité de sources.
- Ajoutez les sites ou portails utiles à vos favoris pour les retrouver facilement.
- Parfois, votre recherche portera sur du contenu accessible depuis un portail, par exemple un document administratif officiel, la définition d'un mot, une comparaison de prix d'hôtels ou de tarifs d'avion ou encore des renseignements sur un produit en vue d'un achat. Pour toutes ces requêtes, vous pouvez utiliser aussi bien les moteurs de recherche que les portails les plus connus comme Booking.com, Wikipédia ou Amazon. De nombreux portails ont leurs propres moteurs de recherche internes, mais vous pouvez également utiliser un moteur de recherche classique et restreindre la recherche au portail en question. Vous pouvez taper par exemple « Hôtel Bruxelles site: booking.com ». Combiner les deux approches est une bonne méthode pour trouver ce dont vous avez besoin.
- Si vous trouvez des informations utiles, imprimez-les, enregistrez-les ou prenez-en une capture d'écran. Il se peut que vous ne les retrouviez plus par la suite ou qu'elles soient retirées du web sans préavis.
- Si vous ne trouvez pas la réponse à vos questions sur un moteur de recherche, posez-les dans un forum de discussion ou sur les réseaux sociaux.
- N'oubliez pas de contribuer à la création de contenus en ligne. Toutes les réponses que vous recherchez lorsque vous utilisez un moteur de recherche ont été rédigées et saisies par quelqu'un. En partageant vos connaissances et compétences, vous pourriez à votre tour aider quelqu'un (voir Fiche d'information 15 sur la créativité).



INFORMATIONS COMPLÉMENTAIRES

- Wikipédia est une encyclopédie gratuite rédigée de manière collaborative par ses utilisateurs dans le monde entier : <<http://www.wikipedia.org/>>.
- Le portail Europeana donne accès à de très nombreux documents numérisés représentatifs du patrimoine culturel européen : <<http://www.europeana.eu/portal/>>.
- Ces moteurs de recherche européens offrent un niveau de confidentialité élevé : <<https://www.qwant.com/>> et <<https://ixquick.com/>>.
- Il existe également un moteur de recherche américain du même type : <<https://duckduckgo.com/>>.
- Le site suivant vous explique comment utiliser le moteur de recherche Google : <<https://support.google.com/websearch/answer/134479?hl=en>>.
- Pour des conseils sur l'utilisation de Bing sous Microsoft Windows 8, voir : <<http://onlinehelp.microsoft.com/enus/bing/jj684589.aspx>>.

- Comment fonctionnent les moteurs de recherche ? voir :
<<http://web.archive.org/web/20160509142554/http://www.bbc.co.uk/guides/ztbjq6f>>.
- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :
Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.
Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile.
Article 17 – Les enfants ont un droit d'accès à des informations fiables provenant des médias. La télévision, la radio et les journaux devraient fournir l'information dans un langage que les enfants comprennent et les protéger contre les contenus qui nuisent à leur bien-être.
- Documents pertinents du Conseil de l'Europe :
 - ▶ Recommandation CM/Rec(2012)3 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche :
<https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caa93>.
 - ▶ Recommandation CM/Rec(2008)6 du Comité des Ministres aux États membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet :
<https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d3bc0>.

Trouver des informations de qualité sur le web



L'idée qui a présidé à la création d'Internet¹ était de constituer une bibliothèque électronique facilitant l'accès à l'information et sa diffusion². À bien des égards, cet objectif a été atteint : Internet fonctionne aujourd'hui comme une gigantesque bibliothèque où l'on retrouve la plupart des bibliothèques publiques et privées du monde. Celles-ci fournissent des informations sur leurs services, programmes et activités, et donnent accès à leurs catalogues d'ouvrages physiques qu'il est possible de réserver en ligne. Les bibliothèques numériques, quant à elles, donnent accès à des ouvrages et collections en ligne, le plus souvent numérisés au format HTML³ qui leur donne l'apparence d'une page web⁴, ou sous forme de documents Word ou PDF⁵ ou de texte brut (ASCII)⁶.

1. http://www.livinginternet.com/i/ii_summary.htm

2. http://www.livinginternet.com/i/ii_summary.htm

3. https://fr.wikipedia.org/wiki/Hypertext_Markup_Language

4. https://fr.wikipedia.org/wiki/Hypertext_Markup_Language

5. <http://www.census.gov/main/www/pdf.html>

6. https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

Certains grands musées et bibliothèques vous permettent de consulter les versions numérisées d'ouvrages ou de collections d'objets rares⁷.

■ Internet surpasse toutefois les bibliothèques en termes d'offre et peut fournir des données à jour et fiables sur tous les sujets susceptibles de vous intéresser : actualités, technologies, loisirs, divertissements, arts, sport, etc. Ces informations sont disponibles sur une grande diversité de sources – parmi lesquelles les chaînes d'information en continu⁸, les journaux⁹, revues¹⁰ et agrégateurs de contenus, plus connus sous le nom de flux ou fils RSS (rich site summary, voir <www.whatisrss.com>) – elles aussi accessibles par le biais de nombreux sites web et plateformes de médias sociaux. Les utilisateurs s'abonnent à ces fils pour recevoir régulièrement en un même lieu et donc consulter plus facilement les contenus web les plus récents des journaux et blogs, podcasts et blogs vidéo en ligne qu'ils ont sélectionnés.

■ De nombreux Européens suivent aujourd'hui l'actualité nationale et internationale sur Internet, qu'ils utilisent aussi pour obtenir des informations sur la santé. Ils s'informent également de plus en plus par le biais des plateformes de médias sociaux. Les forums et groupes de discussion sur l'actualité permettent de tenir des échanges de qualité tout en développant l'aptitude au débat des élèves. Il en existe des centaines de milliers dans le monde et les groupes les plus actifs reçoivent des centaines de nouveaux messages par jour. Ceux-ci sont organisés en fils de discussion qui classent et affichent le nom de l'utilisateur et la date et l'heure d'envoi du message. La plupart des serveurs et navigateurs actuels peuvent vous indiquer les forums présentant un intérêt pour vos élèves¹¹.

■ Twitter est un autre moyen de rester informé de l'actualité sur Internet. Vous pouvez utiliser votre propre adresse Twitter pour suivre les médias, journalistes et experts des secteurs qui vous intéressent, ou vous inscrire à une liste Twitter pour pouvoir les suivre de manière anonyme¹². Les alertes Google peuvent être utilisées de la même manière pour suivre l'actualité sur des thèmes spécifiques, mais si les mots-clés ne sont pas définis de manière suffisamment précise, il se peut que vous receviez trop d'alertes pour que ce service présente un intérêt. Les plateformes de médias sociaux se dotent elles aussi progressivement de nouvelles fonctions pour vous tenir informé de l'actualité mondiale.



INTÉRÊT PÉDAGOGIQUE

- Les compétences requises pour effectuer des recherches sont les mêmes dans les bibliothèques en ligne que dans les bibliothèques traditionnelles. Il est essentiel que les enfants soient guidés par leurs parents et leurs enseignants pour acquérir ces compétences et les mettre en pratique dès leurs premiers pas sur Internet.
- Les sites <<http://vlib.org/>> et <<http://www.sldirectory.com/libsf/resf/libplans.html>> répertorient des milliers de bibliothèques spécialisées permettant d'approfondir tel ou tel aspect ou thème du programme d'études. Les cyberquêtes sont de projets de petite envergure qui utilisent principalement Internet pour trouver des informations et des ressources. Elles peuvent être créées par l'enseignant ou par les élèves, selon l'activité d'apprentissage choisie par l'enseignant¹³. Le modèle proposé à l'adresse <<http://webquest.org/>> vous aidera à créer des activités qui familiariseront les élèves avec l'utilisation des bibliothèques en ligne tout en développant chez eux un certain nombre de compétences fondamentales dans le domaine de la recherche, de l'archivage, de la lecture et de l'écriture, de l'analyse et de l'évaluation.
- Les groupes et forums de discussion sont utiles pour développer la pensée critique et l'aptitude au débat des jeunes, à condition de les encourager à vérifier les faits qu'ils avancent en consultant plusieurs sources différentes. Ils peuvent également constituer un espace d'échange et d'apprentissage au contact des autres.

7. <http://www.bl.uk/manuscripts/Default.aspx>

8. http://wwitv.com/news_tv_live/

9. <http://www.onlinenewspapers.com/french-index.htm>

10. <http://www.e-journals.org>

11. <http://www.newsforum.com>

12. <https://fr.wikipedia.org/wiki/Twitter>

13. <https://www.teachingenglish.org.uk/article/webquests>



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Les cookies (petits fichiers déposés dans votre appareil pour stocker des informations sur vous et vos habitudes) peuvent améliorer la navigation en mémorisant vos préférences ou en vous évitant d'avoir à vous identifier à chaque fois que vous visitez certains sites. Il faut savoir toutefois que les moteurs de recherche qui utilisent des cookies ne vous dirigeront que vers des sites du même ordre, ce qui pourrait progressivement restreindre votre vision de l'actualité et des enjeux du moment.
- Internet démocratise le journalisme en donnant aux personnes de tous âges la possibilité de contribuer activement à l'élaboration de contenus. L'offre d'information sur Internet revêt dès lors un caractère illimité qui fait ressortir plus que jamais l'importance d'apprendre à distinguer le contenu de qualité du contenu non fiable et l'information de la publi-information (contenu publicitaire ressemblant à de l'information objective).
- Les groupes ou forums de discussion sont rarement animés à plein temps par un modérateur et les utilisateurs ne sont donc pas surveillés en permanence. Dès lors, il existe un risque que ces espaces soient exploités pour des activités illégales comme la diffusion de matériel soumis à droit d'auteur, de propagande raciste et de matériel extrémiste ou à caractère pédopornographique. Un certain sens des responsabilités et un minimum de connaissance des conventions sociales acceptables sont nécessaires pour utiliser ces plateformes, l'anonymat qu'elles semblent offrir pouvant donner lieu à des comportements antisociaux, comme la diffusion de messages haineux et délibérément hostiles (flaming) ou le harcèlement¹⁴. Les élèves devraient également être amenés à réfléchir aux questions de protection de la vie privée lorsqu'ils utilisent de tels forums¹⁵.
- La plupart des bibliothèques conditionnent l'accès à leurs collections au respect de certaines règles¹⁶. Elles exigent au minimum le respect du droit d'auteur. N'oubliez pas que, sauf si les œuvres font partie du domaine public, vous n'êtes pas autorisé à les reproduire et de les distribuer sans l'accord de l'éditeur. Le respect du droit d'auteur est également une affaire de responsabilité personnelle. Utiliser le travail de quelqu'un d'autre sans en mentionner la source relève du plagiat. Citez systématiquement vos sources et instaurez cette habitude chez vos élèves.



MODE D'EMPLOI

- Usenet¹⁷ est un système de discussion diffusé dans le monde entier qui se compose d'un ensemble de « groupes de nouvelles » (newsgroups) classés hiérarchiquement par sujet. L'accès à ces groupes est défini par votre fournisseur d'accès à Internet (FAI) ou le serveur¹⁸ de votre établissement scolaire, université ou entreprise. L'accès à certaines plateformes est gratuit, tandis que les services « premium » sont accessibles par abonnement.
- Il existe de nombreux outils pour créer un flux RSS. La vidéo « Get organized: streamline your news feeds »¹⁹ explique étape par étape comment utiliser les outils les mieux adaptés à vos besoins.
- Pour créer une alerte Google, il faut commencer par créer un compte Google. Vous pourrez ensuite saisir les mots-clés pour lesquels vous souhaitez configurer l'alerte, avec la possibilité de paramétrer d'autres options. Google Alertes vous informe alors par courrier électronique ou par fil RSS lorsque ces mots apparaissent en ligne. Vous recevrez une liste d'URL contenant les nouvelles occurrences de ces termes, ou aurez la possibilité d'ajouter l'alerte à un lecteur de flux RSS de votre choix.

14. [https://fr.wikipedia.org/wiki/Flaming_\(informatique\)](https://fr.wikipedia.org/wiki/Flaming_(informatique))

15. <http://www.webwewant.eu/information>

16. http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright__Plagiarism

17. <https://fr.wikipedia.org/wiki/Usenet>

18. https://fr.wikipedia.org/wiki/Serveur_informatique

19. <http://web.archive.org/web/20151231202307/http://www.pcmag.com/article2/0,2817,2458165,00.asp>

- Choisissez l'un des thèmes que vous étudiez actuellement en classe et recherchez une bibliothèque parmi les catégories disponibles à l'adresse <<http://vlib.org/>>. Vous pourrez ensuite créer une cyberquête en vous appuyant sur les ressources trouvées dans cette bibliothèque ou travailler à partir de l'un des exemples figurant à l'adresse <<http://webquest.org/>> ou <<http://www.spiritsd.ca/teacherresources/default.asp>>. D'autres suggestions peuvent également être trouvées sur les moteurs de recherche²⁰. Enrichissez votre cyberquête en paramétrant une alerte Google ou en vous abonnant à une liste Twitter²¹, et comparez la qualité des informations reçues grâce à l'un et l'autre de ces outils.
- Le site multilingue de la Fédération internationale des associations et institutions de bibliothèques (IFLA)²² basée en Écosse recense des sites web d'information et autres activités de qualité sur une grande diversité de thèmes allant de l'art à l'histoire en passant par les sciences et les mathématiques. D'autres liens utiles peuvent être trouvés sur le site « Great websites for kids »²³ créé par un service de l'Association américaine des bibliothèques. Des informations complémentaires sur les bibliothèques et les services d'information sont consultables sur le site web de l'IFLA, considérée comme le porte-parole de la profession dans le monde.



BONNES PRATIQUES

- Avant d'encourager les élèves à consulter les bibliothèques en ligne, revoyez avec eux les bases de la recherche documentaire²⁴. Veillez également à ce qu'ils disposent de solides connaissances sur la protection du droit d'auteur.
- Assurez-vous de la présence d'un filtre antivirus sur tous les appareils que vous utilisez pour télécharger des fichiers. Avant tout téléchargement²⁵ sur le serveur de l'école, vérifiez avec l'administrateur réseau que le système est bien protégé et qu'il offre un espace suffisant pour le stockage et l'archivage²⁶ de fichiers.
- Lorsque vous confiez un travail de recherche d'informations à vos élèves, il est judicieux de leur fournir une liste d'URL²⁷ à consulter. Vous aurez ainsi l'assurance de les orienter vers des liens valides et du contenu approprié.
- Nombre de documents que vous téléchargerez seront en format Adobe PDF pour protéger le droit d'auteur. Assurez-vous d'avoir téléchargé et installé une version récente du logiciel Acrobat Reader pour que les élèves puissent ouvrir ces fichiers. Cela peut être fait à partir du site d'Adobe Systems²⁸.
- Les principes de sécurité de base que vous appliquez lors de la navigation sur Internet sont également valables pour les bibliothèques en ligne. Lisez la politique de confidentialité et les conditions d'utilisation des services, et analysez les fichiers au moyen d'un antivirus.
- Avant de vous joindre pour la première fois à un groupe de discussion, consultez la Foire aux questions (FAQ)²⁹ de celui-ci. Cela vous donnera une idée de la nétiquette du groupe. Tous n'ont pas les mêmes règles.
- Veillez à ce que vos messages soient les plus courts possibles tout en donnant le maximum d'informations pertinentes. Par exemple, lorsque vous cherchez la réponse à un problème technique, précisez le type de matériel et de logiciels utilisés.

20. https://fr.wikipedia.org/wiki/Moteur_de_recherche

21. <https://media.twitter.com/best-practice/create-and-use-twitter-lists>

22. <http://www.ifla.org/FR/activities-and-groups>

23. <http://gws.ala.org>

24. <https://www.pinterest.fr/explore/comp%C3%A9tences-de-la-biblioth%C3%A8que/>

25. <http://www.walthowe.com/glossary/d.html#download>

26. <https://fr.wikipedia.org/wiki/Archives>

27. <http://www.ifla.org/FR/activities-and-groups>

28. <http://gws.ala.org>

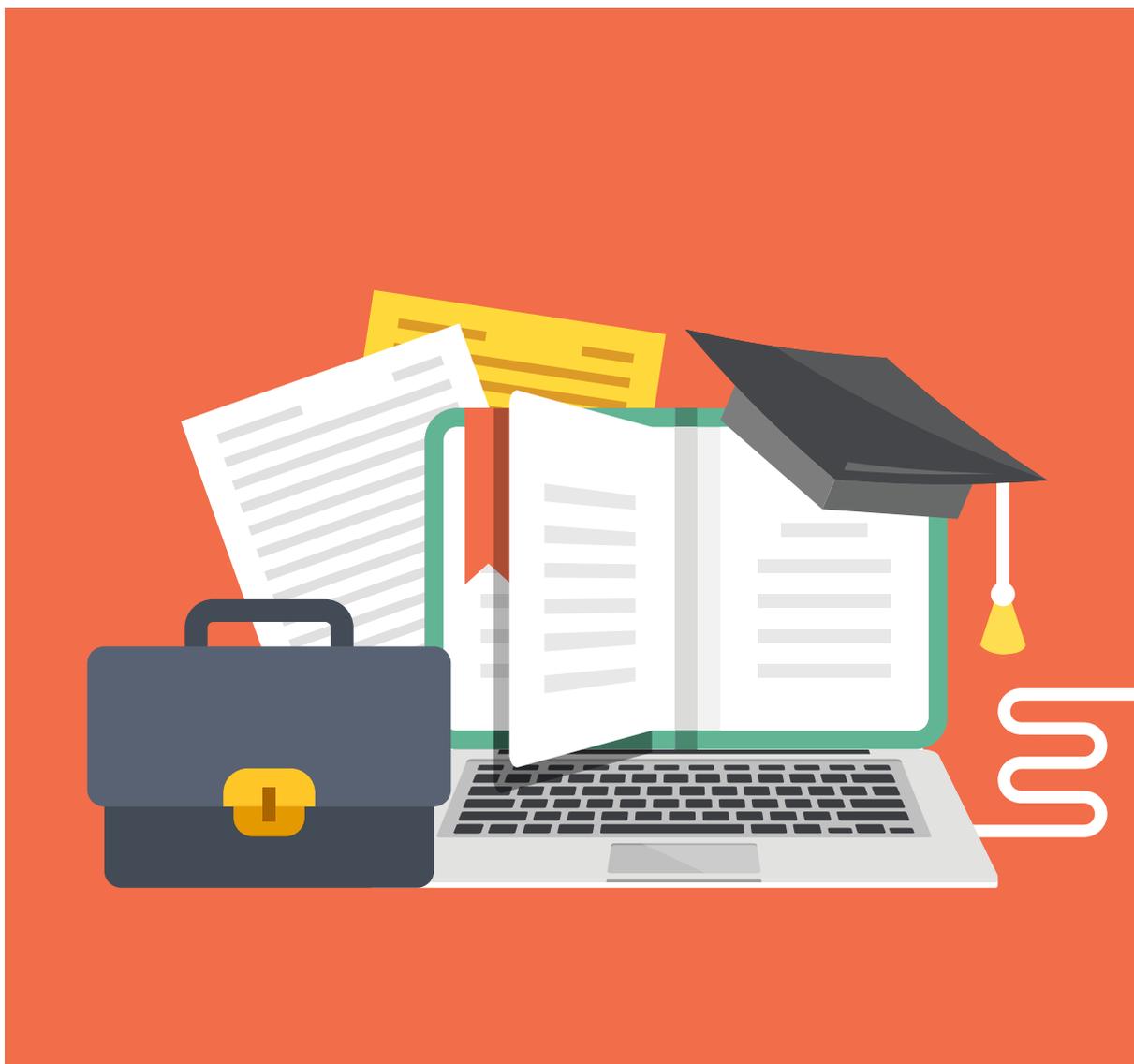
29. <https://www.pinterest.fr/explore/comp%C3%A9tences-de-la-biblioth%C3%A8que/>



INFORMATIONS COMPLÉMENTAIRES

- On trouvera une liste complète de groupes de nouvelles et des archives de près d'un milliard de messages sur Google Groupes <<http://groups.google.com/>>
- On trouvera une liste complète de groupes de nouvelles et des archives de près d'un milliard de messages sur Google Groupes <<http://groups.google.com/>>.
- David Lawrence et Russ Allbery donnent des conseils pour créer un groupe de nouvelles Big 8 : <<http://web.archive.org/web/20140330141231/http://www.faqs.org/faqs/usenet/creating-newsgroups/part1/>>.
- Article de Wikipédia sur les groupes de nouvelles : <<http://en.wikipedia.org/wiki/Newsgroups>>.
- Accès aux collections numérisées de la British Library : <<http://www.bl.uk/manuscripts/Default.aspx>>.
- Des milliers de textes sont disponibles sur le site de la World e-book Foundation : <<http://www.netlibrary.net/>>.
- The Library Spot est un centre virtuel de ressources documentaires gratuites : <<http://www.libraryspot.com/>>.
- « Teacher tap » a établi une liste de plus de 1 000 cyberquêtes et autres ressources : <<http://eduscapes.com/tap/topic4.htm>>.
- Dans la publication produite par des adolescents « Web we want », le chapitre « Information is not knowledge » <<http://www.webwewant.eu/web/guest/information>> propose des activités interactives pour aiguiser la pensée critique et exercer les compétences journalistiques des adolescents.

Apprentissage à distance et formations en ligne ouvertes à tous (MOOC)



L'apprentissage à distance est un mode d'enseignement formalisé dans lequel élèves et enseignants ne se trouvent pas physiquement ensemble dans une salle de classe. Le processus éducatif s'appuie sur des moyens électroniques. L'apprentissage à distance a suivi l'évolution des technologies. Il existe aujourd'hui des salles de classe virtuelles où les élèves et les enseignants échangent du contenu par courrier électronique, messagerie instantanée, vidéoconférences, dialogue en ligne, forums de discussion, etc.

Indépendamment de la technologie employée, l'apprentissage à distance reste une méthode éprouvée qui donne aux élèves de tous pays et de tous âges la possibilité de s'instruire tout au long de leur vie et d'obtenir des diplômes et certificats de la quasi-totalité des universités en ligne du monde. Les élèves peuvent également discuter avec d'autres élèves ou enseignants se trouvant à des centaines, voire des milliers de kilomètres de là, ce qui représente incontestablement un facteur d'enrichissement des apprentissages.

■ Les premières formes d'apprentissage à distance ont vu le jour au milieu des années 1800 lorsque des générations d'adultes ont cherché à se perfectionner depuis leur domicile, sur leur lieu de travail ou dans le cadre de leur service militaire. Les cours avaient généralement lieu par correspondance, le matériel pédagogique et les devoirs étant expédiés par la voie postale traditionnelle. Ces dernières années, l'apprentissage à distance a évolué pour tirer parti de l'ensemble des technologies disponibles. Avec la multiplication des offres sur Internet, les élèves peuvent aujourd'hui préparer un diplôme sans même pousser la porte d'une salle de classe.

■ Les diverses formes d'apprentissage à distance vont de la plus classique définie ci-dessus aux formations en ligne ouvertes à tous (MOOC) en passant par la formation entre pairs et les webinaires sur YouTube ou les sorties éducatives virtuelles sur PériScope. Bien que les technologies aient progressé rapidement, l'objectif fondamental de l'apprentissage à distance reste le même : éduquer.



APERÇU DES DIFFÉRENTES FORMES D'APPRENTISSAGE À DISTANCE

Formations en ligne ouvertes à tous (MOOC)

- Les MOOC ont été créés en 2008 pour diffuser du contenu par Internet à toute personne souhaitant suivre un cours, sans limite de participation. Des forums interactifs ont été créés pour permettre des échanges entre élèves et enseignants.
- En 2012, les MOOC étaient soutenus par des établissements de formation et des universités comme Stanford, Princeton, l'Université du Michigan et l'Université de Pennsylvanie se sont lancées dans un partenariat avec Coursera, entreprise de technologies éducatives.
- Parmi les autres programmes de MOOC ayant rencontré beaucoup de succès, on trouve Udacity, partenariat avec l'Université de Stanford et edX, fondé par l'Institut de technologie du Massachusetts et l'Université de Harvard.
- Les MOOC reposent sur un modèle élève-enseignant tandis que YouTube a créé une autre forme d'apprentissage à distance : la formation de pair à pair.

Formation de pair à pair

- Il s'agit de formations dispensées par certaines catégories de personnes à leurs semblables, par exemple des enfants qui enseignent à des enfants, des avocats à des avocats, etc.
- Ces modules se trouvent facilement sur YouTube où les « enseignants » aux millions d'abonnés proposent des tutoriels portant par exemple sur l'utilisation de tel ou tel logiciel, la conception web ou les techniques de maquillage ou d'écriture, ainsi que des milliers d'autres choses.

Webinars

- Les webinaires (séminaires web) peuvent être proposés par des coaches, enseignants, experts et toute autre personne souhaitant partager des connaissances en ligne.
- Exposés, cours magistraux, diaporamas PowerPoint, vidéos et ateliers comptent parmi les formats que l'on peut trouver sur Internet.
- Les webinaires peuvent également faire appel à des supports téléchargeables sur lesquels il est possible de travailler par la suite.

PériScope

- PériScope est une application qui permet à l'utilisateur de retransmettre en direct ce qu'il est en train de filmer. Elle a rencontré un succès sans précédent lors de sa première année d'existence et les enseignants sont en train de lui chercher des applications utiles.
- Certains considèrent que les sorties pédagogiques virtuelles, la classe ouverte ou la réception en temps réel des questions des élèves qui observent la scène filmée ont une utilité ; quoi qu'il en soit, c'est un outil d'apprentissage à distance dont l'évolution sera à suivre.

■ Les progrès de l'apprentissage à distance révolutionnent les environnements d'apprentissage, de l'école élémentaire à l'enseignement supérieur. Ainsi :

- des cours peuvent être donnés en diffusion en continu (streaming¹ ou au moyen de supports écrits enregistrés sur le serveur de l'enseignant².
- les élèves communiquent avec l'enseignant et entre eux par forums³, courrier électronique⁴ et salons de discussion⁵.
- les ressources éducatives libres sont des documents et des médias (généralement sous licence libre) utiles pour l'enseignement et l'apprentissage, l'évaluation et la recherche. Elles constituent pour les enseignants un nouveau moyen d'utiliser et d'échanger du contenu avec d'autres établissements et enseignants sur tous les continents. Elles sont quelquefois créées par des spécialistes n'appartenant pas au milieu enseignant, sur des sujets bien spécifiques. Le partage et le choix des ressources se font facilement dans des répertoires comme OER Commons⁶.
- les outils précités ont donné naissance à ce que l'on appelle la « classe inversée », une approche pédagogique mixte qui inverse le modèle d'enseignement classique : le contenu de l'apprentissage est mis à la disposition des élèves en dehors de la salle de classe, souvent en ligne, tandis que les activités proposées en classe se rapprochent plus des exercices qui, traditionnellement, sont donnés à faire à la maison. Pour en savoir plus sur cette méthode d'apprentissage, on consultera le site Edutopia⁷.
- les élèves peuvent déposer leurs devoirs dans une « drop box », service généralement gratuit où les utilisateurs inscrits peuvent sauvegarder leurs fichiers, les synchroniser et les partager facilement avec la ou les personnes de leur choix. Même des questionnaires et examens peuvent être informatisés et mis en ligne.
- dans les formations en ligne ouvertes à tous et l'apprentissage à distance, les supports de cours sont accessibles en permanence et peuvent donc être facilement mis à jour. Ces nouveaux environnements d'apprentissage offrent par ailleurs une souplesse inégalée qui permet à chacun de travailler à son rythme.



IMPORTANCE DE L'APPRENTISSAGE À DISTANCE

- Internet est l'outil idéal pour créer des environnements d'apprentissage virtuels. Il permet par exemple aux élèves de rester chez eux tout en suivant les cours d'une université virtuelle à l'étranger ou de partager leur temps de travail entre différents lieux, par exemple une entreprise et une école pour les étudiants en commerce.
- Un accès à l'intégralité du matériel pédagogique rend les élèves plus autonomes et leur permet de mieux comprendre ce qu'ils apprennent et pourquoi.
- Les élèves prennent davantage en main leur propre apprentissage et le rôle de l'enseignant devient davantage celui d'un accompagnateur.
- Les cours ne sont plus limités aux horaires classiques des écoles ou universités, ce qui augmente les possibilités d'apprentissage tout au long de la vie pour tous.
- L'apprentissage à distance modifie les comportements, des enseignants comme des élèves. Les premiers se familiarisent avec les technologies tandis que les seconds apprennent à s'organiser et à faire preuve de persévérance.

1. <https://fr.wikipedia.org/wiki/Streaming>

2. https://fr.wikipedia.org/wiki/Serveur_web

3. [https://fr.wikipedia.org/wiki/Forum_\(informatique\)](https://fr.wikipedia.org/wiki/Forum_(informatique))

4. [https://fr.wikipedia.org/wiki/Forum_\(informatique\)](https://fr.wikipedia.org/wiki/Forum_(informatique))

5. https://fr.wikipedia.org/wiki/Courrier_électronique

6. https://en.wikipedia.org/wiki/Online_chat

7. <https://www.oercommons.org>



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

Agréments

- Une distinction entre les programmes qui disposent d'un agrément et ceux qui n'en ont pas est utile pour juger de la légitimité d'un prestataire de cours.
- Des systèmes de badges numériques pour l'apprentissage à distance⁸ font leur apparition dans un grand nombre de domaines et constituent une mesure importante en faveur de l'égalité des chances en matière d'éducation.
- Lorsque des programmes n'ont pas d'agrément proprement dit mais sont partenaires d'universités renommées, ils prévoient souvent une forme de validation des compétences.

Enseignants et compétences

- L'apprentissage à distance ne modifie pas l'exigence fondamentale de compétence de l'enseignant. Bien au contraire, il souligne plus que jamais la nécessité de proposer davantage de formations aux enseignants afin qu'ils puissent rester au fait des nouvelles tendances dans le domaine de l'éducation.
- Bien que les formes traditionnelles d'enseignement présentent une valeur incontestable, il ne faut pas nier non plus les avantages des nouvelles technologies éducatives.
- Toute personne pouvant créer son propre webinaire ou son propre cours en ligne de pair à pair, voire s'autoproclamer « expert », il faudra ici aussi faire preuve d'esprit critique, comme avec les autres formes de contenu web.



MODE D'EMPLOI

— Certaines précautions s'imposent dans le choix d'un diplôme ou d'un programme d'apprentissage à distance :

- Il existe, parallèlement aux organismes sérieux, des organismes d'apprentissage à distance beaucoup plus douteux. Renseignez-vous bien sur le programme/l'organisme envisagé avant de vous inscrire ;
- Comme pour tout échange d'informations par Internet, les questions de sécurité sont primordiales. Les virus (voir Fiche d'information 19 sur la sécurité) et les hackers⁹ pouvant causer des dommages considérables à un système d'apprentissage à distance, vous êtes invité à consulter les Fiches d'information 9 sur la vie privée et 19 sur la sécurité pour connaître les mesures à prendre ;
- Le droit d'auteur¹⁰ est généralement protégé par les lois en vigueur dans le pays de l'étudiant. Cela dit, si ce dernier suit des programmes d'apprentissage à distance à l'étranger, il sera utile de vérifier que les ressources pédagogiques sont protégées par les lois internationales relatives aux droits d'auteur.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Invitez les élèves à travailler en binômes, l'un jouant le rôle de « l'enseignant » et l'autre de « l'élève ». Demandez-leur d'effectuer une recherche sur un thème du cours et d'indiquer pourquoi, selon eux, telle ou telle forme d'apprentissage à distance serait plus adaptée pour traiter ce sujet en particulier.
- Une fois que les élèves se sont mis d'accord sur le thème du cours et la méthode d'apprentissage à distance convenant le mieux, demandez au groupe des « enseignants » de définir les caractéristiques d'un cours idéal et au groupe des « élèves » de faire de même. Comparez les besoins des enseignants et des élèves.

