A la découverte d'un réseau social numérique : Babelio

Objectifs:

Domaine 3, La formation de la personne et du citoyen : Se construire une identité numérique positive (respecter les autres/se protéger)

Domaine 4, Systèmes naturels et systèmes techniques : Comprendre le fonctionnement des réseaux sociaux numériques à travers l'usage de Babelio

Séance 2 : Données personnelles, traces et identité numériques

Quel est le problème avec les données personnelles ?

A l'aide du document P. 3 répond aux questions suivantes :

Comment qualifierais-tu la quantité d'informations concernant Max Schrems connues par le réseau social Facebook : _____

Comment le réseau social Facebook qualifie-t-il ses utilisateurs et au vu de l'ensemble de la planche de BD, explique pourquoi ?

_____

Que peut savoir sur nous un réseau social en croisant nos profils et les informations collectées au gré de notre navigation sur le web ?

_____

_____

_____

Que font les réseaux sociaux avec nos données ?

_____

_____

_____

Le problème de l'identité numérique :

A l'aide du document P. 4 répond aux questions suivantes :

1. Quel est le slogan qui résume les intentions commerciales des outils numériques proposés par les GAFAM ? _____

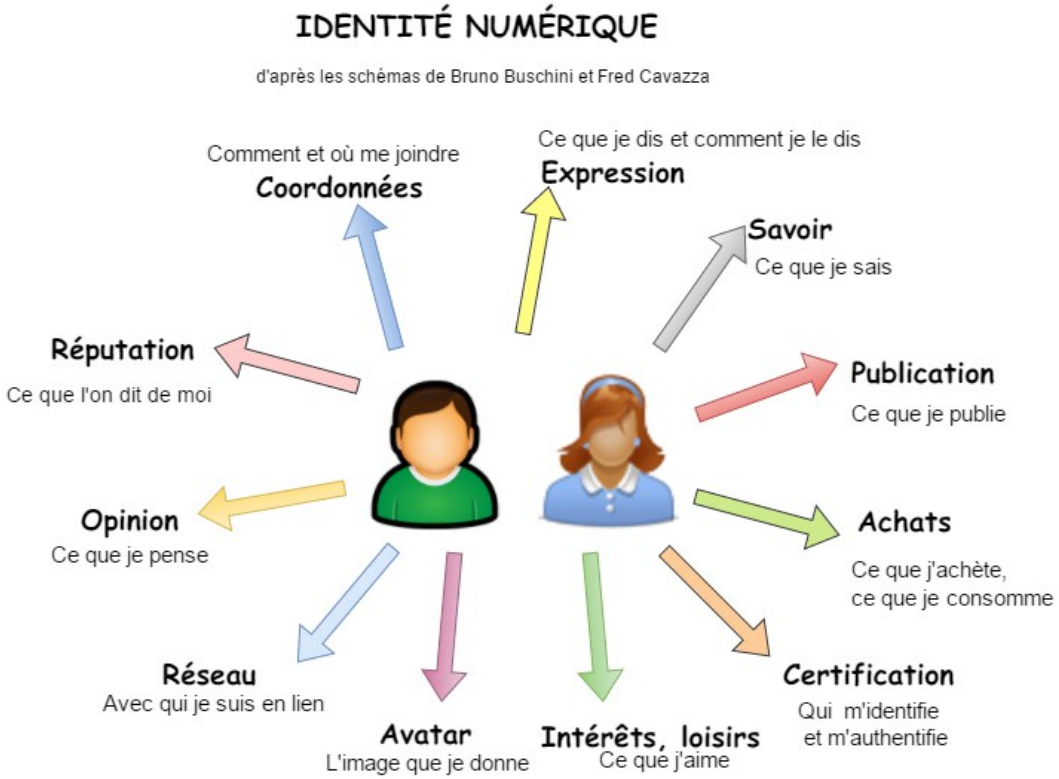
2. En plus de notre identité légales, de nos données personnelles auxquelles on doit faire attention, qu'est ce qui est aussi « tracé » pour obtenir des informations nous concernant ?

