

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 ?

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.

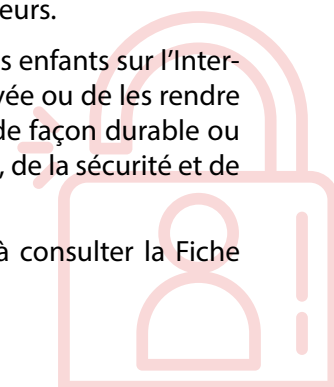
— À chaque fois que vous consultez un site web, publiez du contenu sur un média social ou envoyez un courrier électronique, vous laissez des informations vous concernant. Celles-ci peuvent inclure votre adresse physique et adresse IP, vos numéros de téléphone et de carte de crédit, votre profil de consommateur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