8. <http://www.edutopia.org/blog/flipped-learning-lets-talk-tech-jon-bergmann>

9. <https://wiki.mozilla.org/Badges>

10. [https://fr.wikipedia.org/wiki/Hacker_\(sécurité_informatique\)](https://fr.wikipedia.org/wiki/Hacker_(sécurité_informatique))

- Choisissez une méthode d'apprentissage à distance et cherchez/vérifiez les diplômes existants. L'institution qui les délivre est-elle renommée ? À quoi le remarque-t-on ? Propose-t-elle des certificats ou badges ?
- Examinez les différences entre l'apprentissage avec une application et l'apprentissage en cours. Comment ces deux formes d'enseignement peuvent-elles ouvrir de nouvelles possibilités d'apprentissage aux personnes handicapées.
- Invitez les élèves à créer leur propre cours sur un thème de leur choix et encouragez d'autres élèves à suivre ce cours. À partir de cette expérience, invitez la classe à établir une liste de critères qui rendent l'apprentissage en ligne plus efficace.



BONNES PRATIQUES

- Internet modifie notre façon d'apprendre et il est très important que les élèves aient accès à l'ensemble des informations et des outils disponibles pour les accompagner dans leur cheminement.
- La « fracture numérique »¹¹ est considérée comme un problème crucial du développement social et économique de nombreux pays et le recours à l'apprentissage à distance pourrait être un moyen d'y remédier. Un point de vue opposé consiste à dire que certaines personnes n'ayant pas accès à Internet (et donc à l'apprentissage à distance) du fait de la fracture numérique, celle-ci ne fera que s'accroître.
- Chez les élèves, l'apprentissage à distance améliore l'acquisition des connaissances de manière quantifiable. Ils peuvent notamment, en même temps que les enseignants et les parents, se former directement au maniement des outils Internet.
- L'apprentissage à distance permet aux élèves d'acquérir de nouvelles compétences et qualifications pour s'engager dans de nouvelles voies.
- Grâce à l'apprentissage à distance, des personnes qui ne pouvaient jusque-là suivre un cours dans une salle de classe, comme les personnes handicapées, ont désormais elles aussi la possibilité de participer aux formations en ligne et d'échanger avec l'enseignant et les autres élèves.



INFORMATIONS COMPLÉMENTAIRES

- Le portail Distance Learning donne des informations sur les programmes et organismes d'apprentissage à distance dans le monde : <http://www.distancelearningportal.com/>.
- L'International Council for Open and Distance Education donne des informations et des ressources sur les organismes internationaux compétents : <http://www.icde.org/>.
- L'European Schoolnet, qui regroupe des ministères de l'éducation européens, propose un répertoire de ressources éducatives libres pour les enseignants : <http://lreforschools.eun.org/web/guest> ainsi que des ressources pédagogiques pour les élèves ayant des besoins spéciaux : <http://lreforschools.eun.org/web/guest/sennet>.

11. <http://fr.wikipedia.org/wiki/Copyright>

Achats en ligne



Le commerce en ligne peut se définir comme l'ensemble des services, logiciels et procédures qui permettent la vente de produits en ligne. Tout ou presque peut aujourd'hui s'acheter sur Internet, des livres aux séjours de vacances en passant par les vêtements et l'électronique. On peut également payer des services comme l'accès à du contenu en ligne.

Le commerce en ligne présente des atouts incontestables car il rend les achats plus simples et plus pratiques, mais les transactions ne sont pas sans risques. Ses avantages comme ses inconvénients s'accroîtront à mesure que ce secteur se développera.

Il apparaît que de plus en plus d'enfants font des achats en ligne (souvent au moyen de la carte de crédit de l'un de leurs parents) avant d'avoir atteint l'âge de 18 ans ou d'avoir leurs propres sources de revenus. Cette situation est préoccupante car elle risque d'aboutir à un phénomène de « virtualisation » de l'argent, dont les jeunes ne saisiront plus la valeur réelle. Au plan économique, cela pourrait avoir un impact majeur sur leur vie futur.



ACHATS INTÉGRÉS AUX APPLICATIONS

- L'achat intégré aux applications désigne la capacité d'un smartphone ou d'un appareil mobile à faciliter la vente de produits ou de services au sein même d'une application¹.
- Bien que les achats intégrés aux applications puissent apporter des revenus aux entreprises, ils peuvent poser problème aux personnes qui ne comprennent pas leur fonctionnement.
- En particulier, ils sont accessibles aux enfants et aux jeunes en quelques clics seulement, alors que ces derniers n'ont peut-être pas le droit d'effectuer ce type d'achats.



DROITS DU CONSOMMATEUR

- Les règles de protection du consommateur s'appliquent aux produits ou services achetés en ligne et incluent la livraison dans les délais convenus et la possibilité de renvoyer les marchandises non souhaitées et de ne payer que celles que l'on s'est expressément engagé à acheter. Par exemple, dans l'Union européenne, le délai de retour des marchandises est de 14 jours à compter de leur réception.
- Avant l'achat d'un produit ou d'un service en ligne, le vendeur doit vous fournir certaines informations de base sur ce dernier, qui doivent être claires, exactes et compréhensibles.
- Pour retrouver toutes les informations-clés, consultez les sites web de l'Union européenne mentionnés ci-dessous



COMPRENDRE LES ENJEUX : UN IMPÉRATIF

Les enfants et les jeunes doivent être des consommateurs avertis : ils doivent savoir s'ils sont autorisés à effectuer des achats en ligne, quelles sont les conditions générales de vente des services qu'ils utilisent et comment faire valoir leurs droits en cas de problème. Le commerce en ligne se développant chaque jour un peu plus, il est essentiel qu'ils comprennent comment devenir des consommateurs responsables et tirer parti des avantages tout en se prémunissant contre les risques liés à cette nouvelle forme de commerce.

- Les consommateurs peu avertis, en particulier les jeunes et les personnes âgées, sont plus vulnérables aux tentatives d'escroqueries en ligne et de fraude à la vente par Internet.
- En ligne, acheteur et vendeur ne se connaissent généralement pas et cet anonymat a tendance à faire perdre aux gens la notion de bien et de mal.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Protégez vos données de carte bancaire, numéros de téléphone et autres renseignements personnels. Les pirates peuvent intercepter vos données de carte bancaire en accédant à votre ordinateur ou en pénétrant dans des sites web non sécurisés qui détiennent vos informations. Faites attention aux sites web qui demandent à sauvegarder ces données car elles peuvent être volées.
- Évitez de payer vos commandes en utilisant une connexion Wi-Fi publique. Des zones d'accès à Internet sans fil étant présentes partout, dans des cafés, hôtels, aéroports et même des parcs publics, les pirates peuvent les attaquer et intercepter vos informations personnelles.
- D'autres techniques de fraude consistent à amener par la ruse les utilisateurs à dévoiler leurs données bancaires ou de cartes de crédit. Les attaques d'hameçonnage ou phishing² en font partie. Elles visent souvent les utilisateurs de sites d'achat ou de paiement en ligne, l'escroquerie consistant à leur demander de « reconfrmer » les informations confidentielles saisies.

1. <http://www.techopedia.com/definition/27510/in-app-purchasing>

2. <https://fr.wikipedia.org/wiki/Hameçonnage>

- Les achats en ligne étant souvent réglés par carte bancaire, les consommateurs doivent gérer leur budget pour éviter les dépenses excessives. Vérifiez régulièrement vos relevés bancaires pour vous assurer que vous n'avez pas effectué un achat involontaire ou non autorisé.
- Méfiez-vous des réductions « trop belles pour être vraies ». Allez sur le site du distributeur pour confirmer la validité de l'offre.
- Les méthodes de paiement sur Internet se sont multipliées : PayPal, bitcoins, transferts d'argent, paiement mobile, etc. Gardez à l'esprit qu'aucune méthode de paiement n'est complètement sûre : soyez donc vigilant lors de tout achat en ligne.



MODE D'EMPLOI

— Un certain nombre de précautions particulières s'imposent pour pouvoir acheter en ligne en toute sécurité :

- N'achetez qu'auprès de vendeurs réputés. N'hésitez pas à mener votre petite enquête, même si cela peut devenir difficile compte tenu de l'augmentation du nombre de commerçants en ligne.
- Configurez les paramètres de votre ordinateur, tablette ou smartphone de manière à garantir une sécurité optimale.
- Vérifiez que la zone de paiement de la commande est sécurisée par chiffrement. De nombreux sites utilisent la technologie SSL (Secure Sockets Layer). La présence de l'icône représentant un cadenas dans le navigateur et d'une URL commençant par « https » au lieu de « http » est le signe que la connexion au site est sécurisée.
- Conservez une copie de votre commande en l'imprimant ou en faisant une capture d'écran : elle vous servira de preuve en cas de réclamation.
- Consultez régulièrement vos relevés bancaires pour vous assurer que vous n'avez pas été indûment débité d'un achat que vous n'auriez pas fait.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Apprenez aux élèves à trouver des informations sur le vendeur et les conditions de vente.
- Invitez les élèves à travailler seuls ou en groupe pour rechercher des sites web commerciaux spécifiques à certains produits et services, en leur donnant un objectif particulier, par exemple, programmer des vacances en respectant un certain budget (voir également la Fiche d'information 10 sur la recherche d'informations).
- Planifiez la création d'un site de commerce électronique avec vos élèves (pour vendre du matériel scolaire, par exemple) ou poursuivez des initiatives de ce type déjà engagées dans votre établissement. Quelle est la structure d'un bon site de commerce électronique ?



BONNES PRATIQUES

- Renseignez-vous sur le vendeur. eBay, par exemple, note les fournisseurs sur la base de leurs performances passées et des retours des clients. N'achetez pas auprès de sources non fiables, notamment celles dont la publicité vous est parvenue par spam (voir Fiche d'information 19).
- Vérifiez que vous êtes bien assuré contre l'utilisation frauduleuse de vos cartes de crédit. Vérifiez l'absence d'achats non autorisés sur vos relevés bancaires.
- Lisez les conditions générales de vente. Elles peuvent vous paraître longues et techniques, mais ne cliquez pas sur « lu et approuvé » si vous ne les avez ni consultées ni comprises.

- Faites attention aux coûts cachés. Il peut s'agir de taxes ou de frais de livraison imputés par le vendeur. Des droits de douane peuvent également vous être facturés si vous commandez des produits à l'étranger.
- Le site est-il sécurisé ? Un cadenas ou un symbole « clé » dans le coin inférieur droit de votre navigateur web confirme que vous vous trouvez sur une page sécurisée. Vérifiez la présence de certificats SSL³ qui garantissent le chiffrement des données avant leur envoi.
- Veillez à conserver le contrôle de vos données personnelles et consultez le Règlement général sur la protection des données pour mieux vous informer sur la question. Faites attention aux cases à cocher qui autorisent le distributeur à conserver vos données ou à vous contacter à des fins commerciales.
- Si vous avez un doute quelconque sur le sérieux d'un site web, n'hésitez pas à effectuer quelques recherches en ligne pour trouver des témoignages, évaluations et expériences d'autres consommateurs. Des sites web comme Trustpilot, qui recensent les expériences des consommateurs, sont généralement de bons indicateurs du sérieux d'un site de commerce en ligne⁴.



INFORMATIONS COMPLÉMENTAIRES

- Consultez la page de l'Union européenne sur le commerce en ligne : http://europa.eu/youreurope/citizens/shopping/buy-sell-online/rights-e-commerce/index_en.htm.
- Expliquez à vos élèves ce qu'est le commerce électronique, par exemple à l'aide du site web de Microsoft : <http://web.archive.org/web/20050405134258/http://www.microsoft.com/office/previous/frontpage/columns/edcolumn04.asp>.
- L'ECC-Net « promeut la compréhension des droits des consommateurs européens et aide à résoudre les plaintes concernant les achats effectués dans un autre pays du réseau, lors de voyages ou achats en ligne » http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/ecc-net/index_en.htm.
- TrustArc (anciennement TRUSTe) est une initiative mondiale indépendante et à but non lucratif qui vise à renforcer la confiance dans les transactions en ligne : <http://www.trustarc.org/>.
- Le site Europea.eu donne des informations sur les achats en ligne : http://europa.eu/youreurope/citizens/consumers/shopping/index_en.htm.
- Pour des informations relatives au Règlement général sur la protection des données, voir : http://ec.europa.eu/justice/data-protection/index_en.htm.
- Conseils de PayPal pour prévenir la fraude : <https://www.paypal.com/eBay/cgi-bin/webscr?cmd=p/gen/fraud-tips-buyers-outside>.
- Pour plus d'informations concernant la Recommandation de l'OCDE sur la protection du consommateur dans le commerce électronique, adoptée en 2016, voir : <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.

3. https://fr.wikipedia.org/wiki/Transport_Layer_Security

4. <https://fr.trustpilot.com/>

4. Internet – Pour tous

” « Être créatif, c’est avoir le courage d’abandonner ses certitudes »

Erich Fromm, psychologue

LISTE DE POINTS À VÉRIFIER :

14 . VIDÉOS, MUSIQUE ET IMAGES SUR INTERNET

Vérifiez la licence de tout contenu que vous souhaitez réutiliser.

Appliquez une licence Creative Commons aux contenus que vous créez et publiez en ligne.

Soutenez les modèles de commerce en ligne aux pratiques loyales qui vous permettent d’acheter les productions de votre artiste, musicien ou créateur de contenus favori.

15. CRÉATIVITÉ

Une image vaut mille mots, en particulier si l’on ne fait pas attention à ses données personnelles et à celles des autres.

Savez-vous comment faire en sorte que les autres respectent les droits de propriété sur vos créations ?

Le plagiat est un non-respect des droits de propriété sur les créations d’autrui. Il peut à divers titres, peser lourdement sur la société. Savez-vous comment ?

16. JEUX

L’équilibre de vie est important : le temps que vous passez à jouer en ligne empiète-t-il sur vos activités extérieures/en relation directe avec les autres ?

N’oubliez pas que les inconnus avec lesquels vous êtes amenés à communiquer dans le cadre des jeux en ligne ne sont pas toujours ce qu’ils prétendent être. Choisissez des jeux encadrés par un modérateur ou disposant d’un salon de discussion « sécurisé » qui propose des phrases prédéfinies pour les très jeunes enfants.

Les achats intégrés aux applications peuvent être un piège dans certains jeux pour qui ne se méfie pas. Avez-vous lu les conseils figurant dans la Fiche d’information 13 ?

17. CITOYENNETÉ NUMÉRIQUE

Connaissez-vous vos droits et devoirs en ligne ?

Avez-vous récemment vérifié votre empreinte numérique ? Tapez votre nom dans un moteur de recherche et voyez les résultats.

Quelles sont les compétences numériques nécessaires pour devenir un citoyen éclairé dans le monde numérique ?

18. LA PARENTALITÉ À L’ÈRE DU NUMÉRIQUE : UNE APPROCHE POSITIVE ET PROACTIVE

Adoptez une approche positive dans vos relations avec vos enfants dans le monde numérique et parlez avec eux de ce qu’ils font, des sites qu’ils visitent et des personnes à qui ils parlent en ligne.

Comprenez bien que même si la technologie a progressé à pas de géant, l’exercice des responsabilités parentales repose toujours largement sur les mêmes principes : rester présent dans la vie de ses enfants, les encourager à devenir de bons citoyens (numériques) et privilégier l’empathie et la bienveillance.

Que vous soyez parent d’un jeune enfant ou d’un adolescent, ayez conscience des défis qui pourront se poser du fait des technologies dans le développement de votre enfant. Utilisez les technologies de manière à favoriser ce développement et non à l’entraver.

Vidéos, musique et images sur Internet



Internet est aussi une plateforme multimédia qui propose de très nombreux moyens de communication dont l'échange de fichiers audio et vidéo, de photographies et d'images numériques. Les applications et plateformes en ligne facilitent grandement la production et la diffusion de ce type de contenus, transcendant les barrières linguistiques, culturelles et nationales. Elles soulèvent aussi des questions importantes, liées non seulement à la divulgation d'informations personnelles (voir Fiche d'information 9 sur la vie privée), mais aussi aux violations du droit d'auteur et aux contenus illicites ou préjudiciables.



DROITS D'AUTEUR

- Il existe dans ce domaine un certain nombre de lois et d'accords internationaux. En 1996, plus de 100 pays ont signé deux traités de l'Organisation mondiale de la propriété intellectuelle (OMPI) sur les contenus numériques¹.

1. <http://www.wipo.int/treaties/fr/index.html>

- Tout créateur de matériel audiovisuel bénéficie automatiquement de droits d'auteur sur son œuvre, à moins qu'il y renonce.
- Les lois de la plupart des pays prévoient le maintien des droits d'auteur pendant 50 à 70 ans après la mort du créateur.
- Il existe généralement plusieurs détenteurs de droits d'auteur sur une œuvre musicale. L'auteur, l'interprète, la maison de disques et l'éditeur possèdent tous une part des droits ou des droits « voisins ».
- Au-delà des aspects économiques, le créateur de contenu audiovisuel détient des droits « moraux »² liés au droit d'être reconnu en tant que créateur et au droit au respect de l'œuvre, qui ne peut être modifiée ni publiée sans son autorisation.
- La musique et les films peuvent être achetés en ligne (voir Fiche d'information 13 sur les achats en ligne). Vous trouverez sur Internet de nombreux sites de téléchargement payant d'œuvres musicales comme iTunes³ et Amazon⁴ mais également d'autres magasins en ligne proposant musique, images ou vidéos.
- L'achat de musique ou de films en ligne ne donne généralement pas le droit, ou un droit limité seulement, de les copier ou de les diffuser. Par exemple, le site de téléchargement iTunes d'Apple autorise la copie d'une séquence musicale achetée en ligne sur cinq ordinateurs maximum par foyer⁵.
- Compte tenu de l'évolution de la consommation de contenus multimédia, de nouveaux modèles commerciaux ont fait leur apparition. Au lieu d'acheter une chanson, on peut souscrire un abonnement mensuel à une plateforme de *streaming* en ligne qui permet d'écouter tous les titres de son catalogue musical ou de voir tous les films qu'elle propose. Des exemples de ces services sont Netflix⁶ pour les films et Spotify⁷ pour la musique. Il en existe bien d'autres, que vous pourrez trouver facilement sur le web.
- L'industrie de la musique a engagé des poursuites judiciaires contre des éditeurs de logiciels *peer-to-peer* (P2P) et des utilisateurs de ces systèmes. L'Internaute qui met à disposition les fichiers (*uploader*) a plus de risques d'être poursuivi que celui qui les télécharge.
- Creative Commons⁸ est une organisation à but non lucratif qui propose une alternative au droit d'auteur traditionnel.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Après une hausse de 6,9 % en 2014, les ventes de musique numérique représentent aujourd'hui 46 % des ventes totales de l'industrie du disque. Ces chiffres peuvent s'expliquer par la multiplication des sites légaux de vente de musique numérique ou de *streaming* (voir <http://www.ifpi.org/facts-and-stats.php>).
- L'industrie de la musique a réagi aux actes de piratage en engageant des poursuites judiciaires contre un certain nombre de sites web et de particuliers.
- L'utilisation de logiciels *peer-to-peer*⁹ peut compromettre la sécurité de votre ordinateur, l'un des principaux modes de propagation des programmes malveillants consistant à les dissimuler dans des fichiers de musique et d'images.
- Internet a fait considérablement évoluer la consommation de contenus multimédias. Plutôt que d'écouter en boucle leur CD préféré, les Internautes ont désormais accès à une grande diversité d'œuvres qu'ils prennent plaisir à découvrir. Ainsi, chaque jour, un Américain écoute

2. https://fr.wikipedia.org/wiki/Droit_moral

3. <http://www.apple.com/fr/itunes/>

4. <http://www.amazon.fr/>

5. <http://www.apple.com/fr/itunes/overview/>

6. <https://www.netflix.com/fr/>

7. <https://www.spotify.com/fr/>

8. <http://creativecommons.org/>

9. https://fr.wikipedia.org/wiki/Pair_à_pair

en moyenne trois heures et demie de musique¹⁰. Paradoxalement, c'est le piratage qui a en partie contraint l'industrie à revoir le modèle commercial « traditionnel » de l'achat d'un album complet et à mettre en place des plateformes de *streaming* illimité sur abonnements. N'oubliez pas qu'en choisissant une plateforme de *streaming* plutôt qu'une autre, vous contribuerez à renforcer le modèle économique sur lequel elle repose.



ÉDUCATION

- Les établissements d'enseignement sont autorisés, dans certains cas, à reproduire des œuvres et à les communiquer au public. Référez-vous à votre législation nationale ou à la Directive 2001/29/CE de l'Union européenne du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Les conditions suivantes doivent être remplies :
 - ▶ les œuvres sont utilisées uniquement à des fins pédagogiques ou de recherche scientifique.
 - ▶ la source, et notamment le nom de l'auteur, doit être indiquée, sauf si cela est impossible.
 - ▶ aucun avantage commercial ou économique, direct ou indirect, ne peut être tiré de l'utilisation de ce contenu.
- Avant de publier en ligne des photos d'un mineur, il vous faut obtenir l'autorisation écrite de son parent ou tuteur.
- Tous les contenus publiés sur le site web d'un établissement scolaire, y compris ceux provenant des élèves, relèvent de la responsabilité de l'établissement.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Discutez des aspects moraux. Le piratage de matériel audiovisuel est-il du vol ?
- Informez les élèves des risques liés aux virus et aux logiciels espions lors des téléchargements.
- Informez les élèves des amendes encourues pour téléchargement illégal de films et de musiques soumis à droit d'auteur.
- Les élèves sont invités à produire une œuvre artistique ou une création intellectuelle (poème, récit, dessin, vidéo, chanson, etc.) en équipes, puis à se renseigner sur les licences Creative Commons et à choisir celles qu'ils souhaitent appliquer à leur contenu. Lorsqu'ils ont fini leur travail, demandez-leur d'expliquer leur choix de licence : ils peuvent par exemple avoir opté pour une licence très restrictive car ils ont l'intention de vendre leur création, ou au contraire, autoriser plus librement les modifications et réutilisations en ayant conscience que leur œuvre pourra être réexploitée ou transformée par quelqu'un d'autre.



CONTENUS ILLICITES

- La définition précise du contenu illicite varie d'un pays à l'autre mais on y inclut généralement la pédopornographie, l'extrême violence, l'extrémisme politique, la diffamation ou l'incitation à la haine à l'encontre des groupes minoritaires.
- De nombreux pays ont mis en place un numéro d'urgence pour signaler les contenus illicites. Certains sont membres du réseau INHOPE¹¹.
- Intenter une action en justice contre un contenu illicite peut être long ou difficile, selon la nature du contenu et l'emplacement du serveur qui l'héberge. Les numéros d'urgence travaillent avec les fournisseurs d'accès à Internet et la police et sont les mieux placés pour s'attaquer aux contenus illicites.

10. http://www.digitalstrategyconsulting.com/intelligence/2014/10/us_media_consumption_trends_music_tops_the_charts.php

11. <http://www.inhope.org/gns/home.aspx>

- La plupart des plateformes en ligne disposent d'un arsenal de moyens pour détecter et supprimer les contenus illicites, parmi lesquels la modération humaine ou automatisée, les techniques PhotoDNA et VideoDNA et les dispositifs de signalement.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Sur l'échelle pénale, il convient sans doute d'établir une distinction entre contenus illicites et atteintes au droit d'auteur. Alors que les premiers seront toujours traités comme des infractions graves, notamment pour ce qui est du matériel pédopornographique ou du terrorisme, dans le domaine du droit d'auteur, il existe des notions telles que « l'usage raisonnable » et des dérogations pour un usage à but non lucratif ou à visée pédagogique. S'il est naturel pour les humains, en particulier les enfants et les jeunes, de tester les limites des différentes libertés, et notamment la liberté d'expression, il en est à ne jamais franchir.
- Les contenus illicites sont souvent liés à d'autres activités illégales comme la vente illégale d'armes ou de stupéfiants, dont une grande partie ont lieu sur le « darknet », une partie d'Internet non accessible via les moteurs de recherche traditionnels. La publication, le partage ou la recherche de contenus illicites peuvent donc facilement, par effet boule de neige, mener à des infractions très graves.
- Votre établissement scolaire ou votre entreprise devrait avoir établi une « charte de bon usage » traitant notamment des questions de droits d'auteur et des contenus illicites.
- Vérifiez la licence de tout contenu trouvé en ligne dont vous souhaitez faire usage. Il existe différents types de licences pour le contenu produit par des utilisateurs réguliers d'Internet : la forme la plus « libre » vous autorise à réutiliser et à modifier le contenu sans avoir à en informer le propriétaire, même dans des projets commerciaux. Certaines licences demandent à ce que le nom de l'auteur soit mentionné et restreignent l'utilisation aux buts non lucratifs, tandis que d'autres encore interdisent toute modification. Des moteurs de recherche comme Google ou Bing proposent de filtrer les images et les vidéos par type de licence. De nombreuses plateformes proposent également du contenu à l'achat pour vos projets.
- Veillez à protéger votre contenu par une licence de droits d'auteur. Vous pouvez opter pour le droit d'auteur traditionnel ou appliquer une licence Creative Commons¹² au matériel que vous créez, afin de préciser les usages que les autres pourront en faire.
- Bien qu'il puisse être tentant de rechercher de la musique, des images ou des vidéos « gratuites » en ligne, n'oubliez pas que vous finirez toujours par les payer d'une manière ou d'une autre, que ce soit en étant bombardé de publicité ou en risquant de voir votre ordinateur infecté par des logiciels malveillants susceptibles de voler vos données, voire en étant poursuivi par les titulaires des droits. Soutenir les plateformes qui proposent des services d'un bon rapport qualité-prix permet d'améliorer Internet en évitant de l'inonder de publicités chronophages ou de contenu préjudiciable, tout en assurant aux artistes une rémunération juste pour leur travail.
- Chaque jour, des utilisateurs du monde entier produisent du contenu en masse : vidéos diffusées sur les plateformes de *streaming* vidéo comme YouTube ou Dailymotion, photos et images diffusées sur les réseaux sociaux, ou musique téléchargée vers les plateformes de *streaming* musical. Il convient de rappeler que tout contenu téléchargé vers Internet est protégé, que l'utilisateur concerné lui ait appliqué une licence ou non. Le droit d'auteur ne s'applique cependant pas si l'auteur dit expressément renoncer à tous les droits sur le contenu qu'il a produit.
- Une limite supplémentaire à l'utilisation de contenus est la protection des données personnelles. Transférer une vidéo ou une photo compromettantes, par exemple, constitue une atteinte à la vie privée d'autrui. Cela pourrait également être une forme de cyberintimidation. De manière générale, il convient de toujours demander à la personne qui

12. <http://creativecommons.org/>

a publié le contenu à l'origine si elle vous autorise à le réutiliser, le modifier, le rediffuser ou effectuer toute manipulation similaire. Demander une autorisation en bonne et due forme et mentionner la source est plus qu'une obligation légale : cela contribue à créer un environnement plus positif et incitant à la créativité et à la participation en ligne. Pour des informations plus détaillées sur la protection des données, on consultera le site Justice de l'UE sur la réforme des règles de l'UE en matière de protection des données¹³.



BONNES PRATIQUES

- Les filtres des logiciels peuvent aider à bloquer certains sites illégaux mais ne sont pas la panacée. Aucun filtre ne peut vous protéger si vous recherchez délibérément du contenu illicite.
- En tant que parent, enseignant ou frère/sœur aîné, essayez de discuter de vos expériences en ligne avec votre famille et votre classe. Le terme « illicite » ne désigne pas uniquement les contenus qui enfreignent les droits d'auteur ; bien souvent, il inclut les contenus choquants ou préjudiciables, les logiciels malveillants, le spam et d'autres contenus indésirables du même type.
- Signalez tout contenu illicite à un numéro d'urgence (voir INHOPE ci-après) ou utilisez les moyens de signalement proposés par la plateforme que vous utilisez.
- Veillez à ce que votre établissement ait une politique stricte à l'égard des contenus illicites et que les élèves soient dûment informés des conséquences potentielles de la publication, du partage ou de la visualisation de tels éléments.
- Discutez des contenus préjudiciables et illicites. Les enquêtes montrent qu'un grand nombre d'élèves accèdent à ce type de contenus sur Internet, volontairement ou non, mais que peu en parlent à un adulte.



INFORMATIONS COMPLÉMENTAIRES

- Visitez le site de l'Organisation mondiale de la propriété intellectuelle (OMPI) pour plus d'informations sur le droit d'auteur et les questions connexes : <http://www.wipo.int>.
- Voyez ce que pense votre groupe de musique préféré du piratage de musique sur le site « les artistes s'expriment sur le piratage musical » : <https://www.upvenue.com/article/1590-musician-stances-on-music-piracy.html>.
- INHOPE est un réseau de services téléphoniques de signalement de contenus illicites sur Internet (numéros d'urgence ou hotlines) : <http://www.inhope.org/gns/home.aspx>.
- La page médias du Conseil de l'Europe donne des informations sur le travail de l'Organisation dans le domaine du droit d'auteur : <http://www.coe.int/media>.
- Le site web de la Commission européenne donne des informations sur les droits de propriété intellectuelle : http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_fr.htm.
- L'IFPI, qui représente l'industrie du disque dans le monde, propose un guide à l'intention des parents et des enseignants pour la découverte sécurisée et légale de musique sur Internet : <http://www.ifpi.org/music-andthe-internet-guide.php>.
- L'Agenda numérique européen de la Commission européenne donne des informations supplémentaires sur le droit d'auteur : <https://ec.europa.eu/digital-agenda/en/copyright>.
- Pour plus de précisions sur le « darknet », voir la page Wikipédia qui y est consacrée : <https://fr.wikipedia.org/wiki/Darknet>.

13. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.

Article 17 – Les enfants ont un droit d'accès à des informations fiables provenant des médias. La télévision, la radio et les journaux devraient fournir l'information dans un langage que les enfants comprennent et les protéger contre les contenus qui nuisent à leur bien-être.

Article 33 – Les États parties prennent toutes les mesures appropriées pour protéger les enfants contre les drogues dangereuses.

Article 34 – Les États parties protègent les enfants contre toutes les formes d'exploitation sexuelle et de violence sexuelle.

Article 36 – Les enfants sont protégés contre toute activité susceptible de nuire à leur développement.

Article 37 – Nul n'a le droit de soumettre un enfant à des punitions cruelles ou violentes. Les enfants qui enfreignent la loi ne doivent pas être soumis à des traitements cruels. Tout enfant privé de liberté sera séparé des adultes et a le droit de rester en contact avec sa famille.

Article 40 – Les enfants accusés d'infraction à la loi doivent bénéficier d'une assistance juridique et d'un traitement équitable dans un système judiciaire qui respecte leurs droits. Les gouvernements établissent un âge minimum au-dessous duquel les enfants ne peuvent être tenus pour pénalement responsables de leurs actes et prévoient des garanties minimales d'équité et de résolution rapide des procédures judiciaires ou autres.

Créativité



COMMENT INTERNET FAVORISE-T-IL LA CRÉATIVITÉ ?

— Internet offre une grande souplesse qui fait des salles de classe des espaces de moins en moins rigides. L'évolution rapide des technologies multiplie les possibilités pour les élèves d'étudier les sujets qui les intéressent et d'apprendre de manière non traditionnelle (voir Fiche d'information 3 « Web 2.0, Web 3.0 et plus »).

— Grâce aux outils modernes, les élèves peuvent créer du matériel de qualité professionnelle qui pourra être vu par des publics du monde entier. Ils peuvent également créer leurs propres produits en ligne et mener des expériences et simulations de tous types dans leur classe ou de manière interactive avec d'autres apprenants sur Internet.

— Internet donne à l'éducation une dimension mondiale et permet aux élèves de se connecter en temps réel avec d'autres élèves sur tout le globe. Pour profiter pleinement de ces opportunités, il est important que les jeunes Internautes deviennent des créateurs plutôt que de simples

consommateurs, un objectif à la base des nombreuses initiatives de codage (voir par exemple <<http://codeweek.eu>>) mises en œuvre aujourd’hui dans un grand nombre de pays.



