Identité numérique et sécurité des données sur internet

Des outils et des bonnes pratiques

Une vidéo courte pour commencer : https://www.youtube.com/watch?v=wShQYeH9qJk
Accédez à la vidéo sur YouTube : Datagueule « privés de vie privée ».

1-Définition de l'identité numérique

L'identité numérique (IN) est l'image qu'on peut se faire d'une personne, d'un groupe, d'une organisation, ou d'une entité x (par exemple, un quartier) à partir de l'information numérisée qui existe à son sujet.
L'IN est constituée des publications, des traces que nous laissons de notre passage sur internet (ou que les autres laissent pour nous) volontairement ou non.

Le droit à l'oubli existe même s'il peine à se mettre en place, c'est lié à la difficulté de « contrôler » internet. Pour les mineurs une disposition va être peut-être mise en place avec le projet de loi sur le numérique. L'information que nous déposons sur internet est encore très difficile à « effacer ». Le réseau garde la mémoire de toutes les activités passées.

2-Quels sont les enjeux ?

Internet donne à toutes les personnes qui disposent des moyens techniques suffisants de relier ces différentes traces et de dresser un profil.

Pourquoi ?

- La publicité comportementale ciblée : via les cookies actifs qui sont placés dans votre navigateur lors de votre navigation. Le modèle économique de nombreuses sociétés est basé sur la fourniture de service apparemment « gratuits » mais financés majoritairement par la publicité. C'est devenu une norme, si bien que pour la plupart des services en ligne l'internaute reçoit une quantité croissante de publicité.

Cookies : Les cookies sont des petits fichiers texte stockés dans votre navigateur web ou votre client de messagerie. **Ils sont placés sur votre appareil par des sites que vous visitez ou des publicités que vous consultez en surfant**. Dans certains cas, les cookies sont nécessaires, par exemple pour la connexion à certains comptes en ligne. Les dits cookies tiers permettent aux réseaux publicitaires de suivre l'activité de votre navigateur sur divers sites, même indépendants les uns des autres[1].

Vous pouvez refuser les cookies sur les pages internet ou les effacer. A savoir que dans certains cas, le fait de garder les cookies peut améliorer votre navigation, le tri des cookies peut se faire au cas par cas, selon vos besoins.

Dans Mozilla : Outils > Options > Vie privée > Supprimer des cookies spécifiques. Vous pouvez sélectionner les cookies que vous souhaitez faire disparaître de votre navigateur.

- Contrôler ses cookies : http://www.youronlinechoices.com/fr/controler-ses-cookies/
  Accédez au site via un moteur de recherche et taper « youronlinechoices »

- **La récolte d'adresse mail** à des fins de diffusion massive de publicité.

- **L'établissement de profils** dans le big data qui permettent de dresser des tendances grâce aux données échangées : ce qui se vend, s'achète, se visite, se mange, se dit, etc.

Big data : Les big data, littéralement les « grosses données », ou mégadonnées, parfois appelées données massives, désignent des ensembles de données qui deviennent tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information. Actuellement, ces données sont stockées sans être toutes exploitées vu le volume important de données.

= Enjeu économique majeur de ces prochaines années.

Gérer son identité numérique demande d'entrer un peu dans la « technique », ce n'est pas forcément très intuitif pour l'internaute non-initié.

NB : la dés-appropriation du monde numérique par ses utilisateurs (des milliards!), nous consommons une technologie sans vraiment la maîtriser.

L'usage qui peut être fait de ces données peut aller à **l'encontre des libertés fondamentales** des individus, **la CNIL** est un organisme de protection qui tente de réguler l'activité numérique et œuvre pour la protection des droits des citoyens internautes : la loi informatique et liberté au titre du droit au respect de la vie privée. Par la CNIL l'État est garant des libertés individuelles sur internet. Mais chaque internaute doit être responsable de sa navigation.

- *Sur internet, visitez le site de la CNIL : http://www.cnil.fr/vos-droits/vos-traces/*

3-Quelles traces laissons-nous ?

Il peut s'agir des traces de notre navigation sur les sites, web, les historiques d'achats, des photos (postées par vous ou non), les commentaires laissés sur les blogs, les réseaux sociaux, etc. Ces traces définissent notre identité numérique, nous les contrôlons plus ou moins efficacement.

Il existe différents types de traces :

- Les traces techniques que nous laissons à chaque connexion et qui sont liées à l'utilisation du navigateur / du matériel.
- Les traces dites d'usages qui sont laissées plus ou moins volontairement lors de la création d'un compte sur un service en ligne, lorsque l'on dépose des photos, des commentaires, effectue un achat.

