OUTIL - DONNÉES PERSONNELLES ET IDENTITÉ NUMÉRIQUE

COMMUNICATION ET COLLABORATION > 2.6 GÉRER L'IDENTITÉ NUMÉRIQUE

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Animateurs	N/A	Niveau 1	Fiche de préparation	Creative Commons (BY-SA)	Français

Grâce à cette fiche outil l'animateur.rice se familiarise avec des concepts et notions propre aux thématiques suivantes : la citoyenneté numérique et les données personnelles. La fiche permet donc de définir de manière précise ces thématiques mais elle explique aussi comment protéger son identité numérique et ses données.

Objectif général	Connaissances
Temps de préparation pour l'animateur	moins d'une 1 heure
Domaine de compétence	2 – Communication et la collaboration en ligne
Nom de l'auteur	Samantha Giordano
Ressource originellement créée	Français

DÉROULÉ

1 Que sont les données personnelles ?

Voici la définition fournie par la Commission Nationale de l'Informatique et des libertés (Cnil) :

“ Une donnée personnelle concerne toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement ”

Ce sont par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Cependant il ne faut pas confondre données personnelles publiques qui peuvent être visibles et potentiellement revendues à un tiers (adresse mail, habitudes de consommation…) et les données personnelles privées qui bénéficient de plus de protection (numéro de carte bleue, numéro de sécurité sociale..)

2 Comment sont-elles récupérées ?

Les traces involontaires et les cookies

A chaque fois que vous vous connectez à Internet, vous laissez des traces sans vraiment le vouloir, ni même sans vous en rendre compte. Ces traces sont nombreuses et variées : votre adresse IP, votre position géographique, le système d'exploitation de votre ordinateur, toutes les adresses des sites visitées… Mais ce sont aussi des informations plus personnelles telles que vos habitudes, vos préférences vestimentaires, vos centres d'intérêt, votre langue, votre état de santé,…

Toutes ces traces permettent de mieux vous cerner et de créer un portrait de vous le plus précis possible. L'objectif est de vous offrir une expérience de navigation la plus personnalisée possible, mais surtout de permettre aux annonceurs d'adapter leurs publicités à votre profil. C'est ainsi que lorsque vous venez de faire une recherche pour trouver votre nouveau canapé, vous voyez sur certains site des publicités concernant … des canapés !

Ces données laissées involontairement sont récupérées par ce que l'on appelle des cookies. Ce sont des petits fichiers texte qui permettent de garder en mémoire des informations concernant votre ordinateur et certaines données de navigation : votre identifiant de connexion à un site ou le contenu d'un panier

d’achat par exemple.

Pour visualiser en temps réel l’ampleur des cookies qui transitent via votre navigation Internet, vous pouvez utiliser l’outil CookieViz, développé par la Cnil.

Bien que controversés ces dernières années, il faut savoir que ce ne sont pas des logiciels espions ou des virus, ils sont inoffensifs. A votre arrivée sur un site, vous pouvez paramétrer très facilement vos préférences quant à l’utilisation des cookies. Sachez que pour certains sites les cookies sont essentiels, vous ne pourrez donc pas les désactiver.

Pour en savoir plus sur les cookies, nous vous conseillons de vous référer à la page Wikipédia , dédiée qui est très bien fournie en informations.

Parmi les traces involontaires, on peut également parler des “traces héritées”. Ce sont les informations que l’on retrouve sur Internet et qui vous concernent mais que vous n’avez pas publiées vous-même. Cela peut-être par exemple, une photo postée par un ou une de vos ami.e sur les réseaux sociaux, où un article ou votre nom apparaît.

Les traces volontaires

Ce sont toutes les traces que vous choisissez de publier de votre plein grè sur Internet. Cela peut être des photos, des informations concernant votre emploi, votre site Internet, les likes sur les réseaux sociaux, les avis sur les sites marchands…

Ce sont généralement des traces qui sont visibles par d’autres personnes (pensez à votre employeur par exemple), il faut donc faire attention à ce que l’on fait. D’autant plus que ces traces sont difficilement effaçables et contrôlables

3 A quoi et à qui servent-elles ?

Les données personnelles ont de nombreuses utilités, certaines plus claires que d’autres. En premier lieu, elles servent à vous identifier en ligne via des identifiants ou des adresses mails, de passer des commandes sur des sites marchands. Mais ces données personnelles ont fait fleurir un marché très lucratif sur la Toile !