STIMULER LA CRÉATIVITÉ DANS L'APPRENTISSAGE

- L'intégration réussie des technologies en classe permet aux élèves de montrer leur sens de l'innovation, d'affirmer leur individualité, d'exprimer leur créativité et de cultiver leur esprit d'entreprise.
- L'utilisation de logiciels de création et d'Internet motive les élèves et renforce les apprentissages de manière significative, en classe et au-delà. Le codage les aide à mieux comprendre le fonctionnement de la technologie et peut contribuer à en faire des utilisateurs plus responsables.
- La possibilité d'exercer sa créativité et de jouer un rôle plus actif dans le processus d'apprentissage favorise l'engagement et la participation, qui sont deux pierres angulaires de la citoyenneté.
- Internet et les technologies mobiles offrent aux enseignants et aux élèves de multiples occasions de créer et de mettre en ligne leur propre contenu audiovisuel. Ils peuvent également utiliser Internet pour contacter des artistes du monde entier et leur demander conseils et avis sur leur travail. Ces derniers peuvent avoir recours aux outils de vidéoconférence¹ et aux réunions virtuelles (voir Fiche d'information 12 sur l'apprentissage à distance) pour organiser des ateliers.
- L'utilisation des médias sociaux² et des plateformes sociales dédiées³ en classe encourage les élèves à travailler en collaboration sur des projets communs en ligne. Cela leur permet de mettre en avant tous leurs talents et d'échanger des idées pour stimuler le processus créatif.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- **Égalité** : tout le monde dispose-t-il de l'équipement et de la connexion nécessaires pour accéder à Internet ? Les jeunes du monde entier, indépendamment de leur âge, de leurs capacités ou de leurs besoins spéciaux, ont-ils les mêmes possibilités d'exprimer leur potentiel créatif, autrement dit, savent-ils utiliser l'ensemble des technologies disponibles pour produire leurs propres créations ?
- **Sécurité en ligne** : les filtres⁴ mis en place pour protéger les jeunes utilisateurs, et en particulier les très jeunes enfants et les enfants ayant des besoins éducatifs spéciaux, brident-ils d'une manière ou d'une autre l'accès au matériel nécessaire pour exprimer sa créativité ? Comment faire pour que les élèves bénéficient d'un accès sécurisé à l'ensemble des contenus dont ils ont besoin (voir Fiche d'information 20 sur la classification/étiquetage et le filtrage) ?
- **Formation des enseignants** : bien souvent, les élèves connaissent mieux Internet que leurs enseignants. Ces derniers doivent donc bénéficier d'une offre de formation plus complète pour pouvoir guider leurs élèves sur tous les aspects des TIC, y compris l'utilisation des téléphones portables (voir Fiche d'information 5 « Internet en mobilité » et Fiche d'information 12 sur l'apprentissage à distance).
- **Assistance technique** : un soutien technique adéquat doit être assuré dans les établissements scolaires pour la bonne conduite des programmes et projets.
- **Un environnement protecteur** : la créativité constitue pour les jeunes une manière de dire ce qu'ils ressentent. L'idéal serait d'y laisser libre cours. Cela n'empêche pas toutefois de rappeler les principes de tolérance, d'empathie et de respect des productions d'autrui, notamment dans le cadre des séances de réflexion de groupe. Un enseignant ou délégué de classe devrait toujours être présent pour orienter le travail de manière constructive.

1. <http://web.archive.org/web/20080614214250/http://www.netlingo.com/right.cfm?term=video%20conferencing>

2. <http://www.eun.org/teaching/smile>

3. <http://www.etwinning.net/fr/pub/index.htm>

4. https://fr.wikipedia.org/wiki/Filtrage_d'Internet

- **Protection de la vie privée** : le Web 2.0 et le Web 3.0 facilitent grandement la mise en ligne de photos et d'images. Les élèves doivent avoir conscience qu'une image vaut mille mots et qu'elle pourrait mettre en péril leurs données personnelles et celles des autres.
- **Droit d'auteur** : les jeunes doivent apprendre le plus tôt possible à respecter les droits de propriété intellectuelle et comprendre le coût du plagiat pour la société⁵.



RENFORCER LA CRÉATIVITÉ EN CLASSE

- La cyberquête⁶ est une activité reposant sur la recherche d'informations, qui permet d'intégrer Internet dans le travail en classe.
- L'apprentissage des bases du codage⁷ en vue de la construction d'un site web stimule la créativité des élèves, car cela leur demande notamment de réfléchir au graphisme et au contenu.
- Les élèves peuvent travailler en collaboration sur des projets de récits en ligne et d'autres contenus qui renforcent leurs compétences rédactionnelles et de production audiovisuelle. Les téléphones portables peuvent être utilisés, par exemple, pour enregistrer et échanger avec des étudiants étrangers des images et des vidéos portant sur certains aspects de la culture ou de la vie économique de leur pays. Cela peut les aider à apprendre par la pratique les notions de respect de la vie privée, de crédits photographiques, et bien plus.
- Encouragez les élèves à créer des questionnaires interactifs et des activités pour le Web au moyen de logiciels comme Hot Potatoes⁸ ou des histoires interactives à fins multiples au moyen de logiciels tels que ceux disponibles sur le site web Quia⁹.
- Les élèves de l'enseignement secondaire et supérieur peuvent créer leur propre environnement d'apprentissage en 3D grâce à des logiciels comme Active Worlds¹⁰. Ils peuvent créer le cadre qui leur semble idéal, aménager leur propre campus virtuel mais aussi collaborer avec d'autres élèves à des projets sur divers thèmes.



BONNES PRATIQUES

- Internet peut être utilisé comme simple outil de recherche pour trouver des informations sur différents sujets. Les élèves peuvent ensuite appliquer les connaissances qu'ils ont acquises en réalisant un exercice qui stimule leur créativité. La technologie offre aux élèves la possibilité et la liberté de pousser plus loin leur réflexion.
- Internet et les autres technologies modernes sont de puissants outils de communication qui ont porté à un niveau sans précédent les possibilités de collaboration entre élèves de pays et de cultures différents à la recherche de solutions créatives.
- Les logiciels à code source ouvert permettent aux élèves du monde entier, et en particulier aux enfants de familles moins aisées, d'exprimer leur créativité sans contrepartie financière. Grâce à des logiciels comme Open Office, Gimp, Audacity ou Blender, les enfants peuvent créer des documents, modifier des images ou des fichiers audio et même s'initier à l'animation 3D gratuitement. Ils peuvent également apprendre le codage et partager leurs connaissances en rejoignant une communauté de codeurs bénévoles désireux d'améliorer et de mettre à jour ces logiciels. N'oubliez pas de parler de ces alternatives à vos enfants/élèves.
- Les enseignants estiment que l'utilisation des technologies en classe dans le cadre d'activités pratiques donne aux élèves l'occasion de résoudre des problèmes et de se montrer innovants.

5. <https://www.teachingcopyright.org/handout/copyright-faq.html>

6. <http://webquest.org>

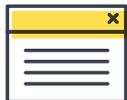
7. <https://scratch.mit.edu/educators/>

8. <http://hotpot.uvic.ca/>

9. <http://www.quia.com/>

10. <http://www.activeworlds.com/>

- Ne perdez pas de vue les objectifs d'apprentissage : le plus important n'est pas le résultat en lui-même, mais plutôt le processus qui y a conduit.
- Les élèves qui mettent en ligne les résultats de leurs activités de création doivent respecter le droit d'auteur¹¹. Invitez-les à se renseigner davantage sur les licences Creative Commons¹² et rappelez-leur de citer leurs sources lorsqu'ils utilisent du matériel créé par d'autres.



INFORMATIONS COMPLÉMENTAIRES

- Certains sites web sont d'excellents points de départ pour associer les élèves à des projets où la créativité est encouragée et la collaboration, essentielle :
- International Schools Cyberfair est un lieu de rencontre en ligne où les parents, les élèves et les éducateurs peuvent collaborer, interagir et mettre au point, publier et découvrir du matériel pédagogique : <http://www.globalschoolnet.org/GSH/>. European Schoolnet propose des ressources similaires pour les écoles : <http://www.eun.org>.
- Future Problem Solving Program International apprend aux élèves à résoudre des problèmes en stimulant leur pensée critique et leur créativité : <http://www.fpsp.org>.
- On trouvera des idées et des ressources pour promouvoir la créativité sur le site d'Education Scotland : <http://www.educationscotland.gov.uk/learningandteaching/approaches/creativity/>.
- Le News Horizons for Learning de l'école John Hopkins <http://education.jhu.edu/PD/newhorizons/> est un répertoire de pratiques didactiques novatrices pour promouvoir l'apprentissage créatif.
- Le chapitre 6, « The artist in you », du guide Web we want <http://www.webwewant.eu> propose un ensemble d'activités qui amènent les jeunes à s'interroger sur leur propre créativité ; il contient également des informations sur le plagiat, le droit d'auteur et bien d'autres sujets.

11. <https://fr.wikipedia.org/wiki/Copyright>

12. https://fr.wikipedia.org/wiki/Creative_Commons

Jeux



Les jeux vidéo peuvent être définis comme un divertissement reposant sur une interaction humaine avec une interface utilisateur en vue de générer un retour visuel sur un dispositif vidéo comme un écran de télévision, un ordinateur, une tablette ou un smartphone. Le terme englobe une grande diversité de genres, des jeux d'arcades aux jeux de rôle en passant par les jeux de stratégie et les mondes fantastiques. On appelle « sports électroniques » les compétitions – sportives ou autres – où les participants (souvent des joueurs semi-professionnels) s'affrontent en vue de remporter des sommes d'argent, devant un public en ligne toujours plus important. Les jeux peuvent être pratiqués seul, avec des partenaires en cercle restreint ou avec des milliers, voire des millions d'autres Internautes. Parmi ces jeux en ligne que l'on appelle « multijoueurs », on peut citer « World of Warcraft » et « Game of Thrones ». L'industrie du jeu vidéo est aujourd'hui le troisième plus grand secteur du marché du divertissement dans le monde, juste derrière la radiodiffusion et la télévision câblée, et a généré des ventes de 74 milliards de dollars américains en 2015 après avoir doublé ses recettes entre 2013 et 2014¹.

1. https://fr.wikipedia.org/wiki/Jeu_vidéo

■ Si l'on regarde de plus près l'évolution des tendances dans le domaine du jeu, on voit qu'elle est largement influencée par les smartphones et tablettes et l'utilisation croissante d'Internet par des personnes de tous âges. Des études de 2015² montrent que près d'un enfant sur trois de moins de 18 ans joue à des jeux en ligne mais que l'âge moyen des joueurs en ligne est de 31 ans. Auparavant dominé par les hommes, le secteur s'est également ouvert aux femmes qui représentent aujourd'hui la moitié des achats, 48 % des utilisateurs de jeux électroniques dans le monde et 52 % au Royaume-Uni. Les usages des consoles de jeux ont également évolué, leurs propriétaires consacrant désormais plus de la moitié du temps passé sur ces appareils à regarder la télévision, à visionner des vidéos en streaming et des disques Blu-ray ou à naviguer sur Internet³.

■ Les jeux sont également une activité de plus en plus largement pratiquée en famille et en classe. 74 % des enseignants des écoles K-8 affirment inclure les jeux en ligne dans les activités en classe, 4 sur 5 étant des jeux « éducatifs ». Par ailleurs, 56 % des parents affirment que les jeux ont un impact positif sur leurs enfants. Compte tenu de la popularité croissante des jeux et des répercussions qu'ils peuvent avoir sur les droits de l'homme, le Conseil de l'Europe a publié un ensemble de lignes directrices pour les prestataires de jeux, élaborées avec eux en collaboration avec des spécialistes de la protection de l'enfance, de l'éducation et des droits de l'homme⁴.

■ Tous ces chiffres montrent l'importance du secteur des jeux en ligne, qui compte chaque jour des millions d'utilisateurs sur Internet et téléphones portables.



DÉVELOPPEMENT PERSONNEL ET INTÉRÊT PÉDAGOGIQUE

- Le jeu est plus qu'un simple divertissement ; c'est une activité de groupe enrichissante qui plaît aux enfants et aux adultes de tous âges. Il favorise la créativité et l'interaction et joue un rôle important dans le développement social et intellectuel de chacun.
- Le jeu fait partie des rares moments où les adultes et les enfants peuvent échanger des idées sur un pied d'égalité (communication intergénérationnelle).
- Les enfants apprennent la démocratie en expérimentant diverses structures sociales dans un environnement encadré par des règles et des paramètres.
- Les jeux font souvent appel au partage et demandent de respecter les droits et les biens d'autrui ; certains permettent aux joueurs de découvrir d'autres cultures et des pratiques interculturelles. Les enfants peuvent y développer leurs aptitudes sociales sans crainte de l'échec et en ayant le sentiment de rester maîtres de la situation. Les jeux leur demandent d'obéir à des règles et des principes, ils renforcent leur aptitude à l'autodiscipline et leur autonomie.
- Les énigmes, jeux de société, jeux d'aventure et quêtes permettent aux joueurs de développer leurs capacités de réflexion stratégique et de résolution de problèmes. D'autres jeux peuvent être utilisés pour développer la motricité fine et l'organisation spatiale chez les enfants les plus jeunes, ou dans un but thérapeutique chez les personnes ayant un handicap physique.
- Certaines études semblent indiquer que les jeux, en particulier ceux comme Minecraft, peuvent avoir une utilité chez les personnes atteintes d'autisme.
- Les jeux en ligne permettent aux débutants d'apprendre les bases de la technologie et du codage, et plus généralement à renforcer leur intérêt pour les TIC⁵ et leur compréhension de ces dernières.
- Les jeux peuvent être intégrés à la quasi-totalité des disciplines du programme scolaire, des mathématiques aux langues en passant par les sciences humaines.

2. <http://web.archive.org/web/20160420163852/http://www.bigfishgames.com/blog/2015-global-video-game-stats-whos-playing-what-and-why/>

3. <http://web.archive.org/web/20151023082205/http://www.nielsen.com/us/en/insights/news/2015/game-consoles-in-2015-one-stop-shop-for-games-and-entertainment.html>

4. <http://www.coe.int/fr/web/portal/guidelines-for-providers>

5. https://fr.wikipedia.org/wiki/Technologie_de_l'information



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- L'existence de liens entre les jeux vidéo et les addictions, les agressions, la violence et l'insociabilité, ainsi que d'autres stéréotypes et questions de moralité sexuelle font débat depuis des décennies sans qu'il n'ait jamais pu être démontré avec certitude que les jeux aient une plus grande influence sur ces comportements que les autres médias⁶.
- Il est important que les jeux soient adaptés à l'âge des enfants, en particulier chez les très jeunes.
- L'addiction est souvent citée comme risque. L'Association américaine de psychiatrie (APA) a conclu en 2013 qu'il n'y avait pas suffisamment d'éléments pour inscrire l'addiction au jeu dans la classification officielle des troubles mentaux mais a proposé le terme « trouble de l'usage du jeu sur Internet » et a appelé à la réalisation d'études complémentaires pour en définir les critères. La question de savoir dans quelle mesure ce trouble est causé par l'activité de jeu elle-même ou s'il résulte d'une manière quelconque d'autres troubles n'est pas tranchée⁷.
- Avec le jeu comme avec les autres activités sur Internet, le maintien d'un équilibre de vie est important. Le temps passé à jouer ne devrait pas empiéter sur les activités extérieures et en relation directe avec les autres.
- Certains jeux en ligne vous font entrer en contact avec des inconnus. Veillez à ce que les jeux qui encouragent l'interaction entre utilisateurs, notamment ceux qui sont destinés aux très jeunes enfants, soient animés par un modérateur ou prévoient un chat « sécurisé » avec phrases prédéfinies.
- Les achats intégrés à certaines applications de jeu font courir le risque que les enfants dépensent par inadvertance une grande partie de l'argent de leurs parents pour s'acheter des outils et des éléments à collectionner.



BONNES PRATIQUES

- Les systèmes d'étiquetage et de classification des jeux encouragent les acteurs de l'industrie du jeu à agir avec responsabilité, en exigeant d'eux qu'ils définissent et décrivent leurs produits. Cela permet également aux acheteurs d'évaluer le contenu des jeux et leur adéquation avec l'âge des utilisateurs, et de faire leurs choix en toute confiance sur le marché des jeux. Le système PEGI (Pan European Game Information) est le seul système de classification paneuropéen qui fournit des recommandations détaillées sur l'âge auquel convient le contenu de divers jeux. La notation de quelque 20 000 jeux peut être consultée sur son site web <www.pegi.info>. PEGI fait également partie de l'IARC (International Age Rating Coalition) qui propose un système global de notation et de classification par âge des jeux et applications numériques⁸. Les classifications PEGI sont désormais disponibles pour tous les produits du Google Play Store et du Marketplace de Mozilla Firefox. Les boutiques d'applications Microsoft Windows Mobile et Windows 10 devraient suivre sous peu.
- Contrôlez le nombre d'heures que l'enfant passe à jouer. Prenez des contre-mesures s'il ne participe plus à d'autres activités sociales ou s'il manque des cours pour jouer.
- Les communautés de jeu peuvent renforcer le sentiment d'appartenance des enfants et les amener à accorder trop facilement leur confiance. Rappelez-leur que ceux qu'ils considèrent comme leurs amis en ligne ne sont quelquefois pas ce qu'ils prétendent être. C'est pourquoi il est important de ne jamais communiquer d'informations personnelles en ligne.
- Les jeux en ligne deviennent une activité appréciée de toute la famille et permettent d'aborder le sujet de l'usage responsable d'Internet. Si vous craignez que vos enfants ou élèves

6. https://fr.wikipedia.org/wiki/Controverse_autour_du_jeu_vidéo

7. https://fr.wikipedia.org/wiki/Dépendance_au_jeu_vidéo

8. <http://www.globalratings.com>

consacrent trop de temps aux jeux électroniques, sachez qu'il existe de nombreux tests d'addiction au jeu que vous pouvez trouver facilement en effectuant une requête sur un moteur de recherche. Ils permettent également d'engager la discussion.

- Le Conseil de l'Europe a produit un jeu en ligne amusant et interactif⁹ pour promouvoir les droits des enfants et les protéger contre toute forme de violence.
- Choisissez un jeu de rôles pour votre classe ou votre famille sur un sujet d'actualité à l'adresse <<http://www.playdecide.eu>>. Vous pouvez également créer votre propre jeu sur le modèle de Play Decide et le partager avec d'autres en le chargeant sur ce site web.
- Les achats intégrés aux jeux, c'est-à-dire l'achat de nouveaux contenus, fonctionnalités, outils et/ou mises à niveau pour un jeu ou une application donnés, mais également dans certains cas d'autres articles disponibles dans des magasins en ligne ne faisant pas partie du jeu, sont une source de préoccupation croissante, surtout pour les parents. Les filtres de contrôle parental permettent souvent de les éviter.



INFORMATIONS COMPLÉMENTAIRES

- Consultez le site « Ask about games » <<http://www.askaboutgames.com/>> pour mieux comprendre les jeux vidéo.
- Pour une revue des études en cours sur les jeux, voir le site de l'International Journal of Computer Game Research : <<http://www.gamestudies.org/>>.
- La législation relative aux jeux vidéo est un vaste domaine qui peut comprendre des éléments de droit pénal, réglementaire, constitutionnel, administratif, contractuel et même, dans certains États, de droit de la concurrence. La section « politiques publiques » de l'ISFE (Interactive Software Federation of Europe – <<http://www.isfe.eu/objectives/public-policy>>) donne des informations utiles sur la législation européenne et internationale en vigueur.
- Le site web de la Pan European Games Information (PEGI) donne des informations sur la classification et l'étiquetage des jeux : <<http://www.pegi.info/pegi/index>>. PEGI Online, en complément de ce système, vise à renforcer la sécurité de l'environnement du jeu en ligne. Les fournisseurs de jeux obtiennent le label PEGI Online s'ils respectent les normes du code de sécurité de PEGI Online <www.pegionline.eu> prévoyant notamment une triple obligation de veiller à l'absence de contenus illicites ou offensants créés par les utilisateurs et de liens indésirables, de protéger la vie privée et de disposer d'un mécanisme indépendant de dépôt de plaintes.
- La vérification de l'âge est un défi pour l'industrie du jeu, comme pour tous les autres secteurs en ligne qui s'adressent aux jeunes enfants. Des projets pilotes sont en cours en Europe pour étudier la possibilité de mettre en place un « échange d'attributs » grâce auquel les sociétés qui distribuent ou qui fournissent un accès à des biens et services réservés aux publics d'un certain âge pourraient regrouper et échanger des informations pour améliorer l'efficacité des systèmes de vérification de l'âge.
- On trouve chaque semaine de nouveaux articles sur les jeux en ligne, qui sont le marché du divertissement le plus florissant. Pour un panorama complet des jeux qui se vendent le mieux, des nouveautés, descriptions, rapports de recherche et statistiques, consultez plusieurs sites. Vous pouvez commencer par les sites web Bigfishgames, IFSE, PEGI et Nielsen. Il est également possible de s'abonner aux fils d'actualité ou aux lettres d'information proposés par ces sites ou de paramétrer avec précision une alerte Google pour rester informé.

9. <http://www.wildwebwoods.org/popup.php?lang=fr>

Citoyenneté numérique



L'usage généralisé d'Internet et des nouvelles technologies de la communication est un puissant moteur de croissance et de création d'emplois, qui améliore la qualité de vie de nombreux citoyens. Beaucoup de gens ont pris l'habitude d'utiliser Internet quotidiennement mais il leur manque peut-être parfois une compréhension plus approfondie des notions de citoyenneté et de droits numériques..

La participation éclairée de tous les citoyens dans « l'environnement numérique » passe par l'acquisition de compétences bien plus vastes parmi lesquelles la capacité à analyser de manière critique la multitude d'informations auxquelles ils sont soumis (contenus audiovisuels), à se forger leur propre opinion, à s'engager dans la vie locale et à maîtriser les nouvelles formes d'interaction sociale. Il y a une vingtaine d'années déjà, une publication de l'UNESCO qualifiait ces quatre compétences – apprendre à connaître, apprendre à faire, apprendre à vivre ensemble et apprendre à être – de « piliers de l'éducation »¹. Être un citoyen dans le monde numérique, c'est aussi savoir manier les outils du web (voir la Fiche d'information 3 « Web 2.0, Web 3.0 et plus ») et comprendre les divers aspects de la protection de la vie privée dans l'environnement électronique (voir Fiche d'information 9).

1. http://www.unesco.org/education/pdf/15_62.pdf



QU'EST-CE QUE LA CITOYENNETÉ NUMÉRIQUE ?

- La citoyenneté numérique est un terme qui décrit la manière dont une personne devrait se comporter² lorsqu'elle fait usage des technologies numériques en ligne.
- Certains experts la décomposent en neuf éléments : l'accès au numérique, la consommation numérique, la communication numérique, la littératie numérique, l'étiquette en ligne ou nétiquette³, la loi numérique, les droits et responsabilités en ligne, la santé et le bien-être en ligne, ainsi que la sécurité numérique⁴.
- Au-delà de la question de savoir ce qu'englobe la citoyenneté numérique, il est évident qu'il est attendu, voire exigé de l'ensemble des Internautes qu'ils agissent de manière responsable lorsqu'ils utilisent Internet et les technologies de la communication.

Empreinte numérique (ou trace numérique)

- L'empreinte numérique désigne les données qui sont laissées par les utilisateurs sur les services numériques.
- On établit une distinction entre les traces numériques passives, créées lorsque des données sont recueillies sans que leur propriétaire en soit informé, et les traces numériques actives, créées lorsque les données personnelles sont diffusées par l'utilisateur lui-même pour partager des informations le concernant sur le web ou les médias sociaux⁵.

Identité numérique

- L'identité numérique est l'information utilisée pour représenter des personnes, organisations ou machines dans les systèmes d'information et les réseaux⁶.

Compétence (littératie) numérique

- La littératie numérique désigne l'ensemble des connaissances, compétences et comportements requis pour faire fonctionner des appareils numériques comme les smartphones, tablettes, ordinateurs portables et ordinateurs de bureau⁷.
- Les technologies de l'information et de la communication ont déjà investi tous les aspects de notre quotidien, modifiant le type de compétences nécessaires pour être des membres actifs de la société.
- Internet continuant d'évoluer grâce au développement des réseaux sans fil⁸, une importance croissante sera accordée à la capacité des individus d'utiliser les technologies actuelles pour recevoir et transmettre efficacement des informations, au-delà de la simple connaissance des médias et d'Internet.

Droits numériques

- Le Conseil de l'Europe a produit un guide intitulé « Droits de l'homme pour les utilisateurs d'Internet » qui explique dans un format convivial les droits et devoirs de chacun dans le monde numérique et souligne que les droits de l'homme s'appliquent de la même manière en ligne et dans le monde réel⁹.
- Le terme « droits numériques »¹⁰ désigne les droits de l'homme¹¹ qui permettent aux individus d'accéder aux médias numériques, de les utiliser, d'en créer et d'en publier, mais aussi d'accéder aux ordinateurs et autres appareils numériques ou réseaux de communication et de les utiliser.

2. https://fr.wikipedia.org/wiki/Internet_citoyen

3. https://fr.wikipedia.org/wiki/Électronique_numérique; <https://fr.wikipedia.org/wiki/Nétiquette>

4. http://www.digitalcitizenship.net/Nine_Elements.html

5. https://fr.wikipedia.org/wiki/Trace_numérique

6. https://en.wikipedia.org/wiki/Digital_identity

7. https://en.wikipedia.org/wiki/Digital_literacy

8. https://fr.wikipedia.org/wiki/Réseau_sans_fil; <https://fr.wikipedia.org/wiki/3G>

9. <https://www.coe.int/fr/web/internet-users-rights/guide>

10. https://fr.wikipedia.org/wiki/Droit_numérique

11. https://fr.wikipedia.org/wiki/Droits_de_l'homme

- Il touche en particulier à la protection et à la mise en œuvre des droits existants, comme le droit au respect de la vie privée¹², dans le contexte des nouvelles technologies numériques et en particulier, d'Internet¹³.
- En ce qui concerne les droits numériques des jeunes en Europe, le Manifeste de la jeunesse de l'UE est une « déclaration » en ligne de jeunes Européens sur les moyens d'améliorer Internet¹⁴.

Citoyenneté numérique et démocratie électronique

- La démocratie électronique englobe l'utilisation des technologies de communication électronique comme Internet pour améliorer les processus démocratiques dans une démocratie représentative ou une république démocratique. C'est une évolution politique, renforcée par les réseaux sociaux qui permettent aux utilisateurs d'exprimer leur point de vue et de commenter « publiquement » les sujets qui les intéressent. D'aucuns affirment en effet que l'utilisation des réseaux sociaux dans le cadre de la démocratie électronique pourrait permettre l'implication d'un plus grand nombre de personnes et donc déboucher sur des politiques plus adaptées, tout en renforçant la transparence et l'obligation de rendre des comptes.
- Aujourd'hui, les femmes et hommes politiques de nombreux pays utilisent les sites de réseaux sociaux pour nouer le dialogue avec les jeunes et solliciter leur avis. Certains le contestent mais il est important d'aller là où se trouvent les jeunes pour se mettre à leur écoute.
- L'une des préoccupations exprimées au sujet de la démocratie électronique concerne l'impact de la fracture numérique sur ceux qui ne peuvent avoir accès aux médias. Cependant, compte tenu de l'augmentation rapide du nombre de personnes de tous âges ayant accès à Internet, cet aspect ne saurait être considéré à lui seul comme un motif de non-reconnaissance des avantages des sites de réseaux sociaux dans la démocratie électronique.
- Dans la communication hors ligne, le pouvoir est souvent considéré comme hiérarchique alors qu'en ligne, il est disséminé et change constamment. De la même manière, en ligne, les frontières deviennent perméables, les rôles sont variables et ajustables ; ils ne reposent pas sur des éléments non verbaux ou des relations hiérarchiques. Ces caractéristiques montrent à elles seules les avantages d'utiliser les sites de réseaux sociaux pour promouvoir la démocratie électronique.
- Cela dit, pour que la démocratie électronique porte ses fruits, les utilisateurs doivent s'ouvrir à la communication non violente, accepter la contradiction et être disposés à participer à un débat pacifique et respectueux. Lorsque des communautés de personnes partageant les mêmes idées se forment et débattent sans considérer d'autres perspectives, cela peut affaiblir la démocratie électronique au lieu de la renforcer, voire conduire à une radicalisation des opinions.



INTÉRÊT PÉDAGOGIQUE

- Internet permet non seulement de publier beaucoup plus d'informations plus rapidement, mais aussi de les mettre à jour en permanence de manière à ce que les citoyens soient toujours informés des dernières évolutions survenues dans les domaines qui les intéressent.
- Tous les enfants bénéficient d'un droit à l'information et d'un droit à la participation en vertu des articles 13 et 17 de la Convention des Nations Unies relative aux droits de l'enfant.
- Autrefois, nous n'avions d'autre choix pour nous informer que de nous en remettre aux versions que la presse écrite donnait des événements et des déclarations ; aujourd'hui, nous pouvons bien souvent aller chercher l'information directement à la source.
- Les citoyens du monde entier devenant des journalistes du quotidien grâce à leurs smartphones équipés de matériel vidéo, nous sommes souvent inondés de scènes filmées en direct. Cela dit, il manque souvent dans cette forme de reportage les moyens d'analyser ce qui se déroule sous nos yeux et ce qui s'est passé avant et après la fin de l'extrait, comme le montrent les fils Twitter, les vidéos YouTube et Vine et d'autres plateformes de médias sociaux.