_____

_____

3. Que peut-on faire, selon l'auteur de l'article pour se protéger ? 3 choses :

_____



Identité numérique :

ensemble des informations nous concernant qui circulent sur le web

≠ identité légale ,

≠ données personnelles

Source : Groom, 2 : méga Spirou Hors-Série. *Réseaux sociaux : addictions, révolutions, chatons*. Septembre 2016. P. 90

Source : Groom, 2 : méga Spirou Hors-Série. *Réseaux sociaux : addictions, révolutions, chatons*. Septembre 2016. P. 84

OBJECTIF :

LE 1/4 D'HEURE D'ANONYMAT !

On utilise beaucoup les réseaux sociaux. Mais eux nous utilisent aussi un peu... Jean-Marc Manach, notre spécialiste du Web, nous explique comment nous sommes surveillés et comment nous protéger.

« Dans le futur, chacun aura droit à 15 minutes de célébrité mondiale », avait prophétisé le pop artiste américain Andy Warhol, en 1968. Bon, ça, c'est fait, grâce à la téléréalité et à YouTube. Le problème, aujourd'hui, ce serait plutôt d'« avoir droit à son 1/4 d'heure d'anonymat »... Parce que si les postes de télévision ne vous regardent pas (ou pas encore : les premiers postes TV espionnant leurs téléspectateurs commencent à être commercialisés), tout ce que l'on fait sur le Web est surveillé, et analysé.

84 Vous croyez que Facebook est un réseau social et Google, un moteur de recherche ? #LOL : « Si c'est gratuit, c'est que vous êtes le produit ! » Il s'agit en fait de régies publicitaires qui, en échange de services « gratuits », collectent vos données personnelles pour alimenter de gigantesques bases de données de « profils » de consommateurs, afin de monnayer votre « temps de cerveau disponible » à des annonceurs.

C'est ainsi que Target (« cible », en VO), une chaîne de grands magasins US, avait envoyé des publicités vantant des habits de bébé et des couches à une jeune fille de 16 ans. Colère du papa, en mode « Vous voulez la pousser à tomber enceinte ? »... Sauf que Target avait raison : les recherches internet de la jeune fille avaient permis à l'enseigne d'identifier qu'elle était enceinte, ce qu'elle n'avait pas encore annoncé à son papa. Nous partageons tellement d'informations en ligne que ceux qui nous y surveillent en savent généralement bien plus sur nous que nos propres parents...

Si l'informatique laisse des traces, il est cela dit possible de maquiller son identité, ou d'avancer masqué. On peut ainsi ouvrir une fenêtre de navigation privée dans son navigateur, afin de ne pas laisser de traces des sites visités dans son historique. Mieux : le navigateur TOR utilise un réseau sécurisé parallèle permettant de naviguer de façon anonyme. Depuis les révélations d'Edward Snowden sur la « surveillance de masse » pratiquée par la NSA (les « grandes oreilles » espionnes des USA), son utilisation a explosé et de nombreux services web ont décidé de protéger la vie privée de leurs utilisateurs. Ainsi, plus de 80 % des requêtes Google sont désormais chiffrées : elles peuvent certes être déchiffrées sur les serveurs de Google, mais elles ne circulent plus « en clair », comme c'était le cas auparavant.

Encore mieux : recommandée par Snowden, l'application Signal d'Open Whisper Systems permet d'échanger des SMS (et même des appels téléphoniques) qui, chiffrés sur votre téléphone (et déchiffrés sur celui de votre interlocuteur), ne transitent plus « en clair » sur les réseaux. Quand bien même ils seraient interceptés, ils resteraient donc indéchiffrables... En avril 2016, WhatsApp, la plus populaire des messageries, rachetée par Facebook en 2014, a elle aussi déployé cette solution de chiffrement.

Enfin, dernier point : ce n'est pas parce que vous avez fermé votre profil Facebook que les publications s'autodétruisent et ce n'est pas parce que vos parents n'utilisent pas WhatsApp que vous pouvez y dire ou faire n'importe quoi : sur un réseau social, ce que vous partagez devient public, vos amis peuvent le copier/coller ou en faire des captures d'écran. Quand on prend la parole en public, que ce soit sur les réseaux sociaux ou dans la vraie vie, il faut pouvoir l'assumer !

Jean-Marc Manach (@manhack)