En effet, les sites et les applications qui les récoltent, peuvent les utiliser à des fins commerciales, et même les revendre, pour mieux cibler la publicité par exemple. 75% des applications que vous installez, récupèrent régulièrement vos données (contact, photos, position géographique).Contrairement à ce que l’on pourrait croire, la vente de données personnelles n’est pas illégale, dans la mesure où elles ont été

collectées dans le respect de la réglementation établie par le RGPD. Pour en savoir plus sur le Règlement Général de la Protection des Données, voici une petite vidéo qui l'explique très simplement.

N'oubliez pas… Si c'est gratuit, c'est vous le produit ! Les sites gratuits doivent trouver des moyens de se financer, la ventes de données personnelles en est un.

Outre la publicité, les données personnelles qui établissent votre comportement en ligne sont également un moyen de propagande. Cela peut être le cas par exemple de certains partis politiques qui proposent un contenu adapté en fonction de ses électeurs. Rappelez-vous le scandale Cambridge Analytica ! L'entreprise à récupéré les données personnelles de plus de 50 millions d'utilisateurs de Facebook afin d'établir des profils type et de produire du contenu adapté à chacun et peser dans la campagne présidentielle de Donald Trump.

4 Données personnelles et identité numérique : quelle différence ?

La différence entre données personnelles et identité numérique est minime dans la mesure où votre identité numérique est constituée de vos données. Mises bout à bout, ces données personnelles permettent d'établir, avec une précision variable, un portrait de qui vous êtes : ce que vous aimez, ce que vous faites, où vous habitez, qui sont vos amis, quel est votre travail… En outre, c'est l'équivalent de votre carte d'identité.

Il existe toutefois, quelques différences notables entre identité civile et identité numérique :

- vous pouvez choisir votre identité. Il n'y a pas d'obligation d'être tenu à une réalité administrative : il est possible de remplacer son nom par un pseudonyme, son adresse par un lieu paradisiaque, son visage par une version améliorée sur un logiciel de retouches… C'est notamment le cas sur les réseaux sociaux par exemple.
- vous pouvez avoir plusieurs identités. Contrairement à notre identité civile unique, sur Internet vous avez la possibilité de créer de nombreuses identités, sans restriction de nombre : un pseudo sur Facebook, un autre sur Instagram, une photo différente sur un forum de discussion…
- votre identité numérique est évolutive. Il est nécessaire de garder en tête que vos goûts, vos opinions, votre look… vont évoluer au fil des années. Cependant les traces que vous laissez,

resteront pendant de longue années. Assumerez-vous encore dans quelques années, cette photo de vous lors de ce voyage entre amis ?

Toutes les informations visibles que vous laissez et qui composent votre identité numérique contribuent donc à vous créer une e-reputation. Il s'agit de l'image que les autres perçoivent de vous, c'est pourquoi il est nécessaire de faire attention à ce que l'on poste sur Internet. L'image qu'une personne se fait de vous ne sera pas forcément la même que ce que vous aviez envisagé. D'autant plus que l'hypermnésie du Web rend les traces difficilement effaçables. Réfléchissez donc bien avant d'agir.

5 Pourquoi les protéger ?

Avant toute chose, il est nécessaire de rappeler que protéger ses données personnelles n'est pas une obligation. Cependant, nous vous conseillons d'être renseigné sur les différentes manières de le faire.