12. https://en.wikipedia.org/wiki/Right_to_privacy ou https://fr.wikipedia.org/wiki/Liberté_d'expression

13. <https://fr.wikipedia.org/wiki/Internet>

14. <http://www.youthmanifesto.eu/>

- Mieux informés, les citoyens peuvent participer davantage à la vie démocratique à l'échelon national, paneuropéen et international. Ils peuvent également utiliser Internet pour rechercher des informations objectives sur la plupart des questions qu'ils se posent.
- Les données géographiques, de trafic routier, culturelles et touristiques collectées par des entités publiques ou privées enrichissent considérablement la vie des citoyens. Dans certains pays, ils peuvent même aller sur Internet pour effectuer leur changement officiel d'adresse, demander le renouvellement de leur passeport ou accomplir d'autres formalités qui prenaient précédemment beaucoup de temps. On rappellera néanmoins que la communication de données personnelles en ligne impose un certain nombre de précautions (voir Fiche d'information 9 sur la protection de la vie privée et 19 sur la sécurité).
- Internet permet aux citoyens de participer à des échanges et débats en ligne sur des sujets concernant la vie publique ou locale, et même de prendre part aux élections grâce au vote électronique¹⁵.
- Au-delà de l'implication politique, il permet également de faire des achats, d'étudier (voir fiche d'information 12 sur l'apprentissage à distance), de participer à des débats culturels, de méditer ou encore de faire du yoga : toutes les activités ou presque y sont présentes.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- En ayant accès à des informations de qualité constamment mises à jour, les citoyens sont mieux à même d'exercer leurs droits fondamentaux. Il faut toutefois être conscient des effets négatifs que la technologie pourrait avoir sur ces droits :
- L'accès à l'information n'est pas le même pour tous. On appelle fracture numérique le fossé qui existe actuellement au sein de la société entre ceux qui ont accès à l'information et ceux qui n'y ont pas accès. Si la situation perdure, la démocratie risque d'être compromise car les plus défavorisés perdront progressivement leur autonomie d'expression. Sans accès direct à l'information, nous sommes moins aptes à nous forger notre propre opinion et donc plus facilement manipulables par ceux qui maîtrisent les nouvelles technologies. Par ailleurs, l'information provenant du secteur public est une ressource essentielle pour la vie démocratique et civique, et plus particulièrement pour l'activité économique. Si nous voulons garantir l'égalité des chances, nous devons faire en sorte que tous disposent d'un même accès à l'information et des compétences de base pour mener une réflexion critique.
- Sur le plan de l'accès à l'information, la technologie et les plateformes en ligne ne sont pas nécessairement neutres. Les algorithmes des moteurs de recherche ou la censure sur les réseaux sociaux déterminent l'information qui est affichée en premier.
- Les technologies de l'information et de la communication occupent aujourd'hui une place si importante dans nos vies que bientôt, seuls ceux qui les maîtrisent seront réellement capables de faire entendre leur voix. Cela dit, les TIC n'étant que des facilitateurs techniques, plus de communication ne signifie pas toujours respect de la liberté d'expression. Les principes tels que le débat et le discours pacifiques, la pensée critique et l'ouverture d'esprit sont primordiaux pour favoriser un environnement en ligne positif et la liberté d'expression.
- La multiplication tous azimuts des moyens de diffuser et d'échanger des informations nous impose de prendre soin de nos données personnelles et de notre droit au respect de la vie privée (voir « Bonnes pratiques » ci-dessous)

15. https://fr.wikipedia.org/wiki/Vote_électronique



MODE D'EMPLOI

- Pour devenir des citoyens engagés, tous les Internautes devraient connaître leurs droits et devoirs élémentaires en ligne. Il faut qu'ils comprennent bien ce qu'ils ont le droit de faire et mais aussi ce qu'ont le droit de faire le secteur privé, le gouvernement et les autres Internautes.
- Des connaissances de base sur les cookies et la manière dont les sites web peuvent collecter et utiliser nos données à caractère personnel sont indispensables (voir Fiche d'information 9 sur le respect de la vie privée).
- En ce qui concerne les jeunes enfants, pour éviter de compliquer les choses, il conviendrait simplement d'étendre au monde en ligne les principes de base de la bonne citoyenneté : respect, bienveillance et action réfléchie.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Invitez les élèves à examiner la Convention des Nations Unies relative aux droits de l'enfant pour voir quels articles sont directement liés aux droits numériques¹⁶.
- Demandez aux élèves de choisir plusieurs comptes Twitter, Facebook et/ou Periscope de personnes s'exprimant sur les questions de citoyenneté et engagez une discussion avec elles pour leur demander leur point de vue sur la citoyenneté numérique et les responsabilités des utilisateurs. Invitez les élèves à trouver d'autres questions à poser.
- Les élèves sont invités à consulter les sites web européens qui donnent des conseils sur les droits numériques, et notamment ceux du Conseil de l'Europe, de la Commission européenne et d'European Digital Rights.
- Le programme d'activités en ligne du Conseil de l'Europe sur les droits de l'homme¹⁷ est une ressource intéressante pour vos cours d'éducation à la citoyenneté. Vous pourriez également demander à vos élèves de rédiger leur propre charte des droits de l'homme et d'appliquer aux environnements virtuels les nouvelles connaissances qu'ils ont acquises sur les droits de l'homme, en examinant par exemple comment ils pourraient transformer Internet en un espace de jeu et de travail plus convivial.
- Dans le cadre de cours d'histoire sur la Révolution française, aidez vos élèves à établir une distinction entre faits et hypothèses en comparant les peintures héroïques de la prise de la Bastille avec les récits qui en sont faits actuellement. Ils devraient être capables d'expliquer pourquoi la prise de la Bastille a donné lieu à des interprétations diverses. Ce thème pourra être élargi à l'éducation aux médias, en examinant les différentes façons de présenter des faits, selon le but poursuivi, ou en s'interrogeant sur la fiabilité des informations qui nous sont données.
- Dans le cadre d'un projet de géographie, par exemple « un passeport pour le monde », invitez les élèves à discuter de l'image qui est donnée sur Internet de tel ou tel endroit du monde et à analyser les différences de traitement (éléments mis en avant, prises de position) qui peuvent exister d'un site web à un autre.
- Pour renforcer les compétences des élèves en matière d'analyse de contenus, choisissez un sujet puis recherchez les articles qui en traitent sur différents sites d'information et analysez-les en classe. Les approches sont-elles différentes selon les médias ? Pourquoi, selon vous ?
- Les téléphones portables faisant partie intégrante de la vie des élèves en dehors de l'école, discutez en classe de la manière dont ils peuvent s'en servir pour obtenir des informations sur la société et participer activement à la démocratie. Établissez une liste des services auxquels ils donnent accès et examinez leur impact sur la vie privée et la démocratie (voir Fiche d'information 5 « Internet en mobilité » pour plus d'informations sur les services mobiles).

16. <http://web.archive.org/web/20160501101507/http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-childrensrights>
17. <http://www.coe.int/fr/web/human-rights-education-youth/human-rights-education-youth-programme>

- Simulez un débat en ligne en affichant un message au tableau et en distribuant des post-it aux élèves. Chacun se verra attribuer un numéro et pourra se lever et lire le message après un nombre de minutes défini à l'avance, correspondant à son numéro. Une fois qu'ils auront lu le message d'origine et écouté toute remarque qui aurait pu être faite directement, les élèves pourront rédiger et publier leur propre commentaire et « répondre » à d'autres messages au fil de la discussion. Ils pourront également choisir de « soutenir » le message d'un autre élève, qui sera alors placé bien en vue à côté du message d'origine. Cet exercice vise à enseigner aux élèves les différences entre un débat en ligne et un débat dans la vraie vie, tout en abordant la question de la liberté d'expression et en leur montrant comment éviter de tomber dans le « flaming » et les autres comportements inappropriés en ligne.



BONNES PRATIQUES

- Le citoyen ne peut exercer le droit de regard dont il dispose sur ses données personnelles s'il ne sait pas quelles informations ont été recueillies le concernant. Dans l'Union européenne, le Règlement général sur la protection des données a été introduit en 2016, notamment pour aider les citoyens à faire respecter ces droits et d'autres droits fondamentaux liés au respect de la vie privée et à la protection des données¹⁸. On trouvera une synthèse des principales dispositions concernant les citoyens dans un communiqué de presse de la Commission européenne du 15 décembre 2015¹⁹.
- Lisez toujours les petits caractères des questionnaires pour savoir comment vos données personnelles seront utilisées, et n'oubliez pas de consulter la Fiche d'information 9 sur la protection de la vie privée pour en savoir plus.
- La communication et la transmission des compétences numériques à l'école, dans l'enseignement supérieur et au sein de la société civile sont essentielles pour accroître la participation au processus démocratique.
- Pourquoi ne pas suivre un cours en ligne sur la citoyenneté numérique et les droits numériques ?
- Un certain nombre d'établissements scolaires travaillent actuellement à l'élaboration de programmes de maîtrise d'Internet qui permettront à leurs élèves d'acquérir les compétences nécessaires pour vivre, travailler et jouer dans la société de l'information actuelle, et notamment :
 - ▶ les compétences nécessaires pour naviguer dans le labyrinthe d'informations disponibles sur Internet ;
 - ▶ la capacité à différencier information et désinformation ;
 - ▶ l'analyse de la pertinence et de la validité de l'information ;
 - ▶ les répercussions des outils en ligne sur la démocratie, d'un point de vue éthique ;
 - ▶ l'utilisation de l'information dans le travail d'apprentissage par projets ;
 - ▶ la compréhension et l'exploitation des multiples possibilités qu'offrent les navigateurs et Internet.

18. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

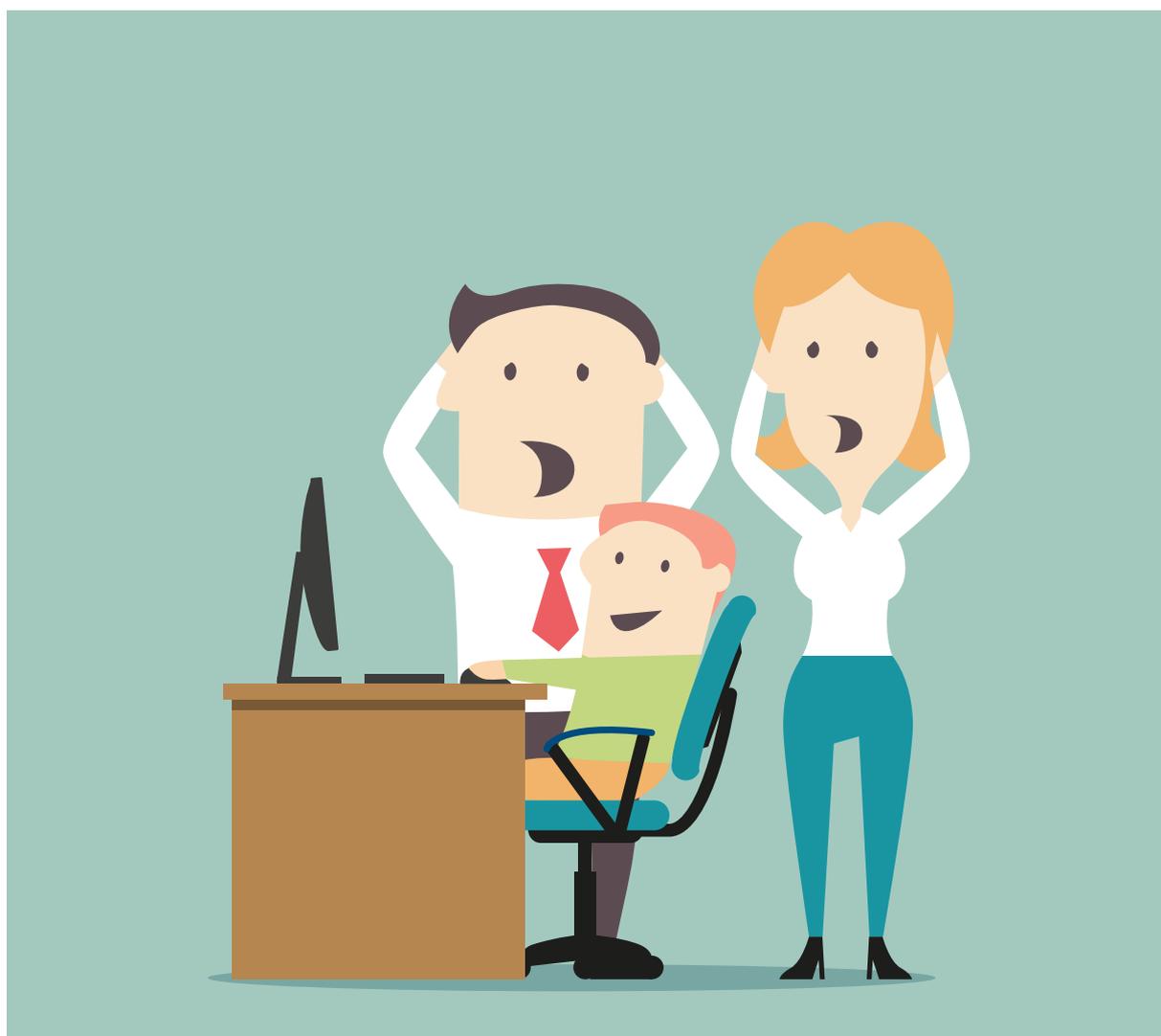
19. http://europa.eu/rapid/press-release_IP-15-6321_fr.htm



INFORMATIONS COMPLÉMENTAIRES

- Pour des informations relatives au Règlement général sur la protection des données, voir : http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
- Le Manifeste de la jeunesse de l'UE est une « déclaration » en ligne de jeunes Européens sur les moyens d'améliorer Internet : <http://www.youthmanifesto.eu>.
- Pour plus d'informations sur les droits numériques européens, voir : <https://edri.org>.
- Amnesty International à l'adresse <http://www.amnesty.org/> et Human Rights Watch <http://www.hrw.org/> sont des organisations non gouvernementales qui militent pour les droits de l'homme. Amnesty propose un manuel multilingue pour les enseignants intitulé « First Steps », qui vise à aider les jeunes à s'informer sur les droits de l'homme, notamment en Europe centrale et en Europe de l'Est.
- La Commission européenne donne des informations sur la protection des enfants et de la dignité humaine dans les services audiovisuels : http://ec.europa.eu/archives/information_society/avpolicy/index_fr.htm.
- On trouvera plus d'informations sur les droits de l'enfant dans la Convention des Nations Unies relative aux droits de l'enfant : <http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.
- Le Code des droits en ligne de l'UE est l'ensemble des droits et principes fondamentaux inscrits dans la législation européenne qui protègent les citoyens lors de l'accès à des réseaux et services en ligne et durant l'utilisation de ces derniers : <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Code%20EU%20online%20rights%20FR%20final.pdf>.
- On trouvera les neuf éléments de la citoyenneté numérique à l'adresse : http://www.digital-citizenship.net/Nine_Elements.html.
- La Déclaration de Paris, adoptée par la Commission européenne et le Conseil en 2015, promeut la citoyenneté et les valeurs communes de liberté, de tolérance, de non-discrimination et d'intégration par l'éducation : http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016_en.pdf.
- Parmi les documents pertinents du Conseil de l'Europe figure le guide « Droits de l'homme pour les utilisateurs d'Internet » : <http://www.coe.int/fr/web/internet-users-rights/guide> dont les principaux thèmes sont :
 - ▶ l'accès et la non-discrimination
 - ▶ la liberté d'expression et d'information
 - ▶ la liberté de réunion, d'association et de participation
 - ▶ la vie privée et la protection des données
 - ▶ l'éducation
 - ▶ les enfants et les jeunes
 - ▶ les voies de recours.

La parentalité à l'ère du numérique : une approche positive et proactive



Les « **enfants du numérique** » (en anglais « digital natives ») sont nés à l'ère de la technologie numérique. Ce sont les enfants qui, quelques minutes seulement après avoir pris en main une tablette ou un smartphone, n'éprouvent ni peur ni appréhension à manipuler la technologie. Ils font glisser leurs doigts sur l'écran sans toujours comprendre ce qu'ils font mais avec la confiance que quelque chose se produira devant leurs yeux. D'après Marc Prensky, « aujourd'hui, nos élèves sont tous des locuteurs natifs de la langue numérique des ordinateurs, des jeux vidéo et d'Internet » (Prensky, M. (2001) « Digital Natives, Digital Immigrants Part 1 », On the Horizon 9(5) p. 1-6, 1. Disponible à l'adresse : <<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>).

Les « **immigrés du numérique** » (« digital immigrants ») sont les personnes nées avant l'apparition de la technologie. Cette expression, également inventée par Prensky en 2001, désigne les générations de personnes qui n'ont pas grandi dans un environnement numérique. L'auteur les décrit très bien en affirmant : « ceux d'entre nous qui ne sont pas nés dans le monde numérique

mais qui ont, à un moment ou à un autre de leur vie, été fascinés par les nouvelles technologies et en ont adopté certains usages, voir tous, sont et seront toujours, comparé aux natifs, des immigrés du numérique » (Prensky (2001), 1-2 <<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>).

■ La « parentalité numérique » est l'idée de donner aux parents « immigrés du numérique » tous les outils dont ils ont besoin pour comprendre ce que font aujourd'hui leurs « enfants du numérique ». Le but est de protéger les enfants, de donner des moyens d'action aux parents et de maintenir la communication entre eux.

La parentalité à l'ère du numérique, c'est :

- communiquer ouvertement avec son enfant sur les avantages et les risques d'Internet ;
- s'intéresser aux activités de son enfant sur Internet ;
- prendre des mesures pour protéger la réputation et l'identité numériques de son enfant ;
- découvrir avec son enfant les possibilités qu'offre Internet ;
- faire en sorte que son enfant soit armé contre les dangers potentiels d'Internet ;
- exercer en ligne ses compétences parentales.

La parentalité positive, c'est :

- guider son enfant grâce à une discipline positive ;
- apprendre les comportements appropriés à son enfant, sans être sévère ;
- apprendre les comportements appropriés à son enfant dès son plus jeune âge, en lui montrant les conséquences des comportements inappropriés et l'intérêt d'agir de manière positive ;
- établir des attentes claires ;
- fixer des limites précises et appropriées ;
- se montrer cohérent.

■ Ces deux aspects sont clairement liés car dans le monde numérique, le parent et tuteur aura besoin de tous les outils disponibles pour se montrer proactif et positif tout en veillant à ce que son enfant fasse un usage responsable d'Internet et des appareils dotés d'une connexion sans fil.



COMPRENDRE LES ENJEUX : UN IMPÉRATIF

- Internet, les téléphones portables et appareils connectés en Wi-Fi étant omniprésents, les parents peuvent se sentir frustrés par leur manque de connaissances concrètes et d'expertise technique. Même ceux qui s'y connaissent en technologies pourront être décontenancés par la rapidité avec laquelle leurs enfants acquièrent la maîtrise d'Internet et des technologies.
- Les parents risquent de ne pas savoir comment réagir face à des enfants qui passent des heures à jouer à Minecraft lorsqu'ils dorment à l'extérieur, quelles limites fixer à l'envoi de textos le soir par un jeune de 17 ans ou encore s'il faut utiliser une application d'apprentissage de la propreté pour leur petit de 2 ans. Ils seront sans cesse confrontés à de nouvelles questions de ce type étant donné l'évolution constante de la technologie et son intégration progressive dans tous les appareils, qui deviendront de plus en plus simples à utiliser.
- Du fait de l'évolution des structures parentales, les parents peuvent avoir des difficultés à faire respecter les mêmes règles partout, que ce soit chez leur compagnon, chez les grands-parents ou dans d'autres environnements familiaux.
- La recherche concernant les incidences des usages en ligne sur le développement de l'enfant progresse en suivant l'évolution de la technologie mais il faudra encore attendre quelques années pour obtenir des résultats à long terme.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Les premières études montrent que l'utilisation d'un smartphone ou autre appareil pour « apaiser » les enfants peut nuire à leur capacité d'autorégulation¹.
- Élever un enfant aujourd'hui, c'est aussi en faire un citoyen numérique responsable, car il doit savoir comment utiliser Internet et les technologies de manière avisée et en toute sécurité.
- Les parents doivent aider leur enfant à comprendre ce qu'est la littératie numérique : la capacité à utiliser les informations à bon escient et à employer les technologies numériques de manière efficace, tout en devenant un citoyen du numérique.
- Le monde numérique et Internet ont également un impact considérable sur la parentalité dans le monde « réel », mais il serait absurde de vouloir séparer les deux. En effet, compte tenu des possibilités infinies offertes par le monde en ligne, les enfants peuvent se retrouver confrontés à certains contenus ou faire certaines expériences plus tôt que dans le monde « hors ligne ». Il peut s'agir de contenu « positif » (apprendre à lire à un âge précoce, à faire de la musique, découvrir une langue étrangère, etc.) mais aussi de contenus violents, effrayants ou à caractère sexuel, de manœuvres d'intimidation ou d'autres actes similaires.
- Soyez conscients de l'aspect commercial d'Internet. La plupart des services en ligne qui sont « gratuits » reposent sur des modèles économiques et structures de coûts opaques ou sur l'exploitation de données à caractère personnel à des fins publicitaires. Certains jeux dits « freemium », par exemple, inciteront votre enfant à dépenser beaucoup d'argent pour progresser dans le jeu tandis que les « publidivertissements » gommant la frontière entre jeu et publicité en faisant discrètement du placement de produit ou de marque dans un jeu.
- Pour les neuf composantes de la citoyenneté numérique, voir « Digital citizenship: using technology appropriately »² et la Fiche d'information 17 sur la citoyenneté numérique.
- Les conclusions des études récentes du Centre commun de recherche de la Commission européenne sur l'utilisation des technologies par les familles avec jeunes enfants sont très utiles pour comprendre les risques et les enjeux³.
- Dans son blog sur la parentalité⁴, EU Kids Online publie des articles sur les préoccupations des parents en Europe.



MODE D'EMPLOI

- Soyez un exemple pour vos enfants et limitez votre utilisation des technologies.
- Informez-vous sur l'actualité du cyberspace et discutez avec vos enfants de leurs activités en ligne.
- Voyez s'il existe un programme de sécurité en ligne dans l'établissement scolaire de votre enfant.
- Ne prenez la décision de retirer un appareil à votre adolescent ou préadolescent à titre de mesure disciplinaire qu'après mûre réflexion, car le priver de ses liens et réseaux sociaux pourrait avoir des conséquences inattendues.
- Parlez avec d'autres parents pour recueillir de bonnes pratiques à tous les âges.
- Pour apprendre à vos enfants à gérer le temps passé en ligne, procédez de la même manière que vous le feriez pour leur apprendre à gérer leur argent de poche. Accordez-leur une durée hebdomadaire de présence en ligne qu'ils pourront « dépenser » à leur guise.
- Soulignez l'importance du temps passé en famille hors ligne et maintenez vos activités de la semaine en famille.

1. <http://web.archive.org/web/20160424230408/https://www.theguardian.com/technology/2015/feb/01/toddler-brains-research-smartphones-damage-social-development>

2. http://www.digitalcitizenship.net/Nine_Elements.html

3. <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>

4. <http://web.archive.org/web/20160415215157/http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/26/svenjas-post-on-little-kids-european-comparison/>



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Demandez à vos élèves de rédiger un court article de blog destiné à leurs parents, dans lequel ils donnent des conseils sur la parentalité à l'ère du numérique.
- Engagez une discussion avec les élèves sur l'utilisation des technologies aujourd'hui. Quels sont les avantages ? Quels sont les risques ? Que peuvent faire les élèves pour tirer parti des uns tout en limitant les autres ?
- Après une discussion sur les bonnes pratiques en matière d'utilisation d'Internet, invitez les élèves à établir une liste des principales recommandations qu'ils souhaiteraient adresser à leurs cadets, nièces, neveux ou voisins plus jeunes. Comment les plus jeunes peuvent-ils profiter de l'expérience des plus âgés ?
- Demandez aux élèves de comparer la technologie des années 1960 à celle d'aujourd'hui. Les parents avaient-ils les mêmes préoccupations ? Pourquoi ?



BONNES PRATIQUES

- Parlez avec vos enfants de leurs interlocuteurs et de leurs activités en ligne, des sites qu'ils consultent et des horaires auxquels ils se connectent.
- Gardez le dialogue ouvert, même si vous n'êtes pas à l'aise avec le sujet, car c'est le meilleur moyen de rester informés des activités de votre enfant en ligne.
- De la même manière que vous parlez avec vos enfants des pratiques sexuelles sans risques, envisagez des discussions sur « l'Internet sans risques » et expliquez les dangers et le caractère inapproprié de certains contenus comme les photos, propos ou messages à caractère sexuel ou extrémiste.
- Soyez prêts à parler de questions comme la violence, le « flaming », l'intimidation, la sexualité, les stéréotypes et rôles sociaux liés au sexe, car vos enfants risquent d'y être confrontés par hasard en ligne et auront besoin de vos conseils pour acquérir une capacité de résilience et adopter un comportement positif face à ces éléments.
- Informez-vous sur l'utilisation des paramètres de sécurité et expliquez à votre enfant comment les configurer et pourquoi il est utile de le faire.
- Informez-vous sur le modèle économique des jeux, services ou sites web que votre enfant utilise. Pour les plus jeunes, assurez-vous que le contenu est sans publicité et sans frais cachés ou fonctionnalités « premium ». Il vaut mieux dépenser un peu d'argent pour lui offrir un jeu ou un abonnement mensuel à un service de qualité qu'exposer votre enfant à des tentatives d'exploitation commerciale.
- Assurez-vous que vos enfants comprennent les modèles économiques des services ou jeux qu'ils utilisent, ou des contenus qu'ils lisent.
- Assurez-vous que vos enfants ne publient pas d'informations en ligne de manière inconsidérée (données personnelles, caractéristiques d'identification, photos inappropriées, etc.).
- Trouvez un juste équilibre quant à l'utilisation d'Internet, vérifiez le temps passé en ligne et montrez vous-même l'exemple.
- Rappelez à vos enfants que tout ce qu'ils écrivent, publient ou partagent restera indéfiniment sur Internet et que ces contenus peuvent être modifiés et transférés à d'autres personnes.
- Apprenez à vos enfants à utiliser les outils mis en place pour signaler tout contenu inapproprié.



INFORMATIONS COMPLÉMENTAIRES

- Pour plus d'informations concernant l'effet des iPad sur le développement de l'enfant, voir le reportage d'information : <https://www.youtube.com/watch?v=VrQhmcPrhFw>.
- Pour lire l'article de Marc Prensky's « Digital natives, digital immigrants » (2001), voir : <http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>.
- La Confédération européenne des familles (COFACE) donne des informations utiles aux familles : <http://www.coface-eu.org>.
- The Parent Zone est un site britannique qui propose une grande diversité d'informations : <http://www.theparentzone.co.uk/>.
- Consultez la publication du Family Online Safety Institute : <https://www.fosi.org/good-digital-parenting/>.
- Vodafone a publié des conseils aux parents et des magazines sur la parentalité numérique : <https://www.vodafone.com/content/parents/howto-guides.html>.
- Le Centre médical de l'Université de Boston a publié un rapport sur l'utilisation des appareils portables : http://web.archive.org/web/20160607121811/http://www.eurekalert.org/pub_releases/2015-01/bumcmai013015.php.
- Le Centre commun de recherche de la Commission européenne a publié un rapport sur les jeunes enfants et la technologie numérique : <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>.
- « Play and learn: being online » contient des activités destinées aux 4-8 ans pour aider les parents et les enseignants à parler avec leurs enfants de l'utilisation responsable d'Internet : <https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=198308>.
- Guidez vos jeunes enfants vers des sites adaptés à leur âge ; il y en a beaucoup, parmi lesquels « Junior: safe search for kids » <https://www.juniorsafesearch.com/> et YouTube Kids <https://kids.youtube.com/>.
- Les documents pertinents du Conseil de l'Europe figurent sur la page web du Conseil de l'Europe consacrée à l'environnement numérique <http://www.coe.int/fr/web/children/the-digital-environment>

5. Internet – Répondre aux défis actuels

” « Refuser de reconnaître leurs droits fondamentaux aux individus, c’est remettre en cause leur humanité même »

Nelson Mandela, lauréat du prix Nobel de la paix en 1993, militant antiapartheid, président de l’Afrique du Sud de 1994 à 1999

« Les droits de chaque individu sont amoindris si ceux d’un seul homme sont menacés »

John F. Kennedy, président des États-Unis de 1961 à 1963

LISTE DE POINTS À VÉRIFIER :

19. CYBERCRIMINALITÉ : SPAM, LOGICIELS MALVEILLANTS, FRAUDE ET SÉCURITÉ

Avez-vous défini des mots de passe solides et différents pour chacun de vos comptes et mis en place une authentification à deux facteurs ?

Avez-vous étudié les paramètres de sécurité de vos appareils/comptes ?

Votre système d’exploitation et vos applications sont-ils à jour ?

Avez-vous effectué une sauvegarde de vos données les plus importantes ?

20. CLASSIFICATION/ÉTIQUETAGE ET FILTRAGE

Avez-vous réfléchi aux conséquences du filtrage au plan culturel et moral ?

Connaissez-vous la différence entre une « liste noire » et une « liste blanche » ?

Connaissez-vous les systèmes d’étiquetage/classification les plus couramment utilisés pour le contenu destiné aux enfants, et leur signification ?

21. HARCÈLEMENT EN LIGNE : INTIMIDATION, TRAQUE ET TROLLING

Votre famille ou votre établissement scolaire ont-ils mis en place des règles claires qui permettent aux enfants de comprendre les conséquences d’une éventuelle implication dans des actes de harcèlement en ligne ?

Protégez-vous suffisamment vos données personnelles ? De nombreux problèmes rencontrés en ligne résultent du partage inconsidéré de photos et d’informations.

Avez-vous cherché des moyens de développer votre intelligence sociale et émotionnelle pour surmonter les difficultés liées à l’anonymat des communications sur Internet, qui facilite de manière générale les actes d’intimidation, le trolling et le harcèlement ?

22. OBTENIR DE L’AIDE

Vos enfants/élèves savent-ils vers qui se tourner pour signaler des contenus illicites ?

Regardez-vous les statistiques fournies par les numéros d’urgence pour comprendre les nouvelles tendances et nouveaux risques dans le cyberspace ?

Quelles sont les cinq principales compétences numériques qui vous protégeront le mieux en ligne ?

Comprenez-vous suffisamment la géolocalisation et le Bluetooth pour utiliser vos appareils mobiles dans les meilleures conditions de confort et de sécurité ?

L’apprentissage mobile et les porte-monnaie électroniques sur appareils mobiles révolutionnent notre façon d’apprendre, de travailler et d’acheter. Que savez-vous de ces évolutions récentes ?

Cybercriminalité : spam, logiciels malveillants, fraude et sécurité



Internet est un moyen formidable d'accéder à des contenus et des services de qualité, mais il peut également être utilisé par des personnes mal intentionnées dans le but de commettre des escroqueries ou de diffuser du courrier indésirable, des virus et des logiciels malveillants.

- La **cybercriminalité** inclut les infractions contre les ordinateurs et les données, par exemple l'accès illégal à un ordinateur (également appelé piratage), l'interception d'une communication, le fait de bloquer le fonctionnement d'un ordinateur ou d'endommager ou de détruire des données, mais également les infractions commises au moyen d'ordinateurs, comme la fraude ou la violence sexuelle à l'égard des enfants. Les logiciels malveillants, le spam, l'hameçonnage et d'autres formes de vol d'identité font partie des outils et techniques utilisés par les cybercriminels.
- « **Logiciel malveillant** »¹ est un terme générique qui désigne différentes formes de logiciels hostiles ou intrusifs, parmi lesquels figurent notamment les virus et les chevaux de Troie.

1. https://fr.wikipedia.org/wiki/Logiciel_malveillant

Les objectifs des logiciels malveillants sont très divers : ils peuvent simplement chercher à perturber le fonctionnement d'un ordinateur en endommageant le logiciel ou le matériel, ou essayer de voler des informations et des données qui pourront d'une manière ou d'une autre être monnayées. Une fois infecté, votre ordinateur peut également devenir un « bot » contrôlé par des criminels à votre insu ; il peut alors être utilisé avec des millions d'autres ordinateurs dans un « réseau de bots » pour diffuser du spam, orchestrer une fraude ou attaquer des hôpitaux, des aéroports ou des banques.

- Le « **spam** » (ou « **pourriel** »)² désigne l'envoi massif de messages non sollicités à de multiples destinataires. Il est habituellement associé au courrier électronique mais s'applique également aux réseaux sociaux, à la messagerie instantanée, aux téléphones portables et autres. Fort heureusement, la plupart des services de messagerie disposent de filtres antispam efficaces. Le spam peut également servir de vecteur de propagation de logiciels malveillants, par exemple lorsque le destinataire ouvre une pièce jointe ou clique sur un lien contenu dans le message qu'il reçoit.
- *Phishing* (**hameçonnage**)³ est un terme tiré de l'anglais « fishing for passwords » (pêche aux mots de passe). Cette technique, qui est une forme de vol d'identité, consiste à envoyer à des destinataires des messages qui prennent la forme de courriers électroniques officiels d'institutions reconnues, par exemple une banque ou un réseau social. Dans bien des cas, ces messages contiennent des liens vers de faux sites web qui servent à recueillir des informations confidentielles sur l'utilisateur comme son numéro de carte de crédit ou ses mots de passe. Ces informations sont régulièrement utilisées à des fins de fraude sur Internet.
- La **fraude sur Internet**⁴ a fortement augmenté ces dernières années avec le développement du commerce électronique et la multiplication des offres de paiement en ligne. Elle englobe la contrefaçon, la fraude immobilière, les services « premium » de sonneries par SMS, la fraude aux transferts de fonds, etc.



COMMENT PRÉSERVER SA SÉCURITÉ ?

— Votre sécurité en ligne est comparable à la sécurité de votre domicile. Vous en protégez l'accès en gardant portes et fenêtres fermées. Une bonne dose de prudence, des capacités de réflexion critique et des compétences en TIC vous éviteront d'être victime de fraude, d'hameçonnage, de logiciels malveillants ou d'escroqueries en ligne.

