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 ?

Fiche d'information 8

Réseaux sociaux et partage social

Un service ou site de réseautage social[1] 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 logiciels[2] 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 social[3].

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, Vkontakte 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 Online[4], 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'indemnisation[5].

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 influer 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 idées[6].
- 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 âge[7]. 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>*.