FICHE PÉDAGOGIQUE

Souriez, vous êtes fichés

COLLÈGE – LYCÉE

Naviguer sur le web, c'est aussi laisser des traces, volontaires ou involontaires, qui ensemble constituent une identité numérique. Sans paranoïa, prendre conscience de ce phénomène et apprendre à gérer ces traces permet de protéger sa vie privée.

OBJECTIFS

> Réfléchir aux notions de vie privée et de données personnelles.
> Distinguer les traces volontaires et involontaires laissées sur le web.
> Réfléchir au modèle économique qu'implique le fichage.
> Connaître des techniques pour maîtriser ses traces numériques.
> Mieux comprendre le « I » de EMI (l'information comme document ou donnée) et voir en quoi les médias et la publication en ligne des élèves y sont associés.

PUBLIC

> Collège, lycée.

RESSOURCES

> Le site de la Commission Nationale de l'Informatique et des Libertés, l'autorité indépendante chargée des données personnelles : **www.cnil.fr**
> Le site de la série webdocumentaire interactive d'Arte sur le fichage avec de nombreux liens vers des ressources documentaires : **https://donottrack-doc.com**

DÉROULEMENT

1. Mes données sont-elles protégées par la loi ?

■ Mettre les élèves par groupes et leur demander de lister quelles informations les concernant relèvent de la vie privée et lesquelles sont des données personnelles. Distinguer les données personnelles (des « informations relatives à une personne physique identifiée, directement ou indirectement », protégées par la Loi Informatique et Liberté de 1978, article 2) et les informations relatives à la vie privée, notion floue, que l'on peut définir comme une intimité qu'on ne veut pas divulguer, par opposition à la vie publique.
■ Conclure que ces informations se recoupent souvent et que le législateur reconnaît leur valeur en les protégeant contre le vol.

2. « Si c'est gratuit, c'est toi le produit ! »

■ Demander aux élèves quels sont les sites web qu'ils utilisent le plus, et parmi ceux-ci, lesquels sont payants.
■ Chercher sur le web les bénéfices d'un réseau social (entreprise dont la source de revenus principale est la revente de données personnelles) sur une année. Conclure que quand un site propose un service gratuit, la valeur ajoutée est constituée par les données personnelles récupérées et revendues.

3. Comment sont recueillies mes traces ?

■ Demander aux élèves de lister les objets ou les dispositifs qui permettent de recueillir leurs données personnelles. Les classer : traces laissées devant l'écran (navigation, publication volontaire de données), objets connectés (bracelets, cartes bancaires, de fidélité, téléphone géolocalisés), reconnaissance faciale, informations données par autrui sur le web…
■ Projeter un historique de navigation anonymisé et demander aux élèves d'imaginer le profil de l'internaute. Réfléchir à qui pourrait être intéressé par ces informations (entreprises, organisations) et dans quel but (commercial, politique, sociologique).

Quelques outils simples et efficaces rendent visibles nos traces : un moteur de recherche sur les personnes (**http://webmii.com**), des logiciels ou des modules complémentaires du navigateur Firefox pour visualiser les échanges entre des contacts d'une boîte mail (**http://immersion.media.mit.edu**), les trackers ou autres « acteurs » qui suivent l'internaute (Collusion, lightbeam et cookieviz de la CNIL), un logiciel qui bloque des « mouchards », appelés « cookies » en anglais (Gostery).
■ Conclure avec les élèves sur la puissance du fichage :
– Il est presque invisible : les utilisateurs s'en protègent peu et livrent beaucoup de petites informations.
– Celles-ci s'accumulent au fil du temps et permettent l'élaboration d'un profil finalement détaillé de chacun.
– Une fois captées, elles peuvent difficilement être effacées : le processus est réputé irréversible pour les usagers.

4. Comment protéger mes données personnelles ?

■ Initier avec les élèves un remue-méninges : par quels moyens peut-on éviter le fichage ?
Quelques solutions possibles :
Utiliser un pseudo, une fausse identité, un moteur de recherche alternatif (Qwant, Duckduckgo) ou plusieurs en ajustant différemment les paramètres de sécurité selon l'usage, ne jamais remplir de formulaire commercial en ligne, ne pas y livrer toute la vérité, ne pas y remplir les champs optionnels, bloquer les mouchards ou cookies dans son navigateur, refuser la géolocalisation, vérifier les paramètres de confidentialité de son profil sur les réseaux sociaux, ne jamais aller sur internet, de peur de laisser des traces.
■ Demander à chacun quelle stratégie parmi celles-ci lui paraît la moins contraignante et la plus efficace, et s'il est prêt à l'adopter pour protéger ses données personnelles.