Laisser de trop nombreuses traces visibles multiplie les risques de se trouver confronté aux attaques informatiques et à l'usurpation d'identité. En effet, ces dernières années, les hackers informatiques ont élaboré de nombreuses techniques pour récupérer les informations présentes en ligne :

- Le phishing : un mail de votre banque vous invitant à vous connecter sur leur site pour récupérer vos données de carte bancaire par exemple. Il s'agit en réalité de faux site construits à l'identique pour créer l'illusion
- Le pharming : les hacker vont profiter des failles de certains sites pour récupérer les données personnelles des utilisateurs. Pas de panique, cela arrive rarement !

Votre présence en ligne vous rend également susceptible d'être la cible d'actes de cyber-harcèlement. En effet, toute personnes qui dispose de données (images, contenus, publications) peut vous nuire de différentes façons, comme par exemple :

- En usurpant votre identité. Une personne peut par exemple créer un faux profil sur les réseaux sociaux grâce à vos données pour se faire passer pour vous
- En proférant des messages haineux à votre égard. Cela peut être des messages de menaces, des insultes, des incitations à la haine ou lynchage public
- En révélant des informations personnelles. Les informations de départ peuvent être un pseudonyme, une photo, une vidéo… Mais aussi votre vraie identité, votre adresse…

6 Comment les protéger ?

Par des gestes simples

Il existe quelques petites astuces très simples et rapides à mettre en place dans votre quotidien pour protéger vos données personnelles et par extension votre identité numérique.

En voici quelques unes :

- Paramétrer votre navigateur de recherche*
- Paramétrer ses réseaux sociaux
- Paramétrer ses applications mobiles, et supprimer celles que vous n'utilisez plus
- Donner le minimum d'informations sur vous. Lorsque vous remplissez un formulaire par exemple, ne remplissez que les champs obligatoires
- Faites régulièrement des recherches sur vous. L'objectif est de vous rendre compte de ce que les autres peuvent voir de vous sur Internet.
- Créer un mot de passe sécurisé
- Réfléchir à deux fois avant de publier du contenu sur Internet.

Par la loi

Afin de protéger nos données personnelles, l'Union européenne à mis en vigueur depuis mai 2018 le Règlement Général de la protection des Données Personnelles. Un texte de référence en matière de protection de nos données numériques, et qui s'applique à tous les citoyens de l'Union Européenne. Le RGPD donne aux citoyens plus de contrôle sur leurs données personnelles via différents mécanismes comme le consentement dit "explicite" et "positif" des cookies. Il permet aussi "le droit à l'effacement ou droit à l'oubli", c'est-à-dire que toute personne qui le souhaite à le droit de demander l'effacement de données à caractère personnel (mais seulement pour motifs valables). Le RGPD est constitué de nombreux articles qui détaillent les droits des citoyens numériques et les devoir des entreprises, pour un résumé plus détaillé de ce règlement vous pouvez aller sur le site de la CNIL ou visionner cette courte vidéo ou alors celle-ci

D'autres organismes de protection des internautes se battent aussi pour mettre en place des recours juridiques pour protéger nos données et notre identité numérique.

Voici les principaux :

- Le droit d'accès. Si un organisme (banque, site internet, réseaux social…) détient des informations

sur vous, vous pouvez lui demander que celui-ci vous les communique. Ce droit permet ainsi de contrôler l'exactitude des données, et de les faire rectifier ou supprimer par la suite

- Le droit de rectification. C'est une suite du droit précédent. Si nous remarquons une information inexacte ou incomplète nous concernant, nous pouvons demander à la rectifier.
- Le droit d'opposition. Il s'agit d'avoir la possibilité de s'opposer à tout moment à ce qu'un organisme utilise certaines données pour un objectif précis. Par exemple, demander à ne plus recevoir de publicités.
- Le droit de déréférencement. Cela permet de demander aux moteurs de recherche de ne plus afficher un contenu qui nous porte préjudice. Mais attention, cela ne veut pas dire que le contenu en lui-même est supprimé.

Pour finir, sur Internet comme partout ailleurs, il est nécessaire de respecter les autres et de ne pas leur porter préjudice. N'oubliez pas que tout commentaire ou discussion laissent des traces ! Aussi, garder en tête que vous ne pouvez pas diffuser de photos, vidéo, en lien avec la vie privée de quelqu'un, ou de données à son sujet sans son consentement. C'est ce que l'on appelle le droit à l'image et le droit à la vie privée.