Ces données peuvent être de **nature administratives** (votre numéro de téléphone, numéro de sécu, code bancaire, etc. ou de **nature personnelle**, c'est à dire pouvant révéler votre personnalité (à travers vos achats, vos goûts, etc.).

4-Peut-on vraiment protéger sa vie privée sur internet ? Les lieux de fabrication de l'identité numérique.

Il faut savoir que dès l'instant que vous achetez un appareil ou que vous vous connectez sur internet, vous êtes déjà repérable et « traçable ». Cela ne veut pas dire que l'on connaît tout de vous, mais vous possédez une identité et vous laissez des traces. Nous ne pouvons pas totalement protéger notre vie privée (Internet est une sphère publique) mais il est important de connaitre les bonnes pratiques et d'agir avec bon sens, comme dans la vie réelle.

Exemple de données « traçables » :

Le numéro de série de l'ordinateur : qui sert à identifier un ordinateur.
L'adresse IP : Votre adresse IP est un numéro unique attribué à votre routeur ou modem par votre fournisseur d'accès à Internet. Elle peut être vue par tous les sites et tous les serveurs auxquels votre ordinateur se connecte. De ce fait, une adresse IP identifie le réseau local que vous utilisez et, combinée avec d'autres traces, comme par exemple le logiciel de navigation que vous utilisez ou vos renseignements de facturation, elle peut vous identifier personnellement.
La connexion Internet auprès d'un fournisseur d'accès à Internet : le FAI doit conserver (sur une période d'un an) les traces de vos connexions à Internet au regard de la législation et possède donc des informations nominatives vous concernant.
La participation à des blogs, wiki, réseaux sociaux ou le partage de contenus via des sites tels que Flickr, YouTube, Deezer, permettent de mieux connaître vos goûts, opinions et centres d'intérêts.
Attention aux « amis » : Les propos tenus par d'autres personnes à votre sujet sur le réseau constituent également votre identité numérique.

5-Quels sont les moyens de sécuriser ses données ? Des outils et des bonnes pratiques.

- **Tracez votre ombre :** https://myshadow.org/fr/trace-my-shadow
  Sur internet, via un moteur de recherche, tapez « tracer mon ombre »

Le site « Tracer mon ombre numérique » propose de découvrir les « ombres numériques » utilisées au quotidien (traces laissées en ligne) et fournit les moyens de changer et/ou réduire les informations et données confidentielles déposées en ligne.
Sur la page, il suffit de cocher les appareils que vous utilisez pour vous connecter à Internet (ordinateur, appareils mobiles) et les usages (accès à Internet, services en ligne) et ensuite de « cliquer pour investiguer ». Les traces laissées en ligne sont alors comptabilisées, analysées avec des explicitations formelles et des conseils.

- I**nstaller et utiliser le logiciel CCleaner** : http://fr.ccleaner-soft.com/

C'est un logiciel gratuit et en français complémentaire de votre antivirus, qui permet de nettoyer votre ordinateur en supprimant les fichiers inutiles, il vous aide aussi à préserver votre vie privé en supprimant les traces laissées pendant vos surfs sur Internet et vos documents récemment ouverts.
D'un coup, il supprime les fichiers temporaires, l'historique de navigation, les cookies, etc. Double avantage de nettoyer vos traces et de ne pas affaiblir inutilement votre appareil, fonctionne sur les ordinateurs et les tablettes Android, iPad.

- **Vider le cache Internet = supprimer l'historique récent** : il accapare de la place sur le disque dur au fur et à mesure de vos passages sur le web. Pour ne pas arriver à saturation de cet espace, vous devez vider ce cache, le supprimer. Par cache Internet, on entend l'ensemble des fichiers constituant une page Internet et l'ensemble des cookies enregistrées sur le disque par le navigateur.

Dans les modules complémentaires des navigateurs, il est possible d'installer **AdBlock Plus** ou **Ublock** qui bloquent les publicités.

- **Sur Google, désactivez les annonces ciblées** :
  https://www.google.com/settings/u/0/ads/authenticated?hl=fr#general

Connectez-vous sur votre compte gmail puis ouvrez un nouvel onglet et copiez/collez l'adresse ci-dessus. Vous accédez à une page qui vous permettra de désactiver les annonces ciblées.

Et il existe des alternatives :

Les moteurs de recherche, il n'y a pas que Google : https://duckduckgo.com/ (duckduckgo) ou https://ixquick.fr/fra/ (ixquick) rendent le même service en toute confidentialité.