— Nombre de points importants pour la sécurité le sont aussi pour la protection de la vie privée (voir Fiche d'information 9).



DÉVELOPPEMENT PERSONNEL ET INTÉRÊT PÉDAGOGIQUE

— La sécurité en ligne est un enjeu tant individuel que collectif. La propagation des logiciels malveillants, virus et spams est le plus souvent le fait des utilisateurs eux-mêmes. En effet, un ordinateur non sécurisé peut compromettre la sécurité d'autres machines, notamment celles des amis et contacts de l'utilisateur.

— L'étude des questions de sécurité en ligne peut être le point de départ du développement des compétences numériques des utilisateurs car elle les amène à se pencher en profondeur sur les paramètres et réglages de leurs appareils et sur les services en ligne qu'ils utilisent, tout en améliorant leurs connaissances techniques sur le fonctionnement de ces services, de leurs systèmes d'exploitation et d'Internet.

2. <https://fr.wikipedia.org/wiki/Spam>

3. <https://fr.wikipedia.org/wiki/Hameçonnage>

4. https://en.wikipedia.org/wiki/internet_fraud



RISQUES POTENTIELS

Spam (pourriels)

- Le spam n'a généralement pas de conséquences autres qu'une perte de temps à trier des messages ou à cliquer sur des liens.
- Le spam inclut souvent des informations fausses ou frauduleuses. L'expéditeur restant anonyme, il n'est pas possible de le poursuivre pour fausses déclarations.
- Les spammeurs profitent souvent de la bonne volonté des destinataires pour récupérer des adresses de messagerie qui alimentent ensuite leurs bases de données. Le destinataire peut recevoir un courrier lui demandant d'ajouter ses coordonnées à une liste pour soutenir une pétition ou une cause particulière. Évoquant souvent un motif humanitaire, par exemple un enfant malade ayant besoin d'une intervention chirurgicale, le texte du message indique qu'une société ou une organisation s'est engagée à verser une somme d'argent à chaque transfert du message.
- De nouvelles techniques de spam apparaissent chaque jour. Sur les réseaux sociaux, il peut prendre la forme d'un « détournement de clic » (click jacking)⁵, avec des messages partagés par des amis portant des titres accrocheurs comme « les 10 meilleures façons de perdre du poids » ou « vous ne croirez jamais ce que fait cette fille devant sa caméra ». En cliquant sur ces messages, vous pouvez soit être redirigé vers un site web qui vous inonde de publicité pour générer des revenus, soit être contraint d'apposer un « j'aime » à une page qui vous enverra d'autres messages du même type.
- Il existe de nombreux types de fraude en ligne et l'évolution de la technologie en crée tous les jours d'autres. L'une des plus courantes porte le numéro « 419 » du nom de la loi nigériane interdisant cette pratique. Le message promet en général une somme d'argent importante à qui aiderait à réaliser des virements bancaires. Une autre fraude consiste à demander à la victime d'envoyer de l'argent via Western Union à titre de dépôt de garantie avant de visiter un appartement à la location.

Hameçonnage (phishing) et vol d'identité

- L'hameçonnage ou le vol d'identité font courir des risques beaucoup plus graves. Selon les informations que vous avez fournies lors de la tentative de phishing, le préjudice peut aller de la perte de contrôle d'un compte en ligne relativement peu important comme celui d'un forum en ligne à la perte de contrôle d'un compte majeur comme celui de votre messagerie électronique, qui pourra ensuite être utilisé pour pirater tous vos comptes en ligne !
- Si vos comptes ont été piratés, vos données peuvent être mises en péril. Tout votre courrier électronique peut être téléchargé, par exemple, et les informations qu'ils contiennent être utilisées pour vous extorquer de l'argent, ainsi qu'à vos contacts, commander des articles au moyen de vos comptes en ligne ou de votre carte de crédit, endosser votre identité en ligne, etc.

Logiciels malveillants

- Les risques liés aux logiciels malveillants sont comparables à ceux de l'hameçonnage ou du spam, voire pires. Ces logiciels peuvent être utilisés à des fins d'hameçonnage pour accéder à des informations sur vos comptes (au moyen d'un enregistreur de frappe⁶, par exemple), à des fins de « spamming » pour vous bombarder de fenêtres intempestives ou de notifications et modifier les pages d'accueil par défaut de vos navigateurs, ou encore pour voler des informations et des données directement sur votre ordinateur, en perturber le fonctionnement ou en prendre le contrôle en vue de commettre des infractions, activer les micros ou des caméras de vos appareils pour vous espionner, voire détruire purement et simplement leur contenu.
- Les techniques visant à berner l'utilisateur pour lui faire installer des logiciels malveillants se développent rapidement elles aussi. Il existe par exemple de fausses fenêtres contextuelles qui reproduisent de manière réaliste une fenêtre d'analyse antivirus de votre ordinateur. À la fin de l'analyse, on vous dit que des virus dangereux ont été détectés sur votre ordinateur et on vous invite à installer un logiciel pour vous en débarrasser, lequel se trouve justement être un logiciel malveillant ou un virus !

5. https://fr.wikipedia.org/wiki/Détournement_de_clic

6. https://fr.wikipedia.org/wiki/Enregistreur_de_frappe



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Par groupes de trois ou quatre, les élèves sont invités à proposer un mot de passe fiable pour un compte factice en ligne. Précisez que ce mot de passe doit être nouveau et ne pas être l'un de ceux qu'ils utilisent déjà. Invitez chaque équipe à présenter son mot de passe et demandez au reste du groupe d'examiner les propositions et de recenser les caractéristiques d'un mot de passe fiable.
- Un mot de passe fiable :
 - ▶ se compose d'au moins huit caractères ;
 - ▶ ne contient pas de mot que l'on peut trouver dans un dictionnaire, de référence à votre vie privée ou à votre nom d'utilisateur, n'est pas votre véritable nom ou celui de votre entreprise ;
 - ▶ contient des caractères de chacune des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et symboles.
- Un CERT (computer emergency response team) également connu sous le nom de CSIRT (computer security incident response team) est un groupe d'experts qui gère les incidents de sécurité informatique. Demandez à vos élèves de trouver votre CERT/CSIRT national et informez-vous sur le rôle et le fonctionnement de ces équipes.
- Bien souvent, les victimes de cybercriminalité ne signalent pas les infractions à la police, si bien que leurs auteurs poursuivent leurs activités et trouvent de nouvelles proies.
 - ▶ Demandez à vos élèves de trouver la marche à suivre pour signaler une infraction à la police ou à une autre administration publique, notamment par l'intermédiaire des numéros d'urgence.
 - ▶ Demandez à vos élèves de trouver la définition de la cybercriminalité dans les lois de leur pays.



BONNES PRATIQUES

- Les utilisateurs espérant souvent pouvoir obtenir tout d'Internet sans rien déboursier, il est de plus en plus fréquent de voir des logiciels malveillants ou spams associés aux logiciels ou services « gratuits » en ligne. La sécurité de l'environnement en ligne est une responsabilité partagée et résulte des comportements et choix individuels de chacun. En soutenant financièrement des services/du contenu/des logiciels de qualité (par des dons à des initiatives open source ou des abonnements auprès d'organisations commerciales), il est possible de contribuer à rendre l'environnement virtuel plus sûr.
- La convivialité peut être l'ennemi de la sécurité. Vous pouvez configurer votre système d'exploitation de manière à ce qu'il vous demande un mot de passe administrateur à chaque action importante (par exemple, installation d'un nouveau logiciel). Cela peut sembler contraignant, mais c'est le prix à payer pour plus de sécurité. Souvenez-vous-en lorsque vous réglez les paramètres de sécurité de votre système d'exploitation.
- Si vous gérez plusieurs utilisateurs ou un réseau, veillez à ce que chaque utilisateur dispose de droits appropriés. La suppression de certains droits d'accès inutiles peut contribuer à éviter des problèmes de sécurité, volontaires ou accidentels.
- Vérifiez la fiabilité de la source avant de télécharger quoi que ce soit sur votre ordinateur. Soyez particulièrement vigilants lors de l'utilisation de logiciels peer-to-peer⁷, ces derniers étant connus pour favoriser la propagation de logiciels malveillants (voir Fiche d'information 14 sur la musique et les images). Quand vous installez un logiciel, lisez bien les instructions à chaque étape avant de cliquer sur le bouton « Suivant ». Faites particulièrement attention aux cases précochées qui pourraient installer des logiciels malveillants sur votre ordinateur !

7. https://fr.wikipedia.org/wiki/Pair_à_pair

- Installez un logiciel antivirus⁸ et mettez-le régulièrement à jour.
- Installez les correctifs de sécurité ou mises à jour des systèmes d'exploitation dès leur sortie. Vous pouvez paramétrer certains systèmes d'exploitation ou programmes de manière à ce qu'ils se mettent à jour automatiquement ou vous informent dès qu'un correctif est disponible au téléchargement.
- Installez un pare-feu⁹ pour contrôler le trafic entrant et sortant de votre ordinateur.
- Créez des comptes de courrier électronique différents pour chaque usage (par exemple, enregistrement sur des forums, formulaires à remplir, etc.) pour éviter de donner systématiquement votre adresse de courrier électronique « personnelle » et de la diffuser à grande échelle. N'oubliez pas que si vous publiez votre adresse de courrier électronique sur un site web, elle peut être repérée par des robots d'indexation et ajoutée à des listes de diffusion de spam. De la même manière, ne répondez pas aux spams car cela confirmerait votre adresse de courrier électronique à celui qui les envoie. Il faut savoir que les liens qui promettent de retirer votre adresse de messagerie des listes de diffusion ne sont pas tous authentiques.
- Si vous devez impérativement diffuser votre adresse de messagerie, vous pouvez la maquiller en y ajoutant des caractères, par exemple Tom[point]Smith[arobase]gmail[point]com, ou la poster sous forme d'image de manière à ce qu'elle ne puisse être copiée automatiquement.
- Soyez vigilant quand vous recevez du courrier électronique. N'ouvrez pas les messages dont la source vous semble douteuse. Vérifiez toujours l'adresse de courrier électronique de toute notification que vous recevez pour vous assurer qu'elle est bien réelle.
- Faites particulièrement attention aux pièces jointes. Si vous n'attendez pas de pièce jointe d'un expéditeur, ou si une pièce jointe vous semble suspecte, supprimez-la immédiatement sans l'ouvrir.
- Ne cliquez jamais sur les liens de destinataires en qui vous n'avez pas confiance, et en particulier sur les URL réduites qui masquent l'adresse d'origine. N'oubliez pas que même les destinataires auxquels vous faites confiance peuvent vous envoyer des messages infectés si leur compte ou leur appareil a été piraté.
- N'envoyez jamais d'informations privées comme un nom d'utilisateur, un mot de passe ou un numéro de carte de crédit par courrier électronique. Aucun service en ligne ne vous demandera jamais votre identifiant/mot de passe par ce biais, et il ne vous sera que rarement demandé de fournir des données comme le numéro de votre carte de crédit (celui-ci peut vous être demandé pour réserver une chambre d'hôtel, auquel cas vous devrez l'envoyer à l'adresse de courrier électronique officielle de réservation de l'hôtel).
- Utilisez un mot de passe différent pour chacun de vos principaux comptes et mettez en place une authentification à deux facteurs chaque fois que cela est possible (ajout de votre numéro de téléphone portable ou d'une phrase/question de sécurité). Veillez à ce que vos mots de passe n'aient aucun lien évident avec vous, qu'ils aient au moins huit caractères et utilisent une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles.
- Effectuez des sauvegardes régulières de l'ensemble de vos données sur un disque dur externe. Il existe de nombreux programmes de sauvegarde qui enregistrent automatiquement et régulièrement vos données. Certains sont même inclus dans votre système d'exploitation (Windows, MacOS, Linux, etc.). Informez-vous régulièrement sur les solutions proposées¹⁰.

8. https://fr.wikipedia.org/wiki/Logiciel_antivirus

9. [https://fr.wikipedia.org/wiki/Pare-feu_\(informatique\)](https://fr.wikipedia.org/wiki/Pare-feu_(informatique))

10. https://fr.wikipedia.org/wiki/Liste_de_logiciels_de_sauvegarde



INFORMATIONS COMPLÉMENTAIRES

- Truth or Fiction est un site web qui permet aux InternauteS de contrôler la véracité des informations contenues dans les messages les plus couramment transférés :
<<http://www.truthorfiction.com/>>.
- Pour plus d'informations sur la lutte contre le spam : <<http://spam.abuse.net>> et <<http://www.spamhelp.org/>>.
- Pour plus d'informations sur Microsoft et la sécurité, voir :
<<http://www.microsoft.com/security/>>.
- Pour plus d'informations sur Apple et la sécurité, voir :
<<http://www.apple.com/support/security/>>.
- L'ENISA, Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, fait régulièrement le point sur les questions de sécurité numérique :
<<http://enisa.europa.eu>>.
- Le Conseil de l'Europe dispose d'une page web intitulée « Lutte contre la cybercriminalité » :
<www.coe.int/cybercrime>.
- TechTarget est un magazine consacré à la sécurité de l'information :
<<http://informationsecurity.techtarget.com/>>.
- On trouvera des informations utiles et des questionnaires sur des sujets allant des cookies aux adresses IP en passant par les vérifications de navigateur à l'adresse :
<<http://www.2privacy.com/>>.
- On trouvera des conseils du gouvernement britannique sur la sécurité en ligne à l'adresse <<https://www.getsafeonline.org>> et pour les États-Unis à l'adresse <<http://www.us-cert.gov/>>.
- Trouvez votre CERT national en tapant « CERT + nom de votre pays » sur un moteur de recherche.
- Bien que les lignes directrices en matière de sécurité de la Direct Marketing Association <<http://www.the-dma.org/guidelines/informationsecurity.shtml>> s'adressent plutôt aux organismes de marketing direct, les conseils qui y figurent peuvent être utiles à toute personne qui s'intéresse à la sécurité en ligne.
- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

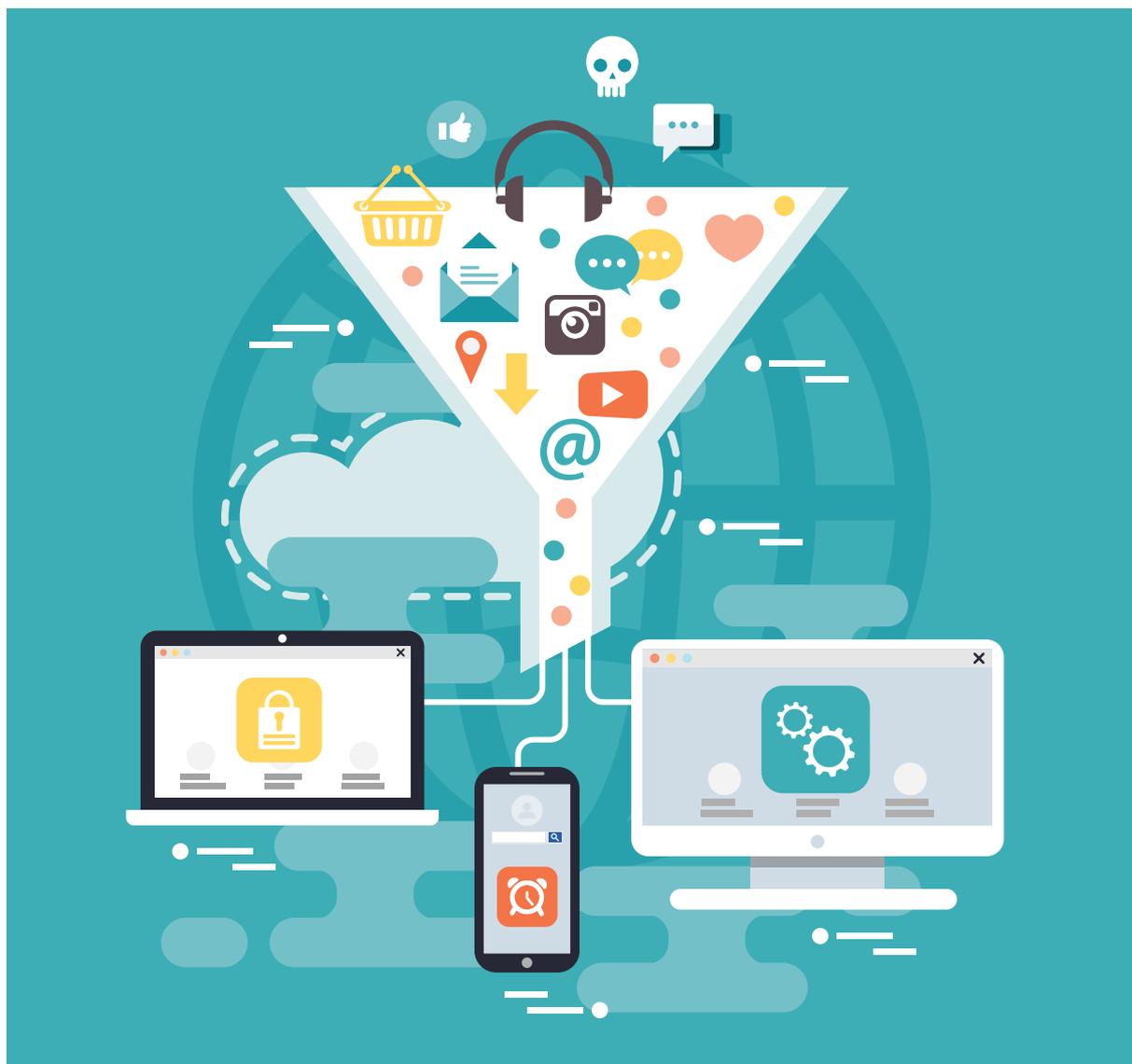
Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile

Article 17 – Les enfants ont un droit d'accès à des informations fiables provenant des médias. La télévision, la radio et les journaux devraient fournir l'information dans un langage que les enfants comprennent et les protéger contre les contenus qui nuisent à leur bien-être.

Article 34 – Les États parties protègent les enfants contre toutes les formes d'exploitation sexuelle et de violence sexuelle.

Article 36 – Les enfants sont protégés contre toute activité susceptible de nuire à leur développement.

Classification/étiquetage et filtrage



CLASSIFICATION

La classification et le filtrage sont deux méthodes qui permettent de restreindre l'accès à des contenus Internet comme les vidéos, images, pages web et jeux. Malgré les espoirs des organismes techniques et des agences de protection de l'enfance, il y a une dizaine d'années, de voir se créer un système de classification électronique qui pourrait être intégré aux sites web à des fins de filtrage, aujourd'hui, l'étiquetage se présente dans la plupart des cas sous la forme d'un pictogramme indiquant que des réglementations ou normes spécifiques sont respectées. Cela dit, l'élaboration de critères destinés aux systèmes d'étiquetage et de labels de confiance permettant aux enfants et à leurs familles d'identifier les contenus appropriés en ligne, ainsi que le partage de bonnes pratiques en la matière, continuent d'être une priorité du Conseil de l'Europe, notamment dans le cadre du Forum de la gouvernance d'Internet qui se tient chaque année sous l'égide de l'Organisation des Nations Unies¹. La classification des sites est un moyen de protéger les mineurs et d'accroître la confiance du public dans les transactions en ligne, tout en favorisant le respect de la loi par les fournisseurs de contenus.

1. www.intgovforum.org/multilingual/fr

■ PEGI est un système européen de classification en ligne bénéficiant du soutien de la Commission européenne, qui donne des indications sur les restrictions d'âge et le contenu des jeux, des applications et d'un certain nombre de sites (voir Fiche d'information 16 sur les jeux). Il met également en avant les fournisseurs de contenus qui respectent des normes de qualité incluant notamment l'obligation de proscrire de leurs sites les liens indésirables et tout contenu illicite ou offensant généré par les utilisateurs, de protéger la vie privée et de mettre en place un mécanisme indépendant de dépôt de plaintes.

■ Des labels de qualité et de confiance figurent également sur certains sites d'achats et de transactions en ligne pour indiquer qu'ils respectent la réglementation et les recommandations relatives à la sécurité des transactions (voir Fiche d'information 13 sur les achats en ligne). L'un des symboles les plus fréquents que vous pourrez voir est le cadenas qui indique que la page du site web sur lequel vous vous trouvez utilise le protocole SSL (Secure Sockets Layer) (norme de sécurité du transfert de données qui chiffre les données et authentifie le serveur et l'intégrité du message) ou TLS (Transport Layer Security). Vous pouvez alors partir du principe que vos données, notamment bancaires, sont sécurisées.



FILTRAGE

■ On entend généralement par filtrage le processus consistant à détecter et bloquer des plateformes et/ou du contenu inappropriés sur Internet. Il peut intervenir au niveau des navigateurs et proxys ou être effectué au moyen d'outils spécialisés comme les logiciels de contrôle parental. Le filtrage se fait en fonction des critères fixés par les parents, les établissements scolaires, les entreprises, les gouvernements et d'autres acteurs. Il fonctionne généralement au moyen de listes « noires » (indiquant les contenus à bloquer) ou « blanches » (qui interdisent l'accès à tous les contenus Internet sauf les éléments approuvés par le filtre). Les listes blanches sont quelquefois regroupées dans un système logiciel qui permet à l'opérateur ou au prestataire de services de contrôler les applications, les contenus et les médias et de restreindre l'accès aux applications ou contenus non approuvés. Lorsqu'un tel système est mis en place pour les enfants, il est appelé « jardin clos » ou « plateforme fermée »² par opposition aux plateformes ouvertes où les consommateurs disposent d'un accès sans restriction aux applications, contenus et autres éléments.

■ Une autre méthode de filtrage consiste à définir des mots-clés ou des termes interdits et à restreindre ou bloquer totalement l'accès à toute page qui les contiendrait. Au moyen d'un mot de passe, la personne qui a défini les règles de filtrage peut également autoriser un accès ponctuel aux sites³.

■ Il existe aujourd'hui des filtres multiappareils. Le logiciel ou l'application de filtrage sont alors installés sur plusieurs appareils (ordinateur portable, tablette, smartphone, télévision ou liseuse) et peuvent être contrôlés de manière centralisée, par exemple par le parent. Des règles différentes peuvent être fixées selon l'âge de l'enfant et être adaptées automatiquement à mesure qu'il grandit. Elles peuvent être utilisées pour limiter le temps passé en ligne et l'accès aux contacts, ainsi que pour le géorepérage et bien d'autres aspects.



ÉDUCATION

- Les listes blanches sont particulièrement intéressantes pour l'enfant qui fait ses premiers pas sur Internet, en lui permettant de retrouver rapidement ses sites préférés. Cela lui permet non seulement de développer sa discrimination visuelle, condition préalable à la lecture, mais aussi de faire en sorte que les activités sur Internet deviennent des activités familiales partagées, un élément essentiel pour garantir sa sécurité en ligne.

2. https://en.wikipedia.org/wiki/Closed_platform

3. <http://internet-filter-review.toptenreviews.com>

- Le filtrage peut être très utile pour protéger les mineurs contre les contenus indésirables en ligne ou contrôler l'usage d'Internet, mais il doit être complété par des recommandations appropriées de la part des parents, des enseignants et des personnes qui s'occupent des enfants.
- En classe, les filtres peuvent diminuer le risque que les élèves accèdent à des contenus inappropriés ou préjudiciables, mais n'évident aucunement la nécessité de vérifier les sites proposés aux élèves dans le cadre de leurs devoirs.
- L'étude de comparaison du programme Safer Internet (SIP-Bench) montre que les outils de filtrage actuels sont capables de filtrer les contenus potentiellement dangereux sans restreindre outre mesure les possibilités qu'Internet offre aux jeunes. On trouvera plus de détails à ce sujet sur le site du programme Safer Internet⁴.
- Les questions posées par les pratiques d'étiquetage et de filtrage offrent suffisamment de substance pour pouvoir être étudiées dans le cadre de cours d'éducation à la citoyenneté ou de sciences sociales. Engagez un débat sur le filtrage en ligne : est-ce une forme de censure acceptable et nécessaire ?



DIFFICULTÉS

- Les filtres peuvent bloquer l'accès à des informations et ressources intéressantes sur certains sites, par exemple ceux traitant de l'histoire des guerres mondiales ou des questions d'éducation sexuelle, en raison des mots-clés qu'ils contiennent.
- La classification et l'évaluation des sites web restent des pratiques largement fondées sur le volontariat, hormis dans les pays qui ont mis en place des lois pour faire respecter certaines normes. Dans notre monde globalisé, leur efficacité est quelque peu compromise du fait de leur mise en œuvre limitée par les plateformes et les fournisseurs de contenus et de l'absence de système commun de classification et d'évaluation.
- La législation ne parvient pas à suivre l'évolution rapide de la technologie ; aujourd'hui encore, les services de logiciels de filtrage ont tendance à appliquer une classification aux pages selon leur propre agenda social et leur propre système de valeurs.
- Il est difficile de déterminer quels contenus sont effectivement préjudiciables pour un public d'un âge donné et qui devrait décider des règles générales à respecter par les fournisseurs de contenus ou de l'application de ces règles. Les outils de filtrage doivent donc être très souples pour permettre aux personnes qui s'occupent des enfants de fixer les critères de filtrage en fonction de leurs valeurs familiales. Il appartient ensuite aux fournisseurs de filtres d'inventer des techniques pour faire en sorte que les contenus soient filtrés conformément à ces critères.
- Les filtres peuvent également devenir un outil de censure pour orienter l'opinion publique et museler les opposants politiques. Certains pays bloquent les sites des partis politiques ou mouvements idéologiques dissidents. Cela peut constituer un point de départ intéressant pour mener une discussion en classe sur les droits de l'homme et la démocratie.
- Certains considèrent que le filtrage est une forme de censure et qu'il est donc contraire à la philosophie d'Internet. D'autres affirment que si les logiciels de filtrage n'existaient pas, les gouvernements seraient contraints de réglementer les contenus en ligne.
- Les distributeurs de logiciels de filtrage s'efforcent par tous les moyens de répondre aux défis posés par les médias sociaux et les appareils mobiles et à l'usage d'Internet par des enfants de plus en plus jeunes.

4. <http://www.sipbench.eu/index.cfm/lang.8/secid.9/secid.2.0>

- Des discussions sont en cours au niveau international pour créer un nom de domaine finissant par *.kids* qui remplacerait *.org*, *.com* et autres pour les sites adaptés aux enfants, afin de les protéger contre les contenus en ligne potentiellement dangereux, malveillants ou inappropriés. Les sites qui utiliseraient ce nom de domaine seraient alors obligés de respecter des lignes directrices en matière d'enregistrement, ce qui nécessiterait entre autres de définir des normes acceptables au niveau international et de désigner une agence internationale de suivi.



MODE D'EMPLOI

- Que vous soyez un développeur de jeux ou d'applications souhaitant faire évaluer son produit conformément aux normes nationales ou internationales ou simplement une personne qui s'occupe d'enfants ou un parent désireux de comprendre le processus d'évaluation, visionnez la vidéo « How to » sur le site web de l'IARC (International Age Rating Coalition)⁵. La plupart des navigateurs et systèmes d'exploitation disposent de contrôles parentaux intégrés que l'on peut paramétrer pour filtrer le contenu indésirable. Le blog « How do I set up non-annoying parental controls on all my devices? »⁶ explique la manière de procéder sur différents appareils et logiciels. La plupart des programmes de filtrage permettent d'indiquer quels types de contenu on souhaite filtrer ou autoriser. Cela dit, les filtres préinstallés ne satisferont peut-être pas à toutes vos exigences, en particulier si vous souhaitez fixer des règles différentes pour chaque utilisateur. Il vous faudra alors faire l'acquisition d'un programme spécifique pour un paramétrage plus précis du filtrage de sites et du contrôle de l'usage. Les récents rapports du programme Safer Internet⁷ et les évaluations de logiciels sur Internet⁸ peuvent être utiles pour faire votre choix parmi la multitude de produits actuellement disponibles sur le marché.



BONNES PRATIQUES

- Avant d'installer un filtre, étudiez bien son fonctionnement. Le filtrage est-il fondé sur des choix idéologiques ou culturels contraires à vos convictions ?
- Utilisez les aides électroniques avec discernement et ne cédez pas aux sirènes de la publicité. Faites-vous votre propre opinion sur les performances des produits. Aucun filtre ne pourra jamais remplacer celui de la « pensée critique » que tous les Internautes doivent développer, indépendamment de leur âge.
- Parlez régulièrement avec les élèves, les parents et le personnel de leurs usages et de leurs besoins. La création d'un environnement où ils pourront discuter librement enrichira bien plus l'expérience de vos apprentis Internautes que la censure ou la chasse aux sorcières. Selon les recommandations des experts, le meilleur moyen de responsabiliser les enfants est de faire en sorte que les parents s'intéressent à leurs activités sur Internet et passent du temps avec eux en ligne.
- Envisagez les solutions de type « liste blanche » (qui n'autorisent l'accès qu'à certains sites approuvés) pour les Internautes les plus jeunes. Ajoutez à vos favoris les sites web adaptés aux enfants pour établir une liste personnalisée que ces derniers pourront utiliser pour accéder facilement par la suite aux sites sécurisés qu'ils ont déjà utilisés.
- Il convient d'encourager les enfants et les jeunes à parler des contenus inappropriés qu'ils trouvent sur Internet. Les adolescents affirment souvent que l'une des principales difficultés qu'ils rencontrent tient au fait qu'ils ne peuvent pas parler à leurs parents des questions morales auxquelles ils sont confrontés en ligne. Signalez tout contenu potentiellement illicite à un numéro d'urgence⁹.

5. <https://www.globalratings.com>

6. <http://web.archive.org/web/20160528132556/http://lifehacker.com/5868750/how-do-i-set-up-non-annoying-parental-controls-on-all-my-devices>

7. <http://www.sipbench.eu/index.cfm/lang.8/secid.9/secid2.0>

8. <http://internet-filter-review.toptenreviews.com>

9. <http://www.inhope.org>

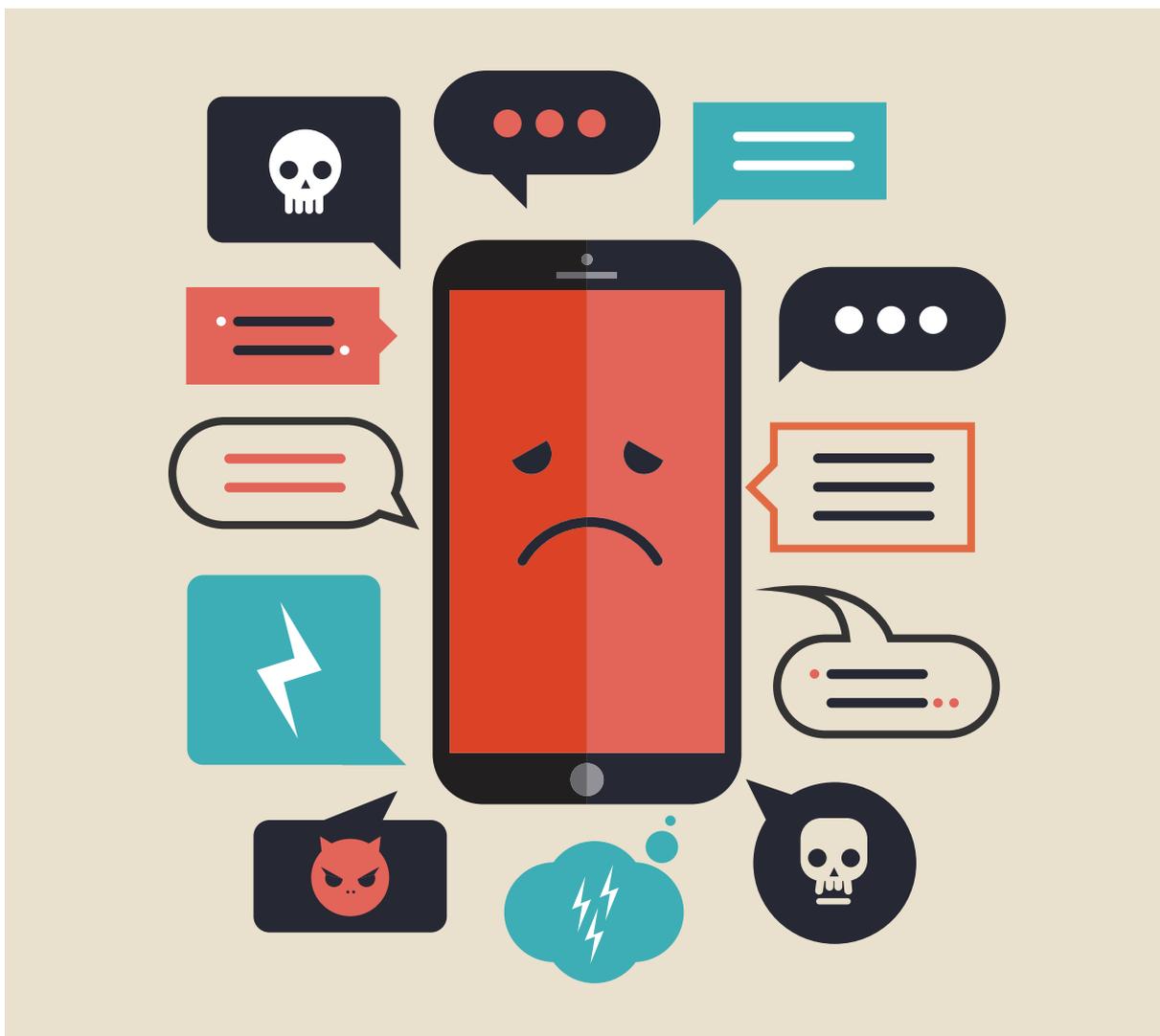
- Surveillez les activités de vos enfants sur les sites web de jeux et vérifiez la présence du label PEGI Online décerné aux sites sûrs.
- De plus en plus de communautés en ligne s'appuient sur les utilisateurs eux-mêmes pour contribuer à l'étiquetage des contenus, notamment ceux générés par l'utilisateur. Veillez à apposer un label sur tout contenu que vous mettez en ligne et aidez à signaler les contenus qui n'ont pas les labels appropriés.