Pour en savoir plus au sujet des droits liés à des usages spécifiques d'Internet et particulièrement sur les droits de publication et de partage, nous vous conseillons de vous référer à la fiche outil dédiée à ce sujet.

* Vous pouvez également utiliser un navigateur tel que TOR qui permettra de protéger vos données.

7 Lexique

- **Cnil (Commission Nationale de l'Informatique et des Libertés) :** Veille à ce que l'informatique respecte les libertés, les droits, la vie privée des internautes.
- **Cookies :** Fichier contenant des informations sur nous, lors de notre visite sur un site (nom d'utilisateur, mot de passe,...).
- **Cyber-harcèlement :** Forme de harcèlement qui se déroule sur internet. Se pratique via téléphone portable, chats, jeux,... Elle peut prendre plusieurs formes, de la moquerie aux menaces, en passant par la propagation de rumeurs. **Si on est victime de harcèlement, il faut en parler à un adulte et ne pas hésiter à porter plainte !**

- **Diffamation :** C’est le fait de s’exprimer de façon injurieuse sur une personne que l’on connaît ou pas, mais qui est reconnaissable. Elle peut être raciste, homophobe ou sexiste.
- **Données personnelles :** Toutes les informations relatives à une personne, permettant de l’identifier (nom, adresse, téléphone,…). Contrairement à l’identité numérique, ce sont des données qui ne sont pas visibles par tout le monde et qui peuvent être réutilisables dans une optique commerciale.
- **Droit à l’image :** Droit qui permet à toute personne de s’opposer ou non à la diffusion de photos, de vidéos,… où elle apparaît.
- **Droit à l’oubli (numérique) :** droit qui consiste à permettre aux internautes de moins de 18 ans de demander la suppression d’informations les concernant dans un délai d’un mois maximum.
- **E-réputation (ou réputation électronique) :** C’est l’ensemble des informations disponibles sur internet concernant un internaute. Ces informations peuvent prendre plusieurs formes : commentaires, « J’aime », photos, vidéos,…
- **Historique :** Enregistrement dans un fichier ou une base de données de l’activité et des interactions d’un utilisateur sur internet.
- **Identité numérique :** Correspond aux traces que nous laissons consciemment : photos, commentaires, mais aussi les publications des autres dans lesquelles vous êtes cité, toutes les recherches auxquelles vous pouvez finalement être associé.
- **Mot de passe :** Mot d’identification pour accéder à un compte personnel. Pour plus de sécurité, il doit être composé de majuscule, de minuscule, de chiffres et de caractères spéciaux (@, !, ?,…).
- **Phishing :** Technique utilisée par les escrocs sur internet pour obtenir des informations personnelles. Ils se font passer, par exemple, pour votre banque et demandent vos coordonnées bancaires.
- **Politique de confidentialité :** Contrat qui explique comment un site traite, publie, efface les données transmises par un.e client.e.
- **Réseau social :** Site sur internet qui permet de mettre en relation des utilisateurs en ligne. Ces sites permettent de communiquer avec des amis, des groupes qui partagent les mêmes intérêts. Les plus connus sont Facebook, Twitter et WhatsApp.
- **Trace numérique :** Informations enregistrées sur l’activité ou l’identité d’un.e internaute.
- **Transparence :** Fait d’utiliser des termes simples et clairs pour permettre la bonne

compréhension d'une règle. Il encadre également le fait de tenir au courant l'internaute en cas de modification du leur règlement.

- **Usurpation d'identité :** Fait de voler l'identité numérique de quelqu'un.e pour faire des achats ou arnaquer d'autres personnes.
- **Vie privée :** Ensemble des activités d'une personne qui concerne son intimité, sa vie familiale, sa santé,... et qu'elle ne souhaite pas divulguer.
- **Vie virtuelle :** Vie que nous nous créons dans le monde du numérique (jeux vidéo en ligne, réseaux sociaux,...).