Les logiciels libres : Face aux grands éditeurs dits « propriétaires » (Microsoft, Apple, Adobe…), depuis plus de trente ans, nombreux sont ceux qui ont fait l'effort de mettre au

point des logiciels dits « libres » sur des fondements de partage de la connaissance et du respect des libertés. Ces logiciels garantissent à l'utilisateur l'usage de standards et de grandes libertés d'utilisation, d'étude, de redistribution et d'amélioration du programme. Cela permet notamment d'auditer le code et limiter des possibilités malicieuses (portes dérobées, contrôle par un éditeur commercial…). En conséquence, la « communauté » exerce un fort contrôle sur ces logiciels. Dans une société où l'informatique est omniprésente, la maîtrise de nos outils est un enjeu majeur. Ce combat est aussi mené par les défenseurs du logiciel libres.

6-Sur les réseaux sociaux : l'exemple de Facebook

Quelques règles à suivre pour une utilisation sécurisée. Le guide de BitDefender formalise des règles à suivre pour la configuration générale et une utilisation sécurisée des réseaux sociaux :

Politique du mot de passe

– Utilisez un mot de passe solide pour les comptes sur réseaux sociaux : 12 caractères en mélangeant majuscules et minuscules (sans utiliser de noms usuels ni de marque).
– Ne conservez pas le mot de passe dans le navigateur d'un appareil portable de manière à ce que, en cas de vol, l'appareil en question ne puisse permettre un accès non autorisé au compte de votre réseau social.

Supprimez les cookies après déconnexion

– Il est conseillé de supprimer les cookies si vous souhaitez naviguer en toute sécurité.
– Une manière plus cohérente de protéger son intimité est d'utiliser la fonction « Effacer les données de navigation » de navigateurs comme Google Chrome ou Mozilla Firefox, qui suppriment les cookies quand vous avez fermé le navigateur.

Utilisez des connexions cryptées

– Naviguez toujours sur le réseau social au moyen d'une connexion sécurisée (le préfixe « https » dans le navigateur).

Activez toutes les notifications de connexion

– Facebook vous permet de recevoir des notifications par e-mail ou SMS à chaque fois que quelqu'un se connecte à votre compte à partir d'un nouvel appareil. Ceci aide à déceler plus rapidement toute activité suspecte qui peut s'exercer sur votre compte..

Sélectionnez avec discernement quelles informations vous publiez

– Il est difficile de supprimer complètement une information une fois qu'elle a été publiée en ligne.
– Sur le web, des robots analysent en permanence le contenu mis en ligne et le multiplient de façon incontrôlable.
– Avant de poster un contenu en ligne, évaluez attentivement ses conséquences éventuelles en termes de légalité ou de réputation.

E-reputation : L'e-réputation est l'impression que produisent les informations disponibles sur Internet vous concernant. Ces informations peuvent prendre différentes formes: commentaires, articles, photos, vidéos, etc. Votre e-réputation peut donc vous aider dans la vie en vous rendant par exemple plus visible pour un recruteur mais aussi vous gêner si vous laissez traîner des informations compromettantes.

Mais aussi :

Vérifier régulièrement le niveau d'exposition de son compte profil Facebook via le menu *« contrôler la confidentialité que de ce que vous publiez »*.

Pour conclure, sans devenir paranoïaque …[1]

- **Protéger son mot de passe** et le changer régulièrement. Choisir un mot de passe qui ne se devine pas facilement et ne pas l'enregistrer sur les ordinateurs publics.
- **Ne jamais afficher de données personnelles** comme un numéro de téléphone, adresse personnelle et date de naissance. Faire particulièrement attention au numéro d'assurance sociale. Le vol d'identité est un problème grandissant.
- **Protéger votre adresse courriel**. Ne pas utiliser son adresse habituelle pour les abonnements, achats en ligne, messages sur des forums... créer une adresse de courriel pour ces pratiques.
- **Etre discret**. Rappelez-vous que ce que vous affichez demeure en ligne en permanence ; nous n'aurons jamais un contrôle total des informations déposées sur Internet.
- **Se poser les mêmes questions que celles que vous vous poseriez dans la « vraie vie »** Choisir ses amis, se donner le droit d'en refuser, faire la différence entre un ami Facebook et un ami dans la vie réelle.
- **Garder la maîtrise des informations** publiées sur internet : la meilleure façon de se protéger c'est de faire attention à ce que l'on publie. Vous êtes responsables des photos, vidéos et commentaires publiés
- **Faire preuve d'une grande vigilance** lors d'une inscription sur un réseau social : donner le moins d'informations possibles ou ne dire que le strict nécessaire. Utiliser des pseudos et des adresses « poubelles ».
- **Sécuriser son compte** sur les réseaux sociaux en apprenant à paramétrer son profil.

Enfin, pour aller plus loin vous pouvez consulter le site Netpublic, **une mine d'or concernant les usages d'internet (avec des guides, des vidéos, des ressources dans des domaines variés).**

[1] Espace Multimédia de Rocheservière