BONNES PRATIQUES

- Article Wikipédia sur la censure dans le cyberspace : https://fr.wikipedia.org/wiki/Censure_de_l'Internet.
- Le site web de la division médias du Conseil de l'Europe donne des informations sur le travail de l'Organisation en matière de promotion de l'autorégulation et de l'autonomisation des utilisateurs : <http://www.coe.int/media>.
- NetNanny à l'adresse <http://www.netnanny.com> et Cyberpatrol <http://www.cyberpatrol.com> sont deux produits bien connus sur le marché.
- L'Electronic Frontier Foundation (EFF) défend les libertés civiles sur Internet : <http://www.eff.org/>.
- Le projet SIP-Bench financé par l'UE publie chaque année les résultats d'études comparatives dans neuf langues sur les systèmes de filtrage : <http://www.sipbench.eu/>.
- L'étude du Conseil de l'Europe « Young people, well-being and risk online » (2006) examine ce que l'on entend par « contenu préjudiciable » dans le cadre de la protection des enfants et des jeunes dans la société de l'information : <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680483b30>.
- Le site web du système PEGI Online donne des informations sur les jeux en ligne, la classification en catégories, les risques, ainsi que des conseils de sécurité et une liste des sites web bénéficiant d'un label : <http://www.pegionline.eu>.
- Recommandation CM/Rec(2008)6 du Comité des Ministres aux États membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet : https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc0.
- Documents pertinents du Conseil de l'Europe pour plus d'informations sur la classification/l'étiquetage et le filtrage : <http://www.coe.int/fr/web/freedom-expression/internet-standard-setting>

Harcèlement en ligne : intimidation, traque et trolling



Internet et les technologies atteignant un public toujours plus large, les tentatives de harcèlement se multiplient elles aussi.

D'après une étude menée en 2014 auprès d'adultes américains par le PEW Research Center, il existe au moins six formes différentes de harcèlement en ligne : les injures, les tentatives délibérées de mettre une personne dans l'embarras, les menaces physiques, le harcèlement continu, le harcèlement sexuel ou la traque. Dans la même étude, les chercheurs ont souligné cinq faits majeurs à propos du harcèlement en ligne :

1. Parmi les personnes interrogées, 40 % des Internautes avaient personnellement été victimes de harcèlement en ligne.
2. Les jeunes adultes sont le groupe démographique le plus exposé au harcèlement en ligne.
3. Les femmes et les hommes n'ont pas le même vécu quant au harcèlement en ligne.
4. La moitié des personnes victimes de harcèlement en ligne ne connaissent pas l'auteur des faits.
5. Les médias sociaux étaient les lieux de harcèlement les plus fréquemment cités.

■ Le harcèlement en ligne consiste à tenir de manière répétée et ciblée des propos injurieux ou médisants à l'encontre de certaines personnes. Il peut prendre différentes formes parmi lesquelles la cyberintimidation et la traque en ligne, le trolling ou la diffusion de propos haineux.



CYBERINTIMIDATION

- L'Organisation mondiale de la santé reconnaît l'intimidation comme une forme de violence, celle-ci étant définie comme « l'usage délibéré ou la menace d'usage délibéré de la force physique ou psychologique ou de la puissance contre soi-même, contre une autre personne ou contre un groupe ou une communauté qui entraîne ou risque fort d'entraîner un traumatisme, un décès, un dommage moral, un maldéveloppement ou une carence » (Organisation mondiale de la santé - 2002) *Rapport mondial sur la violence et la santé : résumé*¹.
- L'intimidation est un acte commis à l'encontre d'une personne en vue de lui nuire, qui se répète sous différentes formes au fil du temps. Parents et enfants n'ont généralement pas la même perception de l'étendue de ce problème.
- L'intimidation peut être physique ou verbale, sexuelle, basée sur des préjugés, ou prendre d'autres formes comme l'agression relationnelle, l'extorsion et la cyberintimidation.
- La cyberintimidation désigne les manœuvres d'intimidation par Internet ou par téléphone mobile, ce qui inclut l'envoi de messages et courriers électroniques ou la publication, sur des forums et salons de discussion, de commentaires insultants ou malveillants, voire la conception de sites complets dans l'intention de nuire à une personne ou à un groupe en particulier.
- Les auteurs de tels actes utilisent également les téléphones portables pour prendre des photos compromettantes d'autres personnes et envoyer des SMS ou MMS blessants. Par rapport aux formes « classiques » d'intimidation, celles qui se déroulent en ligne ont un impact beaucoup plus important car leurs auteurs sont confortés par un sentiment d'anonymat et leurs victimes n'ont aucune possibilité de se soustraire à leur persécuteur : elles peuvent être attaquées jour et nuit, où qu'elles se trouvent.
- La traque en ligne est l'utilisation d'Internet ou d'autres moyens électroniques pour suivre ou harceler une personne, un groupe ou une organisation².
- Le trolling est l'acte de créer des problèmes sur Internet en entamant des querelles, en fâchant ses interlocuteurs ou en publiant des messages incendiaires, inutiles ou hors sujet dans une communauté en ligne comme un groupe d'information³ ou un blog.
- Le trolling est pratiqué dans l'intention délibérée de provoquer une réaction émotive chez les lecteurs ou d'interrompre par d'autres moyens une discussion normale sur un sujet⁴.
- La traque en ligne, le trolling et la cyberintimidation étant généralement inclus dans le harcèlement en ligne, les recommandations et informations ci-après sont à appliquer au cas par cas.



IMPORTANCE DE LA RÉSILIENCE ET DE L'APPRENTISSAGE SOCIAL ET ÉMOTIONNEL

- Travailler sur la résilience et le bien-être social et émotionnel est essentiel pour aider les jeunes à se protéger contre les manœuvres d'intimidation et autres comportements agressifs en ligne.
- Un climat positif au sein de l'établissement ou de la communauté peut atténuer le phénomène d'intimidation en ligne et en classe et plus généralement, le harcèlement en ligne.
- Les parents peuvent aider leurs enfants à développer leur résilience en renforçant leur conscience et leur estime de soi, en leur montrant qu'ils sont acceptés et aimés tels qu'ils sont, en leur expliquant comment s'adapter et faire face aux situations difficiles, en suscitant des émotions positives,

1. http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_fr.pdf?ua=1

2. <https://en.wikipedia.org/wiki/Cyberstalking>

3. https://en.wikipedia.org/wiki/Usenet_newsgroup ; https://fr.wikipedia.org/wiki/Salon_de_discussion

4. [https://fr.wikipedia.org/wiki/Troll_\(Internet\)](https://fr.wikipedia.org/wiki/Troll_(Internet))

en mettant du rire et du plaisir dans leur vie, en insistant sur les compétences de résolution de problèmes, en leur apprenant à être réactifs et en leur montrant l'importance de l'empathie.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- L'intimidation et le harcèlement peuvent saper le moral de toute une classe et créer un climat de crainte et de méfiance rendant l'apprentissage quasi impossible.
- Les problèmes les plus fréquemment rencontrés chez les victimes d'intimidation ou de harcèlement sont la dépression, l'anxiété, la faible estime de soi, les difficultés d'adaptation sociale et l'isolement.
- Chez les auteurs de tels actes, on observe souvent un renforcement de l'anxiété, un risque d'échec scolaire, d'autres comportements délinquants et une probabilité accrue de criminalité à l'âge adulte.
- L'une des mesures préventives permettant d'éviter que l'intimidation ou le harcèlement ne deviennent un problème dans votre établissement consiste à intégrer dans le programme d'études des questions comme la gestion des relations sociales, l'apprentissage de la maîtrise de soi et les techniques de résolution des conflits. Bien choisis, ces modules permettront aux enfants et aux adolescents de se découvrir des talents de médiateur et de réduire le risque que des conflits mineurs ne dégèrent en comportements menaçants, que ce soit en ligne ou dans le monde « réel ».
- Votre établissement devrait se doter d'une politique claire (communément appelée « charte de bon usage »)⁵ – pour définir quand et comment les élèves et le personnel pourront utiliser Internet et leurs téléphones portables à l'école. Ce document devrait interdire expressément tous propos et comportements vulgaires, d'intimidation ou de harcèlement et énoncer clairement les sanctions auxquelles s'exposent directement ceux qui n'utiliseraient pas Internet ou leur téléphone portable conformément aux règles.
- Il devrait y avoir une procédure permettant de consigner les usages d'Internet et notamment de savoir qui est en ligne, quand et où, bien que cela puisse poser quelques problèmes en matière de protection des données.
- Les élèves doivent avoir pour instruction de rompre tout contact avec celui qui les harcèle ou les met mal à l'aise lorsqu'ils sont en ligne.
- Les élèves doivent signaler immédiatement tout incident à un adulte de confiance et si possible, lui montrer le matériel incriminé. L'adulte suivra alors la procédure fixée par l'établissement.
- Cette procédure doit être la même que lorsqu'un enfant est victime de harcèlement dans la vie réelle. Il doit interrompre toute relation avec son bourreau et parler de l'incident à un adulte de confiance. Il ne doit jamais se sentir seul face à son problème ou avoir le sentiment de devoir le régler lui-même.

■ En résumé, la politique de l'établissement scolaire en matière d'utilisation d'Internet et du téléphone portable devrait inclure des méthodes d'intervention telles que la résolution des conflits, la formation des élèves et du personnel sur la conduite à tenir en cas de harcèlement en ligne, la mise à disposition d'un soutien positif aux victimes et, si possible, un accompagnement des auteurs de ces actes afin de les aider à modifier leur comportement. Si de telles dispositions sont prises, l'établissement ne devrait pas avoir trop de difficultés à gérer les problèmes d'intimidation ou de harcèlement et à lutter contre ces phénomènes.

5. https://en.wikipedia.org/wiki/Acceptable_use_policy



MODE D'EMPLOI

De tout temps, les éducateurs ont dû faire face aux cas d'intimidation et de harcèlement à l'intérieur ou à l'extérieur de la classe. Il est impératif de comprendre aujourd'hui le rôle que peut jouer Internet dans ce type d'actes.

- On demande aux élèves d'être capables d'assumer les conséquences de leurs actes, mais le fait est que l'intimidation et le harcèlement ont tendance à réduire l'estime de soi. Lorsqu'une personne est victime d'intimidation ou de harcèlement, elle apprend moins bien car elle ne parvient plus à se concentrer, se sent menacée et perd confiance en elle-même.
- Les élèves qui se sentent menacés (que ce soit en ligne ou dans le monde réel) ont besoin de l'aide d'un adulte de confiance. Cela ne doit pas faire perdre de vue la nécessité d'assurer également un accompagnement de l'agresseur pour qu'il ne reproduise plus ce comportement.
- La gestion des cas d'intimidation et de harcèlement doit faire l'objet d'une approche globale qui implique de discuter ouvertement, au sein de la famille ou en classe, de la nature et des causes potentielles de ces agissements intolérables, ainsi que sur les mesures qui peuvent être prises collectivement pour y remédier.
- L'intimidation et le harcèlement sont des problèmes sociaux. Il est de la responsabilité des enseignants et des parents d'enquêter sur les allégations de tels comportements et de tout mettre en œuvre au sein de la famille ou en classe pour assurer les meilleures conditions d'apprentissage possible, en cours, en récréation ou en ligne.
- Les enseignants doivent être formés à la dynamique de l'intimidation et du harcèlement et à la manière dont Internet et les téléphones portables sont utilisés pour persécuter les autres. Ils doivent apprendre à en détecter les signes à la fois chez les victimes et les harceleurs et à adopter la bonne attitude dans chaque situation.
- Les établissements scolaires devraient prévoir des lignes directrices spécifiques. Il serait judicieux d'intégrer des mesures de prévention dans leurs politiques relatives à Internet pour traiter les cas d'intimidation et de harcèlement.
- Les quatre règles d'or suivantes sont à adopter par les élèves face à la cyberintimidation et au cyberharcèlement :
 1. Faire une copie des contenus incriminés si possible.
 2. Ne pas transférer ces contenus à des tiers.
 3. Éteindre l'appareil récepteur (ordinateur ou téléphone portable).
 4. Signaler l'incident à un adulte de confiance.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- **Jeu de rôles** : les élèves se voient proposer un exercice de simulation d'une résolution de conflit. L'enseignant répartit les rôles et crée des groupes au sein desquels les élèves ont pour mission de régler un différend. Les rôles sont ensuite inversés pour leur permettre d'adopter plusieurs points de vue sur la même situation.
- **Groupes de discussion** : les élèves participent à des groupes de discussion pour évaluer leur participation au travail de groupe, échanger leurs impressions sur des points comme l'intimidation en général, les règles de conduite sur Internet et la question des responsabilités.



BONNES PRATIQUES

Voici quelques idées pour faire face aux cas d'intimidation en ligne et de harcèlement par courrier électronique ou autres messages :

- Apprenez aux élèves à ne pas ouvrir les messages provenant de sources inconnues.
- S'ils constatent en ouvrant un courrier électronique ou un SMS que son contenu est injurieux ou choquant, ils sont invités à en effectuer une copie et à la montrer à un adulte de confiance. Il convient de ne jamais répondre à ce type de messages car cela ne ferait qu'encourager l'auteur des faits à persévérer dans cette voie.
- Si une personne continue d'envoyer ce type de messages et qu'il est possible (grâce à l'adresse de courrier électronique) de déterminer d'où ils ont été envoyés, le harcèlement devra être signalé immédiatement en contactant le fournisseur d'accès⁶ ou l'opérateur de téléphonie mobile concernés.
- Les politiques de l'établissement scolaire sur l'intimidation et/ou les chartes de bon usage devraient contenir des dispositions sur la manière de gérer les situations dans lesquelles des élèves sont impliqués dans le harcèlement en ligne.
- Les élèves doivent savoir qu'ils peuvent à tout moment s'adresser à un parent, un enseignant ou un autre adulte de confiance s'ils sont victimes de harcèlement en ligne ou par téléphone. Cette personne doit prendre au sérieux le récit de la victime et la rassurer.
- Expliquez aux auteurs des tentatives d'intimidation ou de harcèlement que leur comportement est intolérable et qu'il doit cesser immédiatement, mais renseignez-vous également sur leurs motivations. Oseraient-ils dire ou faire les mêmes choses dans la vie réelle ?
- Les parents doivent systématiquement être informés du fait que leur enfant est victime ou auteur d'intimidations. Si un tyran persécute ses victimes sur Internet ou à partir de son téléphone portable, il est probable que ses agissements ne s'arrêtent pas à la grille de l'école et se poursuivent de chez lui.
- ENABLE⁷ (European Network Against Bullying in Learning and Leisure Environments) est un projet financé par l'Union européenne qui fournit des informations détaillées sur les meilleures méthodes de lutte contre les actes d'intimidation et promeut l'apprentissage social et émotionnel tout en proposant des supports d'information pour les parents et des outils de formation par les pairs pour les écoles.



INFORMATIONS COMPLÉMENTAIRES

- La page web du Conseil de l'Europe « Halte au harcèlement » met à disposition des outils pour lutter contre les actes d'intimidation : www.coe.int/en/web/edc/beat-bullying.
- NoBullying.com propose des ressources sur l'intimidation, en ligne et hors ligne : <http://nobullying.com/>.
- Le site web Smile of the Child, basé en Grèce, propose de l'aide pour tous les problèmes que les enfants peuvent rencontrer au quotidien : <http://www.hamogelo.gr/1.2/home>.
- « Stomp Out Bullying » : <http://www.stompoutbullying.org> « Stop bullying now! » est un site web américain qui vise à combattre le phénomène d'intimidation : <http://www.stopbullying-now.com/>.
- #DeleteCyberbullying est une application interactive sous Android donnant des conseils sur la cyberintimidation : <https://deletecyberbullying.wordpress.com/app/>.

6. https://fr.wikipedia.org/wiki/Fournisseur_d'accès_à_Internet

7. <http://enable.eun.org/about-enable-french>

- Childnet International donne des conseils et informations : <<http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/>>.
- « Know the risks: challenging cyber bullying » est destiné aux parents et aux enseignants : <http://web.archive.org/web/20100923133231/http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_bullying.cfm>.
- « What is cyber bullying? » est un site web du gouvernement australien sur lequel on trouve des conseils aux familles : <http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyberbullying/What_is_cyber_bullying.html>.
- Signalez les actes d'intimidation et contenus préjudiciables au réseau Insafe : <<http://www.betterinternetforkids.eu>>.
- Le PEW Research Center a publié le résumé de ses conclusions sur le harcèlement en ligne pour l'année 2014 : <<http://web.archive.org/web/20160703044152/http://www.pewinternet.org/2014/10/22/online-harassment/>>.
- Le mouvement No Hate Speech est une campagne de jeunesse du Conseil de l'Europe : <<http://www.nohatespeechmovement.org/>>.
- Pour plus d'informations sur l'intimidation et des plans de cours, outils pour les parents et kits de formation des pairs, voir le site : <<http://enable.eun.org>>.

Obtenir de l'aide



Internet est un système mondial de réseaux informatiques qui relie entre eux des milliards d'appareils dans le monde grâce à la suite de protocoles TCP/IP¹. Ce réseau est donc très différent des autres médias car c'est le moyen de communication le plus décentralisé qui soit. Il n'a pas de point de contrôle unique car cette nébuleuse d'ordinateurs propose des canaux très divers de communication et de transfert d'informations. Par ailleurs, depuis l'apparition du Web 2.0, les utilisateurs des réseaux en ligne ne sont plus seulement des consommateurs, mais aussi des producteurs d'information (voir Fiche d'information 1 « Se connecter »).

Internet offrant aujourd'hui la possibilité à n'importe qui de publier quasiment n'importe quoi en ligne, et bon nombre de nos données étant stockées dans des lieux hors de notre portée que l'on désigne habituellement sous le terme générique de « nuage », il se pose une multitude de questions sur l'avenir d'Internet et la manière de contrôler ne serait-ce qu'une infime partie de ce flux d'informations. Il nous arrive régulièrement de nous demander qui peut décider que tels ou tels propos ou informations sont choquants ou dangereux pour nos enfants, nos familles et nous-mêmes, mais aussi et surtout comment nous protéger, ainsi que nos proches, contre ces risques?

1. https://fr.wikipedia.org/wiki/Fournisseur_d%27acc%C3%A8s_%C3%A0_Internet



CONTENU ILLICITE

— Chaque pays définit dans sa législation nationale ce qui est légal et illégal. Par conséquent, Internet, en tant que moyen de communication, fonctionne dans un cadre réglementé. Toute action jugée illégale en dehors d'Internet doit être considérée comme illégale sur Internet également. Cela dit, l'immense portée d'Internet peut amplifier les atteintes aux droits d'autrui et en décupler l'impact. Par exemple, de simples « taquineries » en ligne peuvent déboucher sur de la diffamation, voire pire.

— Le terme « contenu illicite » désigne de manière générale tout matériel, activité ou information contrevenant à la loi et susceptible de porter préjudice à un individu ou une entité.

— Cela englobe les images et sites web pédopornographiques, les activités illégales dans les salons de discussion (par exemple les sollicitations d'enfants à des fins sexuelles ou *grooming*), le discours de haine en ligne, ainsi que les messages et sites web à caractère xénophobe. Ces comportements illégaux et d'autres sont couverts par la Convention du Conseil de l'Europe sur la cybercriminalité², premier traité international sur les infractions commises par le biais d'Internet et des autres réseaux informatiques, ainsi que par le Protocole additionnel à cette Convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques³. La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote)⁴ couvre également la collecte et le stockage non autorisés de données, ainsi que l'exploration de données. Cette convention est le premier traité international qui impose des sanctions pénales pour toutes les formes de violence sexuelle à l'égard des enfants, y compris les tentatives d'approche.



OBTENIR DE L'AIDE, UN DROIT FONDAMENTAL

— Internet est un outil facilement accessible à tous et de partout : par conséquent, un contenu considéré comme dangereux ou inapproprié peut facilement être vu par des enfants, des adolescents et d'autres catégories vulnérables de la population. La Déclaration universelle des droits de l'homme érige en droit fondamental le droit de toute personne d'être protégée contre tout préjudice et le droit à un recours contre toute discrimination ou violation quelconque des droits fondamentaux qui lui sont reconnus⁵. La Convention des Nations Unies relative aux droits de l'enfant souligne quant à elle la responsabilité des adultes d'agir dans l'intérêt supérieur de l'enfant et donc de le protéger contre les contenus et actes préjudiciables, et charge les gouvernements et les familles de prendre toutes les mesures nécessaires pour assurer le respect, la protection et la réalisation des droits de l'enfant. Cela implique d'assurer des services sociaux et de mettre en place des systèmes juridiques et des systèmes de santé et d'éducation qui accompagnent les enfants et leur assurent un environnement dans lequel ils pourront grandir et s'épanouir pleinement. Les numéros d'urgence et autres dispositifs de signalement sont des composantes essentielles de ces systèmes.

— Aux côtés d'autres organisations internationales, notamment dans le cadre des activités du Forum de la gouvernance d'Internet, le Conseil de l'Europe a pour objectif de sensibiliser les familles et la société dans son ensemble aux questions de protection des enfants et des jeunes sur Internet. Ce travail passe par la mise à disposition d'informations facilement accessibles sur les outils et procédures permettant d'obtenir une aide adéquate.



MODE D'EMPLOI

- Toute personne découvrant sur Internet un contenu supposé illicite peut le signaler à un numéro d'urgence⁶. INHOPE est une association qui coordonne les numéros d'urgence de bon nombre

2. <http://conventions.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185>

3. <http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/189>

4. <http://www.conventions.coe.int/fr/web/conventions/full-list/-/conventions/treaty/201>

5. <http://www.un.org/fr/universal-declaration-human-rights/index.html>

6. <http://en.wikipedia.org/wiki/Hotline>

de pays⁷. On trouvera sur son site web de plus amples informations sur le type de contenus illicites dont elle s'occupe⁸.

- Pour signaler un contenu illicite, allez sur la page <<http://www.inhope.org/tns/contact-us/details.aspx>> et suivez les instructions. Les services de la plateforme enquêteront⁹ pour déterminer si le contenu signalé est effectivement illicite et, le cas échéant, essaieront d'en retrouver l'origine. Ils contacteront également les autorités de police du pays dans lequel est hébergé le contenu incriminé, ainsi que le fournisseur d'accès à Internet concerné, pour en demander le retrait.

Demande d'assistance à une ligne téléphonique

- Les enfants et les jeunes peuvent obtenir de l'aide en contactant un centre d'assistance¹⁰, entité qui propose un soutien par téléphone et/ou des conseils par courrier électronique, messagerie ou SMS.
- Dans de nombreux pays, les centres d'information Insafe¹¹ travaillent en coopération avec les centres d'assistance nationaux pour répondre aux questions et préoccupations des jeunes quant à leurs expériences en ligne ou au contenu préjudiciable ou illicite auquel ils sont confrontés sur Internet. Nombre de centres d'assistance qui traitent des problèmes liés à Internet peuvent également apporter une aide aux jeunes sur toutes sortes d'autres questions de « la vraie vie ».
- Child Helpline International¹² est un point de contact important dans de nombreux pays européens et non européens. Ce réseau mondial de services d'assistance aux enfants intervient dans plus de 150 pays pour protéger les droits des enfants.
- En règle générale, les centres d'assistance fonctionnent 24 heures sur 24, 7 jours sur 7. Ils proposent des services gratuits et anonymes et ne retracent pas l'origine des appels, des courriers électroniques ou des SMS. Les enfants et les adolescents peuvent les contacter pour parler de différents sujets. Il existe des systèmes qui permettent aux jeunes de communiquer par chat, courrier électronique ou forums, ainsi que par des méthodes plus traditionnelles. Le personnel du centre d'assistance est là pour écouter les jeunes et les aider à trouver par eux-mêmes une solution à leurs problèmes.
- Pour trouver un service d'assistance dans votre pays, tapez le nom du pays et les termes « signalement » et « centre d'assistance » sur un moteur de recherche.

Utilisation des services de signalement spécialisés des plateformes de médias sociaux

- La plupart des plateformes de médias sociaux comme Facebook, Twitter, Instagram ou Google ont un centre de sécurité qui donne des conseils aux utilisateurs et un dispositif qui permet de signaler en ligne tout contenu ou activité inappropriés. Il se trouve généralement dans le menu « assistance » ou « aide ». Signaler des cas d'intimidation, par exemple aux sites de réseaux sociaux, peut aboutir au retrait du contenu incriminé, voire à la suppression des comptes des personnes qui n'ont pas respecté les conditions générales d'utilisation du service. La plupart des sites fonctionnent sur le même modèle : sur Facebook, par exemple, chaque contenu s'accompagne d'un menu déroulant qui permet aux utilisateurs de signaler un article ou une photo et de dire pourquoi ils ne souhaitent pas les voir. On trouvera dans la note de bas de page¹³ ci-dessous le lien vers des informations sur la marche à suivre pour effectuer un signalement.
- Tous les opérateurs de téléphonie mobile proposent des services d'assistance par téléphone, chat ou courrier électronique ainsi que des conseils adressés directement aux familles et aux enfants. Vodafone, par exemple, a créé un site web¹⁴ sur la parentalité numérique contenant des recommandations aux parents et aux enfants et des « modes d'emploi » pour configurer les contrôles

7. <http://inhope.org/gns/who-we-are/at-a-glance.aspx>

8. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx>

9. <http://www.inhope.org/en/about/faq.html>

10. https://fr.wikipedia.org/wiki/Centre_d'assistance

11. <http://www.betterinternetforkids.eu>

12. <http://www.childhelplineinternational.org>

13. <https://www.facebook.com/help/181495968648557/>

14. <http://www.vodafone.com/content/digital-parenting.html>

parentaux. Il propose également des services de contrôle parental et d'autres fonctionnalités de sécurité par le biais de SecureNet¹⁵. L'application Vodafone Guardian sur Android permet également de bloquer les contacts indésirables.



INFORMATIONS COMPLÉMENTAIRES

- Consultez la Convention des Nations Unies relative aux droits de l'enfant <<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>> et/ou le document de présentation établi par l'Unicef <http://www.unicef.org/crc/files/Rights_overview.pdf> pour en savoir plus sur le droit des enfants à une protection et une assistance.
- Pour de plus amples informations sur la protection contre la violence et le signalement de la violence, la stratégie intégrée du Conseil de l'Europe sur la violence est consultable à l'adresse : <<http://www.coe.int/en/web/children/integrated-strategies>>.
- Pour signaler du contenu illicite, vous pouvez contacter INHOPE : <<https://www.inhope.org/>>.
- Le portail d'Insafe, réseau européen de centres de sécurité Internet <<http://www.betterinternetforkids.eu/>> donne des informations sur les points de contact et services d'assistance téléphonique nationaux en Europe.
- Pour signaler un cas de cyberintimidation ou obtenir une aide, vous pouvez contacter Childline <<http://www.childline.org.uk/>>, service d'assistance téléphonique 24 heures sur 24 pour les enfants et les adolescents (numéro de téléphone : 0800 1111).
- Befrienders.org <<http://www.befrienders.org>> est un site web qui vous permet de trouver le service d'assistance le plus proche lorsque vous avez besoin d'aide, par exemple pour tout ce qui touche au suicide.
- Europe Direct <https://europa.eu/european-union/contact_fr> est un service gratuit qui permet d'obtenir des réponses immédiates à des questions générales sur l'UE ainsi que les coordonnées des organismes compétents tels que les centres nationaux d'assistance.

15. <https://securenet.vodafone.com/>

6. Internet – Et demain ?

” « La liberté d’expression est la base des droits de l’homme, la racine de la nature humaine et la mère de la vérité. Tuer la liberté d’expression revient à insulter les droits de l’homme, étouffer la nature humaine et supprimer la vérité »

Liu Xiaobo, lauréat du Prix Nobel de la paix en 2010 et militant pour les droits de l’homme

LISTE DE POINTS À VÉRIFIER :

23. INTERNET DES OBJETS

De la même manière que vous protégez déjà votre ordinateur et d’autres appareils contre les intrusions, sécurisez également vos appareils de l’Internet des objets.

Il est difficile de protéger chaque appareil individuellement, mais vous pouvez protéger votre réseau et réduire ainsi les zones de vulnérabilité.

Réfléchissez bien avant de faire l’acquisition d’un objet de « l’Internet des jouets » que vous ferez entrer dans votre maison et auquel votre enfant aura accès. Cet achat est-il vraiment nécessaire ? Vérifiez les paramètres de sécurité et de confidentialité du jouet en question.

24. INTELLIGENCE ARTIFICIELLE, AUTOMATISATION ET BOULEVERSEMENTS TECHNOLOGIQUES

Vous êtes-vous informé des évolutions récentes de l’intelligence artificielle et de l’automatisation ?

Investissez-vous dans vos compétences interpersonnelles, sociales et émotionnelles ?

Avez-vous paramétré vos appareils connectés pour assurer un niveau approprié de sécurité et de protection de l’utilisateur ?

25. RÉALITÉ VIRTUELLE ET RÉALITÉ AUGMENTÉE

Avez-vous parlé à votre enfant/vos élèves de sujets essentiels comme le sexisme, la sexualité, le racisme, le harcèlement, les stéréotypes et les autres formes de discrimination ?

Vous êtes-vous assuré que les appareils utilisés par votre enfant/vos élèves sont paramétrés correctement, pour assurer une protection élevée de leur vie privée et de leur sécurité ?

Avez-vous vérifié que votre enfant/vos élèves maintiennent un équilibre de vie sain lorsqu’ils utilisent des technologies de réalité virtuelle ou augmentée ?

26. ÊTES-VOUS LE PRODUIT ? BIG DATA, EXPLORATION DE DONNÉES ET PROTECTION DE LA VIE PRIVÉE

Avez-vous pris le temps d’examiner la manière dont vos données à caractère privé sont traitées par les services en ligne que vous utilisez, et de bien configurer les paramètres de confidentialité ?

Avez-vous récemment fait le point sur tout le contenu que vous avez déjà mis en ligne pour vous assurer qu’il est encore valable et que vous souhaitez toujours qu’il reste public ?

Vous informez-vous des évolutions les plus récentes du « big data » pour comprendre comment elles peuvent vous concerner et ce que vous pouvez faire ?

Internet des objets



Les avancées technologiques récentes qui permettent aujourd'hui de se connecter à Internet sans fil depuis des appareils équipés de la fonction de transmission de données suscitent un réel engouement dans bien des domaines. Mais ce secteur émergent qui promet d'accroître la rentabilité des entreprises et d'améliorer le confort de vie grâce à des appareils connectés au web, connu sous le nom d'« Internet des objets », est également une source d'inquiétude potentielle non seulement pour les parents mais aussi pour chacun d'entre nous.

Les questions de sécurité, de protection de la vie privée et de collecte des données ne sont que quelques-uns des aspects dont les experts et les responsables politiques doivent tenir compte aujourd'hui face à l'augmentation générale du nombre d'appareils conçus et commercialisés. L'Internet des objets pose à cet égard des difficultés particulières car il leur faudra trouver des moyens novateurs pour, à la fois, optimiser les avantages de cette nouvelle technologie et en limiter, voire en réduire les risques.

■ Le fait que des objets commencent à « réfléchir » suscite des interrogations légitimes chez le consommateur, qui doit également s'inquiéter du risque que des personnes mal intentionnées aient accès à ces objets. Un article récent « Hackers remotely kill a jeep on a highway »¹ relate ainsi le cas de deux pirates qui ont joué avec la climatisation, la radio et les essuie-glace d'un véhicule avant de couper son moteur. Cette attaque a lancé le débat sur la sécurité numérique des voitures et des camions.

■ Certains voient dans l'Internet des objets la prochaine révolution industrielle. Selon les estimations, il y aurait aujourd'hui près de 10 milliards d'appareils connectés ; ce chiffre pourrait atteindre 26 à 30 milliards d'ici 2020, ce qui représente un marché de 6 000 à 9 000 milliards de dollars américains².

■ Cette explosion du nombre d'appareils connectés s'accompagnera d'une explosion des données. Celles-ci se retrouveront partout et créeront de nouvelles difficultés qu'il faudra résoudre dans le cadre du Règlement général sur la protection des données.



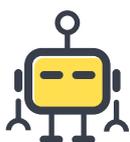
INTERNET DES OBJETS

- Le terme « Internet des objets » est apparu pour la première fois en 1999 mais il a fallu attendre encore plusieurs années pour voir véritablement apparaître sur le marché des objets connectés à Internet.
- L'Internet des objets³ est le réseau d'objets physiques et autres appareils équipés d'électronique, de logiciels, de capteurs et de fonctions de connectivité pour pouvoir recueillir et échanger des données.
- Ce terme s'applique à tous types d'appareils, des thermostats intelligents qui mettent en route le chauffage avant votre retour chez vous aux réfrigérateurs qui commandent du jus d'orange quand vous n'en avez plus, en passant par les dispositifs portables de suivi à usage médical et sportif pour l'homme (trackers d'activité) et les puces de géolocalisation pour les animaux⁴.
- Une autre caractéristique de l'Internet des objets est la connectivité à Internet qui permet aux appareils de communiquer entre eux et qui facilite le contrôle et l'automatisation des tâches, ainsi que la collecte de données.
- Le PEW Research Center estime que l'Internet des objets et les vêtements connectés seront couramment utilisés dans leurs applications bénéfiques⁵ d'ici 2025.



TECHNOLOGIES PORTABLES

- Les « technologies portables » sont les vêtements ou accessoires équipés de composants informatiques et électroniques de pointe.
- On parle de « vêtements et accessoires connectés » ou plus généralement, d'« informatique vestimentaire » ou d'« objets connectés personnels/portables »⁶.
- Les technologies portables fournissent des données instantanées à l'utilisateur qui peut soit s'en servir pour contrôler la technologie en temps réel, soit les télécharger en vue d'une utilisation ultérieure ou d'une impression.



INTERNET DES JOUETS

- L'Internet des objets peut également s'appliquer aux jouets pour enfants. La connectivité sans fil permettra à un jouet d'interagir avec d'autres appareils ayant accès à des données ou d'autres jouets.

1. <http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>

2. <https://securityintelligence.com/data-protection-in-the-internet-of-things/>

3. https://fr.wikipedia.org/wiki/Internet_des_objets

4. <http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security>

5. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf

6. https://fr.wikipedia.org/wiki/Technologie_portable

- L'Internet des jouets propose de nouveaux moyens de familiariser les jeunes avec la technologie et les encourage souvent à interagir avec le jouet.
- Hello Barbie, objet de l'Internet des jouets créé par Mattel en 2015, qui permettait à Barbie d'écouter les enfants, a provoqué l'inquiétude de parents et de spécialistes des questions de protection de la vie privée ainsi que d'éminents psychologues qui se sont demandé si ce type de jouets ne risquait pas de nuire au développement des enfants et à leur capacité à créer, à imaginer et à apprendre de manière autonome. ToyTalk, société créée en 2011, défend au contraire le point de vue selon lequel les jouets parlants et équipés de la technologie sans fil peuvent offrir aux enfants de multiples possibilités d'apprentissage⁷.
- Malgré la commodité de l'Internet des objets et des technologies portables et le côté amusant et divertissant de l'Internet des jouets, il est possible que les utilisateurs ne soient pas suffisamment conscients des dangers que ces objets connectés, à l'instar des téléphones portables et des ordinateurs, pourraient faire courir sur le plan de la sécurité et du respect de la vie privée. Dans le cas des jouets, il pourrait même y avoir des risques pour le développement des enfants.



COMPRENDRE LES ENJEUX : UN IMPÉRATIF

■ L'Internet des objets inclut des appareils portables que de nombreux utilisateurs ne considèrent peut-être pas comme des équipements informatiques, le risque étant alors qu'ils ne prêtent pas attention aux questions de protection de la vie privée.

■ Le côté futuriste de l'Internet des objets et des technologies portables plaît beaucoup. Leur accessibilité à tous appelle cependant à la réalisation d'études plus poussées. Comme l'ont déjà constaté les sociétés de cybersécurité par le passé, ceux qui nourrissent des intentions criminelles se montrent toujours plus prompts et assidus à trouver de nouveaux moyens de parvenir à leurs fins.

■ Les avancées réalisées par les fabricants de jouets dans le domaine de l'Internet des objets laissent certes entrevoir de fantastiques nouvelles possibilités de jeu pour les enfants, mais les parents doivent être conscients des risques encourus en laissant des appareils dotés de microphones ouverts entre les mains des jeunes et en faisant entrer à leur propre domicile des liaisons de données ouvertes.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

■ L'objectif premier de ces nouvelles technologies est d'améliorer les performances des objets, mais l'interconnectivité que cela implique n'est pas sans risques.

- Le simple fait de penser que des personnes puissent avoir accès à distance à vos appareils et à vos données fait frémir.
- La majorité des appareils et technologies portables ne sont pas conçus avec le souci d'assurer une sécurité ou une confidentialité optimales.
- De récentes intrusions ont montré que des pirates parvenaient à observer les gens à leur domicile par le biais de babyphones ou de webcams⁸.
- Les consommateurs peuvent courir un risque de cyberintrusion comparable au risque d'intrusion physique à leur domicile.
- Les consommateurs doivent savoir que le Règlement général sur la protection des données leur permet de contrôler l'utilisation qui est faite de leurs données et devraient se renseigner sur les modalités de mise en œuvre de ce texte.

7. http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0
 8. <http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159>



MODE D'EMPLOI

- Les appareils de l'Internet des objets ont des applications très diverses. Le mieux est de lire attentivement leur mode d'emploi pour en comprendre toutes les fonctionnalités.
- Il est important de parcourir les différentes options de réglage pour savoir comment activer/désactiver les paramètres de confidentialité selon vos besoins.
- Essayez d'effectuer quelques recherches sur l'appareil qui vous intéresse avant de l'acheter car il peut avoir fait l'objet d'un rappel ou ne pas fonctionner aussi bien qu'annoncé dans la publicité.
- N'oubliez pas que ce secteur est en plein développement et que si vous attendez quelques semaines, voire quelques mois, il y aura toujours quelque chose de plus récent et de plus perfectionné sur le marché, souvent à un prix inférieur.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Demandez aux élèves d'établir une liste de tous les appareils pouvant être connectés dans une maison, puis de recenser les risques potentiels pour la sécurité ou la confidentialité des données. Que peut faire l'utilisateur pour réduire ces risques ? Le fournisseur des appareils ? Le fournisseur d'accès à Internet ?
- Après une discussion sur l'Internet des objets, demandez aux élèves de rédiger un exemple de consignes aux utilisateurs pour les aider à comprendre les enjeux de sécurité.
- Lisez un résumé du Règlement général sur la protection des données et invitez les élèves à recenser toutes les dispositions applicables à l'Internet des objets⁹.
- Téléchargez le clip vidéo de la campagne de sensibilisation aux droits du consommateur¹⁰ et engagez une discussion avec les élèves sur les droits du consommateur et l'Internet des objets.
- Demandez aux jeunes de trouver des idées de nouveaux jouets à développer pour l'Internet des jouets. Qu'apporteront-ils ? Quels sont les risques encourus ? Comment protéger les jeunes utilisateurs ? Comment rassurer les parents sur la sécurité du jouet ?



BONNES PRATIQUES

Il est important de s'ouvrir à cette nouvelle technologie mais on ne peut le faire qu'à condition de prendre des mesures de sécurité appropriées pour protéger ses données et sa vie privée.

- Limitez les informations personnelles sur les appareils équipés de fonctions d'envoi et de réception de données.
- Renforcez votre sécurité sur le réseau sans fil de votre domicile.
- Choisissez des mots de passe sécurisés.
- Lorsque cela est possible, ne conservez pas les appareils ensemble.
- Limitez les interactions des jouets de l'Internet des objets avec vos autres appareils et déterminez les actions qu'ils sont autorisés à effectuer.

Points à prendre en considération lors du choix d'un appareil de l'Internet des objets :

- Compatibilité et interopérabilité : l'appareil est-il compatible avec ceux d'autres fabricants ou faut-il rester dans le même « écosystème » pour pouvoir l'utiliser ? Cet aspect est extrêmement important car vous risquez de vous retrouver dans un marché captif sans pouvoir changer de marque ou en intégrer d'autres.

9. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

10. http://ec.europa.eu/justice/newsroom/consumer-marketing/events/140317_en.htm

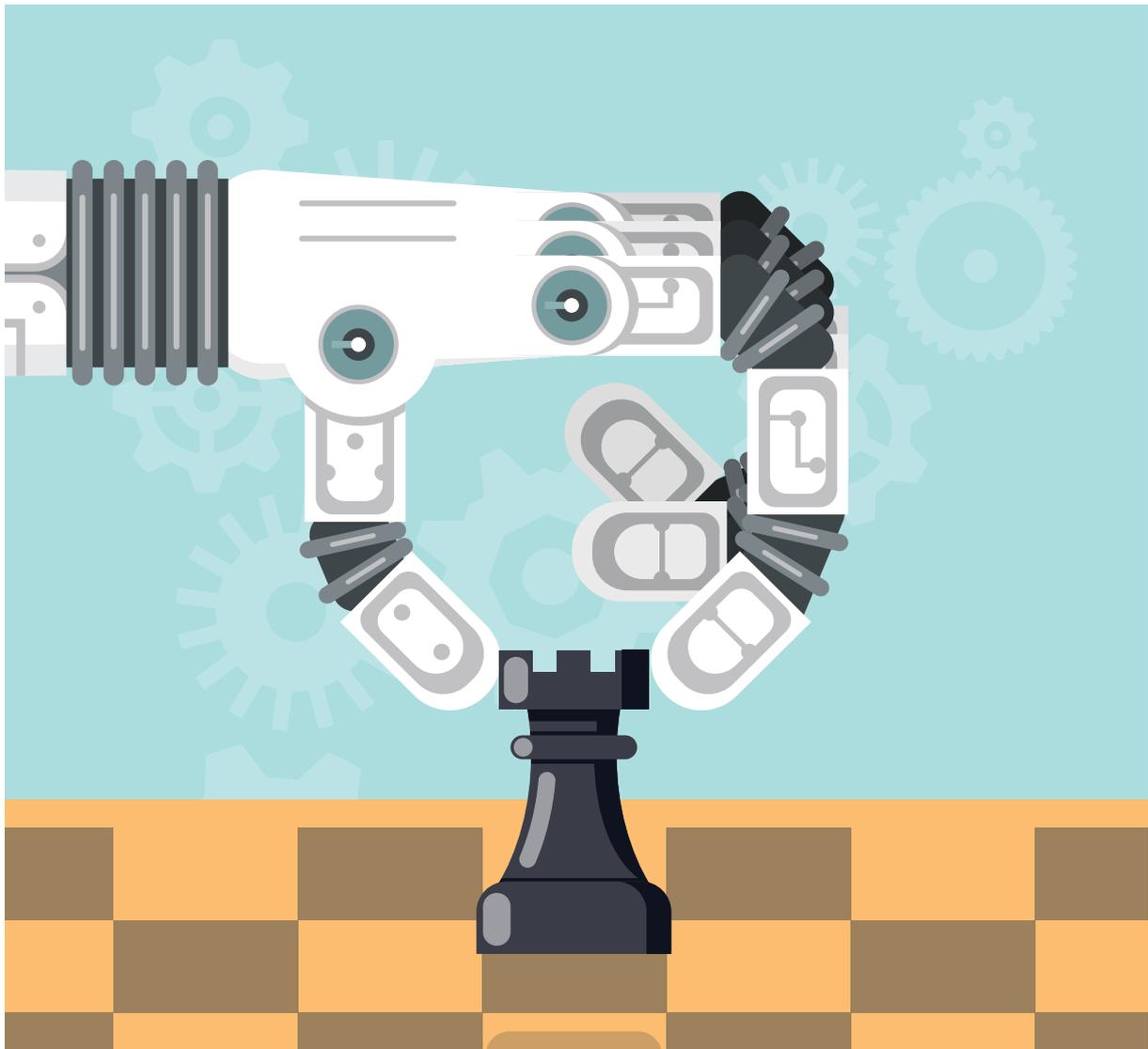
- Connectivité : l'appareil de l'Internet des objets dépend-il uniquement de la connectivité à Internet pour fonctionner correctement ? Dans l'idéal, il devrait pouvoir être utilisé sans avoir à se connecter à Internet. Cet aspect est particulièrement important car si le fabricant de votre appareil ferme la plateforme en ligne qui permet d'en exploiter les fonctionnalités, il n'aura plus aucune utilité.



INFORMATIONS COMPLÉMENTAIRES

- On trouvera plus d'informations sur les droits des consommateurs et la législation européenne à l'adresse : http://ec.europa.eu/consumers/consumer_rights/index_en.htm.
- Articles du Guardian sur l'Internet des objets : <http://www.theguardian.com/technology/internet-of-things>.
- On trouvera plus d'informations sur l'Internet des objets dans l'infographie d'Intel : https://www.intel.fr/content/www/fr/fr/internet-of-things/infographics/guide-to-iot.html?_ga=2.232706015.1300622365.1501789574-718356108.1501789574.
- Disney a mené des études sur l'Internet des jouets : <http://www.disneyresearch.com/project/calipso-internet-of-things/>.
- On trouvera un guide de l'Internet des jouets à l'adresse : <http://www.mutualmobile.com/posts/iot-internet-toys>.
- On trouvera également des informations détaillées auprès du Centre des médias numériques pour enfants (Children's Digital Media Center) : <http://cdmc.georgetown.edu/publications-and-papers/textbooks/>.
- Documents pertinents du Conseil de l'Europe : « Droits de l'homme pour les utilisateurs d'Internet : enfants et jeunes » <http://www.coe.int/fr/web/internet-users-rights/children-and-young-people>.

Intelligence artificielle, automatisation et bouleversements technologiques



L'automatisation¹ est le processus qui consiste à remplacer l'être humain par une machine pour l'exécution d'une action ou d'une fonction données, tandis que le terme « intelligence artificielle »² désigne l'intelligence des machines ou des logiciels

À de nombreux moments de l'histoire, les avancées technologiques ont détruit des emplois pour en créer de nouveaux. Le métier d'opératrice téléphonique, par exemple, a complètement disparu avec l'évolution des technologies de la communication. Les bouleversements du marché de l'emploi provoqués par les révolutions technologiques ne sont pas un phénomène nouveau mais la société redoute toujours qu'il n'y ait pas suffisamment de créations d'emplois pour compenser le nombre d'emplois supprimés.

1. <https://fr.wikipedia.org/wiki/Automation>

2. https://fr.wikipedia.org/wiki/Intelligence_artificielle

■ Jusqu'à présent, ces craintes se sont toujours révélées injustifiées, car de nouveaux métiers ont vu le jour en remplacement des anciens. Personne n'aurait pu imaginer par exemple il y a vingt ans qu'il y aurait un jour des « gestionnaires de médias sociaux » ou des « optimisateurs de moteur de recherche ».

■ Cela dit, les évolutions technologiques actuelles dans le domaine de l'intelligence artificielle, de l'apprentissage machine et de l'automatisation menacent une part beaucoup plus importante du marché de l'emploi que celle se limitant aux emplois peu qualifiés.



INNOVATIONS RECENTES

Véhicules autonomes

■ Bien qu'il reste encore beaucoup de chemin à parcourir jusqu'à ce que les véhicules autonomes soient suffisamment au point pour être produits en série, les progrès dans ce secteur sont indéniables. Tesla, par exemple, fabrique déjà des voitures capables de rouler de manière autonome sur autoroute. Les suites données au tout premier accident mortel dû à une erreur logicielle dans un véhicule Tesla en mai 2016 détermineront l'avenir de la technologie des véhicules autonomes. L'obstacle majeur n'est pas la technologie en elle-même, mais la question des responsabilités en cas d'accident et de la nécessaire adaptation de la loi aux situations dans lesquelles des décisions critiques sont prises par des machines. Une fois ces obstacles levés, les chauffeurs de taxi, camionneurs et conducteurs de transports publics (métro, bus, tram) disparaîtront. Dans l'UE, l'industrie du transport représente 4,5 % du total des emplois.

Sites web, applications et jeux générés automatiquement

■ La conception web est une profession récente mais elle pourrait être amenée à disparaître, plus rapidement même que les opératrices téléphoniques par le passé. Avec les constructeurs de sites web, la création de sites devient de plus en plus facile, puisqu'un simple glisser-déposer suffit pour ajouter du contenu à l'écran. Des algorithmes complexes sont aujourd'hui en mesure de générer un site web automatiquement. « The Grid »³ est le premier à proposer ce service. Il n'a besoin que d'images, de contenu et de quelques informations sur le but du site web et les préférences de l'utilisateur pour produire un site web totalement évolutif (compatibles tous écrans de l'ordinateur au smartphone). Et ce n'est qu'un début. Au fur et à mesure de l'évolution de l'intelligence artificielle, des algorithmes et de l'apprentissage machine, de nombreux emplois qui faisaient appel à des compétences de programmation seront automatisés, et ne subsisteront que ceux qui nécessitent une grande créativité, un degré élevé de personnalisation ou un sens aigu de l'innovation.

Art génératif

■ Grâce aux progrès de l'apprentissage machine, les ordinateurs sont désormais capables de produire des créations artistiques allant des images et peintures à la musique. Le générateur « Deep dream »⁴ de Google analyse des images pour y trouver des objets imaginaires, un peu comme lorsque vous décelez la forme d'un chien ou d'une fleur dans un nuage. D'autres programmes peuvent copier le style d'un peintre comme Van Gogh ou Picasso et l'appliquer à un cliché que vous aurez pris⁵. Dans le domaine de la musique, Emily Howell⁶ est un programme qui analyse des partitions musicales et en déduit des « règles » ou « schémas » pour composer des morceaux dans le même style. Bien que ces avancées ne signent pas la mort des artistes, elles auront certainement un impact sur l'art.

Robots et libre-service

■ Les grands vendeurs en ligne comme Amazon investissent massivement dans des robots pour effectuer des tâches comme le tri et l'organisation de produits ou leur préparation avant livraison. Le tout premier hôtel géré entièrement par des robots a ouvert ses portes au Japon.

3. <https://thegrid.io/>

4. <http://deepdreamgenerator.com/>

5. <http://web.archive.org/web/20160114142911/http://arxiv.org/pdf/1508.06576v2.pdf>

6. <http://artsites.ucsc.edu/faculty/cope/Emily-howell.htm>

Les caisses automatiques des supermarchés, le libre-service dans les restaurants, certains services dans l'hôtellerie, les lignes de production industrielle robotisées, les robots assistants dans le domaine de la santé et des soins aux personnes âgées ou les processus d'envoi automatisés pour le commerce en ligne sont autant d'exemples de services qui commencent à être gérés par des robots. Les exemples d'automatisation des tâches seront de plus en plus nombreux, un peu partout dans le monde. Même les activités de construction seront concernées avec l'avènement de l'impression 3D.

Algorithmes prédictifs et précis

■ Les métadonnées, superordinateurs et puissants algorithmes révolutionneront de nombreux secteurs, dont la santé. La masse de données disponibles dans ce domaine rend les algorithmes plus efficaces que les médecins pour établir un diagnostic à partir des symptômes, des données enregistrées en temps réel par des capteurs et des informations relatives aux antécédents médicaux du patient.

Intelligence artificielle et apprentissage automatique (apprentissage machine)

■ Les ordinateurs et les logiciels de pointe permettent aujourd'hui aux machines d'« apprendre » soit par l'observation des actions humaines pour en tirer des « règles » ou « schémas » et les imiter, soit plus simplement par la pratique, en partant du résultat de certaines actions pour en déduire des « règles ». Des programmes informatiques sont ainsi parvenus à terminer des jeux vidéo en apprenant à battre des ennemis, franchir des obstacles et ainsi de suite. On ignore tout ce que les machines sauront faire à l'avenir mais il est évident que ce qui relève des tâches répétitives est entièrement à leur portée.



INTÉRÊT PÉDAGOGIQUE

- L'apprentissage du codage permet de mieux comprendre la robotique et les logiciels, y compris les bases de l'intelligence artificielle et de l'automatisation. Cet aspect est particulièrement important pour recenser et approfondir les compétences qui restent hors de portée des ordinateurs et des machines mais aussi acquérir celles qui seront nécessaires pour perfectionner toujours plus ces technologies. Vu que les machines seront amenées à remplacer l'homme dans les tâches répétitives et les emplois peu qualifiés, il n'y a pas d'autre solution que de s'instruire davantage.
- Par ailleurs, l'acquisition de connaissances en automatisation et en intelligence artificielle aidera chacun à se forger une opinion sur les grandes décisions politiques à prendre pour faire en sorte que ces technologies aient des retombées utiles à l'ensemble de la société. De nombreux auteurs spécialistes de l'automatisation et de l'intelligence artificielle réclament par exemple un salaire universel et une réduction des heures de travail. Plusieurs scientifiques, chercheurs et personnalités comme Stephen Hawking ont publié une lettre ouverte appelant à donner une orientation claire au développement de l'intelligence artificielle pour nous éviter de devenir un jour les esclaves des machines⁷.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

Destruction d'emplois

■ Le risque le plus évident posé par l'intelligence artificielle et l'automatisation est qu'elles ne fassent disparaître plus d'emplois qu'elles n'en créent. Bien qu'impossibles à prévoir, les emplois de demain liés à l'évolution de ces technologies nécessiteront une main-d'œuvre hautement qualifiée et les perspectives d'emploi pour les personnes n'ayant pas fait d'études au-delà de l'enseignement secondaire seront limitées.

7. http://futureoflife.org/AI/open_letter

Renforcement des inégalités

■ Les emplois peu qualifiés se raréfieront, ce qui creusera les inégalités entre ceux qui auront les compétences recherchées et ceux dont le travail sera progressivement remplacé par des machines. D'autres formes d'inégalités s'observeront également entre les pays qui disposeront du savoir-faire technologique nécessaire pour effectuer la transition vers l'automatisation et les innovations de l'intelligence artificielle et les autres qui continueront de s'appuyer sur le travail manuel. Sans politiques adaptées dans le secteur de l'emploi, de l'éducation et de la formation et dans le domaine social, ces inégalités pourraient causer des troubles sociaux.

Dépendance excessive à l'égard des machines

■ L'automatisation et l'intelligence artificielle ne sont pas des solutions miracles. Aujourd'hui, elles nécessitent encore une supervision par l'homme et ne font qu'apporter une assistance dans la réalisation de tâches plus complexes. Par exemple, si piloter un avion en mode automatique à une altitude de croisière ne pose aucun problème à un logiciel, l'intervention de l'homme reste nécessaire au décollage et à l'atterrissage. Cela dit, moins de formation et moins de pratique risquent de mettre les pilotes en difficulté devant une situation critique ne pouvant être résolue par le pilote automatique. Il en va de même pour les voitures automatiques. Dans un futur où le transport sera automatique, que se passera-t-il en cas de défaillance du logiciel, si aucun humain ne sait plus conduire ? Que restera-t-il à l'homme si les machines finissent par tout faire à sa place, et sont même capables de se créer et de se réparer toutes seules ? Une telle situation risquerait d'entraîner une régression massive d'une partie de la population qui ne rechercherait plus que le divertissement au détriment de l'approfondissement de leurs compétences et de leurs connaissances, ce qui créerait des inégalités supplémentaires et des tensions sociales.

Ajustement et évolution lents ou inappropriés des compétences

■ Il est très difficile aujourd'hui de prévoir ce que l'automatisation et l'intelligence artificielle permettront de faire demain et donc d'imaginer quelles compétences privilégier comme étant celles « du futur ». Alors que le monde de l'éducation s'éveille tout doucement à l'idée d'enseigner la programmation et le codage à l'école, les derniers développements de l'intelligence artificielle montrent qu'il est possible d'automatiser la programmation car elle repose sur des règles logiques et claires. La conception web générée automatiquement en est l'illustration.

Sécurité

■ Comme tous les appareils connectés à Internet ou fonctionnant à l'aide d'un logiciel, l'intelligence artificielle et l'automatisation sont vulnérables au piratage, mais avec des conséquences potentiellement beaucoup plus graves que le vol ou la destruction de données à caractère personnel. Une équipe de spécialistes de la sécurité a montré qu'il était possible de pirater une voiture connectée et d'en prendre le contrôle pour éteindre le moteur, par exemple, ou prendre le volant à faible vitesse. Imaginez les conséquences du piratage d'une voiture autonome sans volant.

La fin du travail ennuyeux, le début d'un monde insipide ?

■ Les principaux défis posés par l'intelligence artificielle et l'automatisation sont peut-être d'ordre philosophique. Qu'est-ce qui rend notre monde intéressant ? L'homme peut-il être heureux dans un monde dont il comprendrait tout, qui serait entièrement prévisible et optimisé et où il n'y aurait pas le moindre accroc ? Qu'en est-il de la spontanéité humaine, du choix délibéré de faire des erreurs et d'en tirer des enseignements, voire du droit de prendre une décision déraisonnable car on le peut, tout simplement ? L'introduction de décisions « automatisées » est une suite logique de la domination de la société par la science, les faits et la raison, mais est-ce sain pour les humains ? Alors que de nombreux scientifiques et intellectuels avaient prévu, il y a un siècle, la disparition du religieux au profit de la science, on assiste aujourd'hui à un regain d'intérêt pour la spiritualité et la religion. Est-ce là le symptôme d'un monde incapable de donner un sens à notre vie et en guerre avec tout ce qui fait de nous des êtres humains : les émotions, les sentiments, l'impulsivité et l'irrationalité ?



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Une bonne activité d'introduction à l'intelligence artificielle en classe est celle dite du « papier intelligent ». Elle consiste à présenter une fiche d'instructions permettant de battre tout enfant ou jeune à un jeu de morpion. Voir les instructions détaillées ici : <http://web.archive.org/web/20160326100226/http://csunplugged.org/artificial-intelligence/>.
- À la suite de cette activité, demandez à vos enfants ou élèves s'ils peuvent citer des exemples d'utilisation de l'intelligence artificielle dans leur vie quotidienne.
- La plupart des smartphones sont équipés de leur propre « assistant personnel », à savoir Siri pour iOS/Apple, Google Now pour Android/Google et Cortana pour Windows/Microsoft. Tous trois présentent des caractéristiques de l'intelligence artificielle : ils sont dotés d'un système de reconnaissance vocale qui s'améliore en écoutant des millions de voix humaines, d'un algorithme pour répondre aux questions que vous leur posez et de fonctions de personnalisation de l'information affichée en fonction des données que vous y intégrez (données de recherche, coordonnées, données de localisation, etc.). Il en va de même pour d'autres fonctionnalités de base comme la saisie prédictive, qui relèvent elles aussi de l'intelligence artificielle.



BONNES PRATIQUES

- L'intelligence artificielle, l'automatisation et l'apprentissage machine peuvent être très utiles à condition de toujours maintenir des compétences manuelles en cas de défaillance. Par exemple, même si les applications GPS sont aujourd'hui courantes sur les smartphones, il n'est jamais vain d'apprendre à lire une carte routière et de développer son sens de l'orientation.
- Gardez tout sous contrôle. Il existe de nombreux degrés d'automatisation, le plus haut étant celui où une machine prend toutes les décisions sans intervention ou validation par l'homme. De la même manière que la saisie prédictive laisse à l'utilisateur le choix d'accepter ou de rejeter la proposition faite par le logiciel, il faudrait également configurer tout appareil ou logiciel automatisé ou doté d'intelligence artificielle de manière à ce qu'il demande votre aval.
- Soyez préparé au changement et disposé à acquérir des compétences très diverses. Compte tenu des bouleversements qu'apporteront ces nouvelles technologies, ce seront les travailleurs les plus flexibles et polyvalents qui s'adapteront le plus facilement. Il est probable qu'à l'avenir, ils doivent régulièrement suivre des formations ou retourner en classe pour apprendre de nouvelles choses. L'apprentissage tout au long de la vie sera la norme.
- Renforcez vos compétences interpersonnelles, sociales et émotionnelles car celles-ci échappent à toute forme d'automatisation. Les robots et algorithmes pourront peut-être exécuter des tâches demandant peu de qualifications, mais jamais ils ne remplaceront les interactions humaines.
- L'intelligence artificielle et l'automatisation s'appuient sur des logiciels. Veillez à mettre à jour régulièrement vos appareils connectés pour qu'ils soient toujours équipés de la version la plus récente du logiciel d'exploitation et configurez les paramètres de sécurité au niveau le plus élevé. Si votre appareil n'a pas besoin de connexion permanente à Internet pour fonctionner, veillez à ce qu'il soit déconnecté pour limiter le risque de piratage.
- Pour bien comprendre les enjeux et avoir une vision globale de ce que l'avenir nous réserve, lisez également les fiches d'information sur les métadonnées, la réalité virtuelle et la réalité augmentée et l'Internet des objets. Il faut bien comprendre que les métadonnées alimentent l'intelligence artificielle et l'automatisation, tandis que la réalité augmentée et la réalité virtuelle sont de nouveaux moyens d'interagir avec l'intelligence artificielle et les machines. L'Internet des objets remplit également cette fonction d'interaction mais apporte en plus des données utiles qui contribueront au développement de ces technologies. Ce n'est qu'en ayant une vue d'ensemble des choses que les citoyens pourront faire des choix conscients et éclairés sur la manière d'appréhender ces changements pour améliorer la société.



INFORMATIONS COMPLÉMENTAIRES

- Article de la BBC sur l'intelligence artificielle : <http://web.archive.org/web/20160509115227/http://www.bbc.com/news/technology-34224406>.
- Page de recherche Google sur l'intelligence artificielle et l'apprentissage automatique : <http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>.
- Les actualités de l'automatisation sont présentées sur le site : <http://www.automationworld.com/>.
- Page officielle du Consumer Electronics Show qui présente souvent les innovations les plus récentes dans les différents secteurs de la technologie : <https://www.cesweb.org/>.
- On trouvera des informations sur les études et dernières évolutions dans le domaine des TIC dans le magazine Horizon (the EU Research and Innovation Magazine) de la Commission européenne : <http://horizon-magazine.eu/topics/ict>.

Réalité virtuelle et réalité augmentée



Réalité virtuelle¹ est une expérience multimédia d'immersion où l'on reproduit un environnement qui simule la présence physique dans le monde réel. L'expérience sensorielle ainsi créée peut faire appel à la vue, à l'ouïe, au toucher, à l'odorat et au goût, les deux premiers sens étant les plus fréquemment utilisés.

■ La réalité augmentée² consiste à ajouter des éléments sensoriels générés par ordinateur, comme du son ou des images, à des environnements du monde réel.

■ Bien que l'idée de réalité virtuelle et de réalité augmentée ait été évoquée pour la première fois il y a plusieurs décennies déjà, ce n'est que récemment que la technologie a suffisamment évolué pour permettre d'envisager la commercialisation d'appareils, de services et de logiciels de réalité

1. https://fr.wikipedia.org/wiki/Réalité_virtuelle

2. https://fr.wikipedia.org/wiki/Réalité_augmentée

virtuelle et de réalité augmentée. Les applications de réalité augmentée ont connu une croissance rapide grâce aux smartphones, à l'Internet mobile et aux techniques de géolocalisation.

■ Voici quelques exemples d'évolutions récentes dans le domaine de la réalité virtuelle et de la réalité augmentée :

- la multiplication des casques de réalité virtuelle comme Oculus Rift, Samsung Gear VR, HTC Vive ou Sony Playstation VR, avec un certain nombre de jeux prêts à être mis sur le marché, notamment par le biais des plateformes mobiles Android et iOS, la PlayStation 4, la Xbox One et les jeux informatiques traditionnels sur PC ou Mac ;
- la multiplication des casques ou lunettes de réalité augmentée comme les lunettes Google Glass et le HoloLens de Microsoft, qui prévoit aussi de lancer une version de Minecraft en réalité augmentée à laquelle vous pourrez jouer depuis votre salon ;
- la sortie de jeux de réalité augmentée comme Pokemon Go qui permet d'attraper des Pokemons dans le monde réel grâce à un smartphone (iOS et Android).



INTÉRÊT PÉDAGOGIQUE

- La réalité virtuelle, en permettant de simuler une expérience du monde réel, offre de très nombreuses possibilités d'apprentissage. Il est par exemple possible de simuler avec beaucoup de précision la conduite d'un véhicule.
- Les premières expériences d'utilisation de la réalité virtuelle à des fins thérapeutiques, par exemple pour soigner l'arachnophobie ou surmonter un stress post-traumatique, ont donné des résultats prometteurs. Du fait du degré d'immersion qu'elle permet, cette technologie accroît également le niveau d'empathie et de compréhension de l'autre en permettant à l'utilisateur de se rendre compte de ce que vit, par exemple, une personne handicapée (un aveugle ou une personne en fauteuil roulant) ou une personne appartenant à une minorité victime de discrimination.
- Bien que rien ne puisse remplacer la réalité, tout le monde n'a pas la chance de pouvoir voyager. La réalité virtuelle permet de simuler la visite d'un monument ou de tout autre lieu « comme si l'on y était », et va même plus loin en vous faisant découvrir des endroits où vous ne pourriez jamais vous rendre en temps normal, comme la Lune ou l'espace, ou l'intérieur d'un volcan. Elle peut également vous transporter dans le passé, sur un champ de bataille au XVIIIe siècle ou au milieu des dinosaures.
- Les applications pratiques de la réalité augmentée sont trop nombreuses pour pouvoir toutes être citées ici. Cette technique consistant à ajouter des informations ou des objets au monde réel, elle offre des possibilités quasi illimitées. Elle peut ainsi remplacer un guide touristique en superposant toutes sortes d'informations à l'image que vous verrez d'un monument ou d'une statue. Elle peut afficher des informations concernant tout autre objet du monde réel, par exemple un menu ou une évaluation d'un restaurant, rappeler des noms de personnes ou des informations à leur sujet lorsque vous les voyez, et ainsi de suite. Sur le plan de l'apprentissage, elle ouvre également des possibilités infinies : vous montrer les étapes à suivre pour réparer ou remplacer une pièce automobile, aider un chirurgien lors d'une opération ou encore vous assister dans la préparation d'une recette en expliquant la manière de découper et de mélanger les ingrédients, par exemple. Tout ce que vous voyez peut être « augmenté » par l'ajout d'informations. Une salle de classe peut ainsi devenir une scène à laquelle on pourra ajouter des objets virtuels, par exemple un modèle de corps humain semi-transparent.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

Risques comportementaux

■ La réalité augmentée s'appuie sur l'analyse permanente, en temps réel, du monde physique qui nous entoure pour l'augmenter avec précision au moyen d'éléments virtuels. Autrement dit, elle nécessite d'intégrer votre localisation et vos recherches à des supercalculateurs, généralement en ligne, pour définir exactement les éléments à afficher. Sans protection adéquate de la vie privée, la réalité augmentée pourrait devenir un moyen d'espionner toujours plus les individus, en temps réel.

Sécurité

■ Les appareils étant connectés en permanence à Internet, le piratage en direct à distance devient plus facile. Lorsque nous commencerons à utiliser des appareils de réalité virtuelle et de réalité augmentée, comme des lunettes ou des lentilles de contact, de nouvelles situations potentiellement graves pourront se présenter. On pourrait imaginer par exemple qu'une personne mal intentionnée décide de distraire un automobiliste de la route en piratant l'écran de réalité augmentée utilisé par celui-ci pour s'orienter.

Manipulation et consumérisme

■ La réalité virtuelle et la réalité augmentée s'accompagnent également de nouvelles stratégies publicitaires. En l'absence de réglementation, le champ des possibles est illimité et l'on peut aisément imaginer des techniques qui permettraient « d'augmenter » votre domicile à l'aide de publicités. Par exemple, vous pourriez ouvrir votre réfrigérateur et un dispositif publicitaire « augmenterait » le contenu de celui-ci pour afficher les produits qui « devraient » s'y trouver. Autre possibilité : au supermarché, après avoir scanné un produit avec votre smartphone, vous recevriez un message vous suggérant l'achat d'un autre produit.

Dépendance et caractère addictif

■ Les neurosciences ont fait des progrès considérables ces dernières années et l'on a beaucoup appris sur le fonctionnement de notre cerveau. Les circuits cérébraux du plaisir sont activés par des stimuli rapides comme l'action ou le mouvement. C'est ce qui fait le succès des jeux vidéo et des films d'action. Hélas, vivre dans le monde « réel » requiert un certain nombre de qualités dont la réserve, la maîtrise de soi, la patience, la persévérance et l'anticipation. Tout ne peut pas être rendu ludique ou agréable par la technologie. L'apprentissage du violon en est un exemple. Les enfants grandissant avec la réalité virtuelle et la réalité augmentée, il y a un risque qu'ils ne puissent s'adapter à un monde qui ne serait pas « augmenté » ou aussi « riche » et stimulant que leur réalité « virtuelle ». Les jeux de rôles multijoueurs en ligne le montrent parfaitement. Bien qu'ils permettent de développer un grand nombre d'aptitudes comme le sens de l'organisation, la planification, les capacités d'animation et la coopération, ils sont conçus de manière à être juste assez captivants pour conserver l'intérêt des joueurs mais pas trop difficiles pour ne pas les décourager. La réalité virtuelle et la réalité augmentée aggraveront encore ce problème et pourraient créer un phénomène d'addiction à un monde moins frustrant et beaucoup plus grisant que le monde réel, dans lequel il est plus facile de s'en sortir.

Perte des compétences interpersonnelles et comportements asociaux

■ Bien que restant marginale, la tendance au « hikikomori » – ces adultes et adolescents qui se retirent complètement de la société – est en augmentation dans certains pays comme le Japon. La télévision, les médias et Internet, même s'ils ne sont pas directement liés à ce phénomène, le rendent plus supportable car ils distraient des difficultés de la vie « réelle ». La réalité virtuelle et la réalité augmentée pourraient le renforcer car le virtuel peut sembler plus facile à surmonter et plus gratifiant que des relations humaines complexes. Même la sexualité peut induire des émotions négatives, imposer une pression de la performance ou rendre difficile l'acceptation de son image corporelle, autant de blocages qui disparaissent dans un monde virtuel où l'utilisateur maîtrise tout.

Santé physique

■ La réalité virtuelle et la réalité augmentée donnent également la possibilité de pallier le manque d'activité physique, par exemple d'utilisateurs assis passivement derrière leurs écrans pendant des heures. Les jeux basés sur la localisation, par exemple, peuvent se dérouler dans le monde réel grâce à la réalité augmentée, et des salles peuvent être spécialement créées pour les environnements de réalité virtuelle. Cela dit, les expériences d'immersion posent de nouveaux problèmes comme l'absence de réaction aux signaux de la douleur ou les excès d'utilisation dus à la faculté du contenu virtuel ou « augmenté » de capter pleinement notre attention. Des mouvements répétitifs dans un jeu peuvent créer des tendinites, comme cela a été vu avec certains jeux sur Wii. De même, une expérience immersive dans le cadre de la réalité augmentée peut provoquer des nausées semblables à celles dues au mal des transports lorsque les images qui parviennent au cerveau par le biais d'un écran monté sur casque se heurtent aux informations transmises par les capteurs de mouvement dans l'oreille interne. Enfin, de nombreux bêtesteurs ont indiqué s'être blessés en tombant ou en se cognant à un objet lorsqu'ils étaient immergés dans la réalité virtuelle ou lorsqu'ils fixaient leur écran de smartphone en jouant à des jeux de réalité augmentée dans le monde réel.

Harcèlement, cyberharcèlement et risques liés aux contacts

■ Les frontières entre réel et virtuel se modifiant, la réalité virtuelle et plus encore la réalité augmentée pourraient être utilisées comme moyen instantané et direct d'humilier quelqu'un, par exemple en programmant l'affichage d'une tête de rat sur une personne avec la fonction de reconnaissance des visages ou en partageant une vidéo en direct de quelqu'un se trouvant dans une situation embarrassante.

■ La réalité augmentée, et dans une moindre mesure la réalité virtuelle, posent des risques liés aux rencontres que l'on fait. Les jeux de réalité augmentée massivement multijoueurs impliquent de jouer dans le monde réel contre des personnes qui nous sont étrangères. Cela peut donner lieu à des agressions dans le monde réel.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

- La réalité augmentée et la réalité virtuelle nécessitent du matériel. Si votre établissement ou votre institution ne sont pas dotés de tablettes, par exemple, vous ne pourrez pas profiter pleinement de ces technologies. Dans certains cas, il serait possible d'utiliser les appareils des élèves (par exemple leurs smartphones) mais cela pourrait entrer en conflit avec la politique de l'école en la matière, certaines interdisant l'utilisation de ces appareils pendant les heures de cours, et pourrait être porteur de discrimination car les élèves n'auront peut-être pas tous un téléphone portable suffisamment puissant pour permettre une telle activité, voire n'en auront aucun.
- Cela dit, il existe de nombreuses ressources en ligne pour vous aider à utiliser la réalité augmentée et la réalité virtuelle en classe. La première est plus simple à mettre en œuvre car elle ne nécessite pas de casque pour l'immersion totale et fonctionne avec les appareils existants comme les smartphones et tablettes.
- Si vous vous intéressez à la réalité augmentée, vous trouverez une liste de tutoriels, de guides et d'applications sur le site web de Kathy Schrock « A guide to everything »³.



BONNES PRATIQUES

- Une nouvelle fois, le manque de connaissances sur les effets d'une utilisation ou d'une exposition prolongées à ces nouvelles technologies impose de maintenir un équilibre de vie sain. Veillez à ce que vos enfants et vous-même pratiquiez, en plus des activités « connectées », virtuelles ou augmentées, des sports ou d'autres loisirs plus « classiques ».

3. <http://web.archive.org/web/20160318145342/http://www.schrockguide.net/augmented-reality.html>; <http://www.onlineuniversities.com/blog/2012/09/20-coolest-augmented-reality-experiments-education-so-far/>

La même remarque vaut dans le domaine de l'enseignement. La réalité augmentée et la réalité virtuelle sont en plein essor et même s'il est indéniable qu'elles possèdent des vertus pédagogiques, il n'y a pas de solution miracle pour garantir une éducation de qualité. Là encore, un bon équilibre entre méthodes d'enseignement traditionnelles et pédagogies plus novatrices est la voie à suivre.

- Choisissez avec soin le contenu que vous achetez à vos enfants s'ils utilisent des appareils de réalité virtuelle ou de réalité augmentée et vérifiez ce à quoi ils ont accès. Lisez les restrictions d'âge et les étiquettes, par exemple les labels PEGI (voir Fiche d'information 20 sur la classification/étiquetage et le filtrage et Fiche d'information 16 sur les jeux). Sur les appareils utilisés par les plus jeunes, activez les outils de contrôle parental pour vous assurer qu'ils ne peuvent accéder à du contenu librement et utilisez des listes blanches si cette fonctionnalité existe dans votre pays/votre langue car c'est le meilleur moyen de protéger les enfants tout en veillant à ce qu'ils soient exposés à du contenu positif évalué par des professionnels.
- Il est plus important que jamais de parler ouvertement avec les enfants et les jeunes de la violence, de la cyberintimidation, des questions de sexualité et des droits et responsabilités de chacun. Une solide éthique dès le plus jeune âge constitue le moyen le plus efficace de neutraliser tout message sexiste, raciste, discriminatoire ou négatif que les enfants pourraient rencontrer en ligne ou sur leurs appareils de réalité augmentée et de réalité virtuelle.
- Réglez les paramètres de confidentialité et de sécurité au niveau le plus haut pour les jeunes enfants. Voir la Fiche d'information 9. N'oubliez pas que ces appareils peuvent être piratés.
- Vérifiez bien le modèle commercial qui sous-tend le contenu ou l'appareil que vous utilisez dans le cadre des activités de réalité virtuelle ou augmentée, car votre enfant ou vous-même risquez d'être exposés à de la publicité intempestive.



INFORMATIONS COMPLÉMENTAIRES

- On trouvera l'actualité de la réalité virtuelle sur le site Venture Beat : [<http://venturebeat.com/tag/virtual-reality/>](http://venturebeat.com/tag/virtual-reality/).
- Article de l'Université de Stanford sur la réalité virtuelle et l'éducation : <https://teachingcommons.stanford.edu/teaching-talk/virtual-reality-and-education>.
- On trouvera l'actualité de la réalité augmentée sur le site Venture Beat : <http://venturebeat.com/tag/augmented-reality/>.
- Les guides de recherche de la bibliothèque du Dartmouth College contiennent des informations sur la réalité augmentée : <http://researchguides.dartmouth.edu/AR>.

Êtes-vous le produit ? Big data, exploration de données et vie privée



Big data¹ (« mégadonnées ») est un terme générique utilisé pour désigner un ensemble de données si vaste qu'il ne peut être analysé ou traité au moyen de méthodes traditionnelles (avec un ordinateur ou une application simple, par exemple).

■ Le big data est né de la conjonction entre :

- une augmentation continue et spectaculaire de la capacité de stockage numérique ;
- la production d'un volume toujours plus important de données dans nos sociétés (de plus en plus, tout ce que nous faisons laisse une trace numérique) ;
- un monde interconnecté via Internet qui permet de relier entre elles les données, et
- une capacité croissante à analyser et à interpréter l'ensemble des données ainsi générées.

1. https://fr.wikipedia.org/wiki/Big_data

■ Parmi les services en ligne qui utilisent les métadonnées, on peut citer les réseaux sociaux comme Facebook, les moteurs de recherche comme Google ou Bing et les vendeurs en ligne comme Amazon. Cela dit, elles ne se limitent pas au monde en ligne et sont également présentes partout dans notre quotidien.

- Les supermarchés utilisent les cartes de fidélité pour analyser les habitudes d'achat et ajuster leur inventaire en temps réel ou programmer un événement commercial (offres spéciales, soldes, etc.).
- Les données générées par les automobilistes, les capteurs des véhicules et les GPS contribuent à fournir des informations en temps réel sur le trafic routier.
- Dans les hôpitaux, l'analyse en temps réel des données enregistrées par des capteurs, comme la fréquence cardiaque, peut contribuer à détecter des infections ou d'autres problèmes de santé avant l'apparition de signes et symptômes externes.

■ Les données sont également devenues l'une des monnaies d'échange les plus courantes en ligne. Au lieu d'acheter avec de l'argent les services que vous utilisez, par exemple les réseaux sociaux ou les moteurs de recherche, vous « payez » avec les données que vous leur apportez et qui leur permettent de personnaliser leur publicité et leurs stratégies commerciales en fonction de vos préférences pour les rendre plus efficaces. Mais la comparaison ne va peut-être pas suffisamment loin car par rapport à l'argent, les données possèdent une caractéristique qui leur confère une importance névralgique : elles peuvent être réutilisées et revendues. Il serait donc plus juste de dire que cet « échange » équivaldrait à céder les clés de votre maison pour pouvoir accéder à un service !

■ Cette révolution n'en est qu'à ses débuts car les données deviendront de plus en plus abondantes, par exemple avec l'Internet des objets (voir Fiche d'information 23) et seront analysées de plus en plus finement grâce à la puissance croissante de l'informatique et aux avancées techniques (intelligence artificielle, etc.).



INTÉRÊT PÉDAGOGIQUE

- Les métadonnées peuvent vous faciliter la vie à bien des égards : en faisant en sorte d'augmenter la précision de vos requêtes, d'optimiser votre temps de trajet entre votre domicile et votre lieu de travail ou d'études, d'approvisionner les commerces locaux avec les produits dont vous avez besoin, et ainsi de suite.
- Il est essentiel de s'informer sur le big data et son fonctionnement pour bien comprendre son pouvoir et en faire un atout plutôt qu'un obstacle. Cela implique de définir le type de données que vous souhaitez partager et de choisir vos produits ou services en fonction de l'usage qu'ils feront de ces données.
- Le big data peut également nous aider à comprendre nos sociétés puisqu'il rend possible, pour la première fois dans l'histoire de l'humanité, l'analyse et l'interprétation de grands volumes de données générées par les individus. Pour les sciences sociales, la psychologie, les sciences comportementales, le secteur médical, le marketing et bien d'autres secteurs de la recherche, le big data est une véritable révolution. Les enseignants pourront exploiter les données recueillies dans ces domaines pour illustrer certains concepts sociologiques à l'aide d'exemples et de chiffres tirés de la vie réelle.
- Dans le monde en ligne, la prévalence des modèles économiques ayant pour principale source de revenus les données nous impose d'acquérir de nouvelles compétences, notamment en matière de gestion des données à caractère personnel et de protection de la vie privée. Par conséquent, de la même manière que vous gérez votre budget et vos finances de manière responsable sans effectuer de dépenses inconsidérées, vous devrez apprendre à gérer vos données personnelles avec rigueur et à ne pas les partager à l'excès.



CONSIDÉRATIONS ÉTHIQUES ET RISQUES

Protection de la vie privée et des données

■ Bien que de nombreuses lois protègent les données et la vie privée des individus, dans la pratique, elles sont difficiles à mettre en œuvre. Le Règlement général sur la protection des données demande aux services de solliciter le consentement explicite de l'utilisateur, mais il est probable que cela se limite à un nouvel exercice de « cases à cocher » comparable à l'approbation des « conditions d'utilisation », que l'utilisateur est souvent contraint d'accepter s'il ne veut pas renoncer au service. Il n'exerce alors qu'un contrôle partiel sur ses données et n'a que deux choix possibles : ne rien partager ou tout partager. Même si le Règlement précité essaie de traiter la question du consentement du consommateur en introduisant le principe de proportionnalité (seules les données strictement nécessaires à l'exécution d'une prestation pourront être demandées à l'utilisateur par un service donné), son interprétation et son application concrètes pourraient ne pas être suffisantes pour protéger les utilisateurs. Les réseaux sociaux ont-ils par exemple besoin d'utiliser vos données pour trier votre fil d'actualités ?

■ Les notions mêmes de respect de la vie privée et de protection des données devront être approfondies dans les années à venir. Que signifie « respect de la vie privée » ? Vos données peuvent-elles être exploitées tant qu'elles restent anonymes ? Comment mieux contrôler le partage et l'utilisation de vos données vu la quantité de données générées par les utilisateurs chaque jour ?

Discrimination

■ Que ce soit pour souscrire une assurance-vie, postuler à un emploi, demander un prêt ou faire assurer une voiture, votre situation fera systématiquement l'objet d'une évaluation. Un questionnaire de santé vous demandera si vous fumez ou si vous faites du sport, vos compétences seront testées lors d'un entretien d'embauche et votre banquier examinera de plus près la manière dont vous avez géré votre budget récemment et remboursé vos précédents prêts. Dans pareils cas, où se situe la limite entre une évaluation « raisonnable » et une violation pure et simple de votre vie privée ? De nombreux employeurs utilisent déjà les informations qu'ils trouvent en ligne sur les candidats à un poste pour prendre leurs décisions de recrutement et de nombreux indices révèlent une tendance, de la part des compagnies d'assurance et des banques, à analyser les données en ligne pour estimer la probabilité d'une capacité de remboursement insuffisante ou d'un problème de santé grave. Si les métadonnées peuvent sauver des vies par leurs capacités prédictives, elles peuvent également empêcher certaines personnes d'avoir accès à des services financiers ou aux soins médicaux de base.

Quand la lutte contre la discrimination devient un commerce

■ Des sociétés de gestion de la réputation en ligne ont commencé à faire leur apparition sur Internet. Les particuliers et entreprises peuvent faire appel à leurs services (payants) pour gérer leur réputation et veiller à ce que leurs données ne les excluent pas de l'accès à certains services comme le crédit/l'investissement, l'assurance ou l'emploi. Il s'agit là d'un exemple d'exploitation commerciale d'un cycle d'externalités, un peu comme si l'on polluait une rivière et l'on vendait des médicaments aux citoyens empoisonnés avant de rémunérer une société pour dépolluer l'eau.

Manipulation et consumérisme

■ Le modèle commercial le plus courant des applications et services en ligne étant la publicité « gratuite », souvent basée sur l'exploitation des données des utilisateurs, il existe un risque que les consommateurs soient exposés à un nombre toujours plus important de messages les incitant à consommer. La publicité en ligne croît chaque année et les nouvelles techniques qui forcent les consommateurs à visualiser une publicité ou à cliquer sur une publicité évoluent rapidement. Les publicités vidéo en pre-roll (c'est-à-dire diffusées avant que l'Internaute n'ait accès au contenu vidéo qu'il souhaite consulter), par exemple, ne sont apparues qu'il y a quelques années. Le big data alimente cette croissance en optimisant la publicité et en l'adaptant aux habitudes et intérêts des individus tout en déterminant à partir de la masse de données disponibles l'esthétique, le lieu et la méthode les plus efficaces pour qu'une publicité soit vue et génère des interactions.

Persécution politique

■ Bien que certains gouvernements respectent la vie privée et n'espionnent pas leurs citoyens, ce n'est pas le cas de tous. Les révélations d'Edward Snowden ont montré que des gouvernements du monde entier espionnent les Internautes. Dans certains cas, ces ingérences sont justifiées pour des raisons de sécurité comme la lutte contre le terrorisme et la prévention d'attaques terroristes, mais il convient de toujours s'interroger sur leur proportionnalité. La police peut par exemple se servir des profils sur les réseaux sociaux pour identifier les citoyens présents lors d'une manifestation.

Droits du consommateur

■ Les métadonnées sont la nouvelle monnaie d'échange en ligne, mais que reçoivent les utilisateurs en contrepartie ? Le droit d'utiliser un service en ligne truffé de publicités intempestives ? Lorsqu'ils paient un abonnement mensuel pour bénéficier d'un service, ils sont protégés par les lois relatives au droit du consommateur et peuvent demander une indemnisation si le service ou le contenu ne répond pas à leurs attentes ou présente de sérieuses lacunes. Un utilisateur pourrait ainsi demander à une plateforme de vidéo en ligne de se faire rembourser s'il ne peut visionner un film, mais qu'en est-il si votre réseau social préféré présente des dysfonctionnements ou devient indisponible ? À quelle compensation avez-vous droit ? Après tout, il exploite vos données pour vous montrer des publicités et en tire des revenus. Ce nouveau modèle commercial exploitant les données pose de nombreux problèmes du point de vue des droits du consommateur. Étant présenté comme « gratuit », il ne propose bien souvent aucune compensation aux utilisateurs et ne leur accorde que des droits très limités.

La fin de l'anonymat

■ Bien que les pseudonymes et surnoms n'aient pas encore disparu, l'anonymat est sérieusement menacé par l'avènement du big data. En établissant des liens entre plusieurs ensembles de données anonymisées, il est en effet possible d'identifier une personne par son véritable nom en ligne. Même en prenant beaucoup de précautions quant au contenu que l'on met en ligne, il sera difficile dans les prochaines années de rester anonyme en ligne, ce qui laisse présager le meilleur comme le pire.

Internet n'oublie jamais

■ Le droit à l'oubli s'est progressivement imposé depuis que l'Union européenne a pris des mesures juridiques pour le mettre en œuvre. Dans la pratique, il reste toutefois difficile à faire respecter. Le contenu numérique peut aisément être transféré, légèrement modifié pour ne plus pouvoir être reconnu par les robots ou les modérateurs ou être hébergé sur des serveurs ou auprès de services ne relevant pas du droit de l'UE. Grâce aux fonctionnalités des smartphones, plus personne n'est à l'abri de retrouver en ligne des photos ou des vidéos de lui en train de faire le pitre lors d'une soirée, qui lui vaudront des railleries du monde entier. Il restera encore à trouver un compromis entre droit à l'oubli et droit de demander des comptes.

Contenus et services de mauvaise qualité

■ Les prestataires en ligne et les créateurs de contenus s'appuyant de plus en plus sur la publicité pour générer des revenus, ils chercheront à optimiser l'attractivité de leur service ou de leur contenu. Les métadonnées aident à déterminer ce qui rend un article, une photo ou une vidéo attractifs, mais cela ne risque-t-il pas d'affecter la qualité du service ou du contenu en question ? De plus en plus d'articles en ligne sont rédigés de manière à attirer les utilisateurs et à les faire cliquer sur des liens ou des messages qui les redirigent vers des pages truffées de publicités. On voit fleurir un peu partout sur Internet des titres aguicheurs comme « trois secrets pour perdre du poids », « vous ne devinez jamais ce que cette femme va faire devant sa caméra » ou « les 10 chats les plus mignons du web ». Bien que le divertissement et les contenus anecdotiques ne constituent rien de mal en soi, de tels modèles commerciaux reposant sur la publicité incitent fortement à ne créer que ce type de contenu au détriment d'éléments factuels fiables ou de contenus à caractère pédagogique.



SUGGESTIONS D'ACTIVITÉS EN CLASSE

Pour les jeunes de plus de 14 ans : invitez les jeunes à effectuer une recherche sur leur nom et/ou à voir quelles données les concernant sont accessibles en ligne, puis à les examiner du point de vue d'un employeur, d'une compagnie d'assurances et de la police. Quelle image renverraient-ils à ces personnes si ces dernières s'appuyaient sur ces informations pour mieux les connaître ? Des partages d'articles sur les bienfaits de la procrastination ou des mises à jour de statut contenant de nombreuses fautes d'orthographe pourraient par exemple les discréditer auprès de l'employeur. De la même manière, des photos sur lesquelles on les verrait fumer ou boire ou pratiquer des activités dangereuses pourraient être très mal vues par l'assureur. Enfin, des messages critiquant leur gouvernement et appelant à un changement radical pourraient paraître suspects aux yeux des services de police.



BONNES PRATIQUES

- Internet et les métadonnées ne sont finalement qu'une étape de plus dans la révolution technique. L'impact, bon ou mauvais, qu'ils auront sur l'humanité et la société dépendra de l'utilisation qui en sera faite. À titre individuel, vous pouvez influencer sur la manière dont le big data sera utilisé, soutenir les initiatives prises pour le bien de la société et faire échec à celles qui vont à l'encontre de l'intérêt général. Par exemple, en tant que citoyen, vous pouvez voter pour des responsables politiques qui promeuvent le respect d'une éthique stricte quant à l'utilisation des données ; en tant qu'Internaute, vous pouvez privilégier des services et des entreprises qui gèrent vos données de manière responsable et respectueuse de la déontologie.
- Informez-vous régulièrement sur les évolutions du big data car elles auront de profondes répercussions sur votre vie quotidienne. Cela vous permettra non seulement de choisir les données que vous souhaitez partager, mais aussi d'identifier et de soutenir les responsables politiques et les entreprises qui partagent votre vision sur la manière dont vos données à caractère personnel devraient être traitées.
- Conservez une trace de tous les services que vous utilisez et de tout ce que vous avez publié depuis le début de votre présence en ligne, surtout si vous avez commencé jeune ! Les commentaires ou messages que vous avez mis en ligne alors que vous n'étiez qu'un enfant ou un adolescent pourraient resurgir du passé pour vous hanter dans votre vie d'adulte. Prenez le temps de revoir ce que vous avez mis en ligne et archivez ou supprimez les contenus qui ne correspondent plus à ce que vous êtes aujourd'hui.
- Étudiez avec soin la manière dont les services en ligne utilisent vos données à caractère personnel et choisissez-les en conséquence. Vérifiez toujours l'ensemble des paramètres de confidentialité disponibles pour mettre en place la bonne protection pour vos données.



INFORMATIONS COMPLÉMENTAIRES

- On trouvera sur le site web de la Commission européenne des exemples d'utilisation du big data dans l'intérêt de la société : <https://ec.europa.eu/digital-agenda/en/what-big-data-can-do-you>.
- Informations sur la réglementation européenne relative au droit à l'oubli : http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
- Data & Society est un groupe de réflexion américain qui examine les enjeux sociaux, éthiques et culturels du développement des technologies centrées sur les données : <http://www.datasociety.net/>.
- Rapport « Civil rights, big data and our algorithmic future » : <https://bigdata.fairness.io/>.

- Informations de l'Electronic Frontier Foundation sur la protection de vos droits dans le monde numérique : <<http://www.eff.org>>.
- Informations d'European Digital Rights sur la défense des droits et des libertés dans l'environnement numérique : <<http://www.edri.org>>.

Depuis la publication de la première édition du Manuel de maîtrise d'Internet en 2003, le monde en ligne a beaucoup changé. Les Internautes sont de plus en plus jeunes, leur nombre a augmenté, leurs usages d'Internet et l'objet de leurs recherches évoluent et de nouveaux dangers, par exemple en matière de sécurité individuelle, apparaissent chaque jour.

Cette nouvelle édition tient compte de ces nombreux changements mais conserve son objectif, qui est de donner aux familles, aux enseignants et aux décideurs politiques des connaissances techniques suffisantes pour pouvoir naviguer, avec les jeunes, dans le monde des technologies de la communication. La nouvelle édition étend également le contenu des Fiches d'information aux concepts qui étaient alors « nouveaux » de citoyenneté numérique et de parentalité numérique, ce qui porte le nombre de fiches à 26, organisées en six thématiques dont l'une est spécialement consacrée à l'avenir d'Internet. Le manuel se veut convivial et pratique, comme l'illustre la fiche intitulée « Trouver de l'information de qualité sur le web ». Il est également accessible en ligne où il peut être téléchargé dans son intégralité ou fiche par fiche.

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il compte 47 États membres, dont les 28 membres de l'Union européenne. Tous ont signé la Convention européenne des droits de l'homme, un traité qui vise à protéger les droits de l'homme, la démocratie et l'état de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE