

Récolte des données personnelles sur Internet et les réseaux sociaux

Thème	Récolte des données personnelles sur Internet et les réseaux sociaux
Degrés	9 ^e -10 ^e -11 ^e
Durée indicative	45 minutes
Objectif	<p>Cet atelier a pour but de permettre aux élèves de</p> <ul style="list-style-type: none"> - Comprendre la manière dont les données personnelles sont récoltées sur Internet et les réseaux sociaux - Mettre en place des bonnes pratiques pour protéger leurs données
Liens PER	<p>CT - La capacité à développer une démarche réflexive permet de prendre du recul sur les faits et les informations, tout autant que sur ses propres actions ; elle contribue au développement du sens critique.</p> <p>PER EN 22 - S'approprier les concepts de base de la science informatique Sensibilisation aux enjeux de la collecte et l'exploitation des données personnelles et des traces numériques</p> <p>PER EN 23 - Utiliser des outils numériques pour réaliser des projets Découverte de la notion d'identité et d'empreinte numériques</p> <p>PER EN 31 - Analyser et évaluer des contenus médiatiques en étudiant l'influence des outils numériques et des médias sur notre société</p> <p>PER EN 32 - Poser et résoudre des problèmes en science informatique Analyse des processus derrière la collecte et l'exploitation des données personnelles et réflexion sur leurs enjeux politiques, économiques et médiatiques</p> <p>PER EN 33 - Exploiter des outils numériques pour collecter l'information, pour échanger et pour réaliser des projets Analyse de certains usages du numérique, opportuns ou à risques, de leur impact sur l'identité numérique</p>
Matériel	<ul style="list-style-type: none"> - Beamer - Accès Internet - Vidéo « Récolte des données – Algorithme et cookie » :

	<p>https://www.actioninnocence.org/wp-content/uploads/2021/09/Re%CC%81colte_des_donne%CC%81es.mp4</p> <ul style="list-style-type: none"> - Site pour le jeu CheeseMaster : https://www.cheesemaster.ch/ - Site pour le Quizz addict : www.quiz-addict.ch
<p>Déroulement</p>	<ol style="list-style-type: none"> 1. Pour démarrer l'activité, les élèves visionnent la capsule vidéo « Récolte des données - Algorithme et cookie ». La vidéo est un levier de discussion pour les inviter à débattre de leurs pratiques numériques en se basant sur leurs expériences. 2. Les élèves jouent ensuite à Cheesemaster une activité en ligne leur permettant de prendre conscience des données récoltées à leur insu et d'en discuter avec leurs camarades. 3. Lors de la troisième étape, les élèves sont réparti·e·s en petits groupes et répondent à la question « Comment pouvons-nous laisser moins de traces sur Internet et les réseaux sociaux ? » en s'appuyant sur leurs expériences. Les propositions de chaque groupe sont partagées à l'ensemble de la classe. 4. Pour terminer l'activité, les élèves répondent au quizz « Internet te piste ! » sur le site quiz-addict.ch pour évaluer leurs connaissances.
<p>Étape 1</p>	<p>Visionner la capsule vidéo « Récolte des données - Algorithme et cookie »</p> <p>Accès à la vidéo sur le site : https://www.actioninnocence.org/wp-content/uploads/2021/09/Re%CC%81colte_des_donne%CC%81es.mp4</p> <p>Cette vidéo vise à mieux comprendre la récolte des données personnelles sur Internet et les réseaux sociaux ainsi que la notion d'empreinte numérique. Il s'agit de questionner les élèves quant à leurs pratiques, de se baser sur leurs expériences dans une attitude de non-jugement.</p> <p>Questions de relance et de mise en débat à la fin du visionnement :</p> <p>Qu'avez-vous découvert avec cette vidéo ? Que saviez-vous déjà ?</p> <ul style="list-style-type: none"> • En écoutant les avis et les commentaires des élèves, il est possible d'identifier leurs compétences, leurs connaissances et leurs représentations.

Qu'est-ce que l'empreinte numérique ?

Il s'agit de l'ensemble des traces numériques que nous laissons sur Internet et les réseaux sociaux. En voici des exemples :

- Les données personnelles que nous avons transmises (âge, nom et prénom, pseudonymes, adresse email, numéro de téléphone, adresse, etc.)
- Nos recherches (historique de navigation, mots-clés utilisés lors des recherches, etc.)
- Nos publications (photos, vidéos, commentaires, etc.)
- Nos réactions (likes, commentaires, partages de contenu, etc.)
- Les personnes à qui nous sommes abonné-e-s sur les réseaux sociaux
- Le temps que nous passons sur certaines pages ou certains contenus
- Nos heures de connexion (durée et moments de la journée)
- Les réglages de nos appareils (localisation, connexion wifi, accès au micro, accès aux contacts, langues utilisées, type d'appareil utilisé, etc.)

Pour plus de détails, voir la définition d'empreinte numérique dans le lexique p.7

Sur notre fil d'actualité sur les réseaux sociaux ou lorsque nous effectuons une recherche sur Internet, avons-nous toutes et tous les mêmes propositions ?

Non car :

- L'accès au réseau Internet et aux contenus est différent selon les régions et les pays.
- Les contenus qui nous sont proposés dépendent de notre empreinte numérique (cf. lexique p.7)

Quels sont les avantages de laisser des traces sur Internet ?

- Cela nous permet de trouver facilement et rapidement des informations et des produits qui correspondent à nos intérêts et nos goûts.

Quels sont les inconvénients de laisser des traces sur Internet ?

- Toutes nos traces sont récoltées, stockées et analysées pour permettre aux fournisseurs de contenus d'établir un profil basé sur nos goûts, nos intérêts, nos activités, notre situation familiale, le milieu social dans lequel nous évoluons et bien d'autres informations qu'ils peuvent utiliser pour influencer nos choix et nos comportements, notamment à travers la publicité.

Quels sont les inconvénients liés à la collecte de nos données, à leur conservation et analyse ?

- Les services et plateformes qui stockent nos données peuvent se faire pirater. Des pirates (hackers) peuvent alors accéder à nos données et tenter de nous arnaquer en les utilisant. Par exemple, le mot de passe de l'un de nos réseaux sociaux devient accessible. Un pirate le change et nous sommes victimes de chantage pour récupérer l'accès à notre compte.
- Ce qui nous est proposé sur Internet et les réseaux sociaux est avant tout le fruit de l'analyse de nos données. Nous sommes pris dans une « bulle de filtres » (cf. lexique p.6), nous ne voyons qu'une partie infime de ce que nous pourrions trouver sur Internet. Par exemple, lorsque nous publions ou likons des contenus liés à une mouvance politique, les plateformes en ligne vont nous proposer de l'information propre à cette mouvance et réduire l'accès à des opinions contraires qui pourraient nous faire réfléchir.

Connaissez-vous le terme « bulle de filtres » (cf. lexique p.7) ?

Pensez-vous que nos appareils nous espionnent ?

- Selon les conditions générales d'utilisation (CGU) que nous avons tendance à accepter sans les lire, nous donnons accès à de nombreuses informations personnelles. Nous acceptons qu'elles soient récoltées, stockées, analysées et potentiellement revendues/mises à disposition de tiers. Par exemple, selon les CGU de Snapchat : nous accordons à ce fournisseur une licence mondiale et irrévocable, sans contrepartie, d'héberger, stocker, utiliser, afficher, reproduire, modifier, adapter, éditer, publier, analyser, transmettre et distribuer nos contenus privés ou publics à des fins commerciales ou non. Notre photo pourrait ainsi être modifiée et être utilisée pour faire de la promotion pour un produit n'importe où dans le monde.
Source : <https://snap.com/fr-FR/terms>
- Pour utiliser les réseaux sociaux, nous autorisons l'accès à notre micro et notre caméra. Techniquement, les réseaux sociaux pourraient alors les employer pour nous espionner mais ils n'ont pas le droit de le faire. Nous ne pouvons qu'espérer qu'ils respectent la loi.
- Nos données récoltées sont nombreuses et si finement analysées que les réseaux sociaux arrivent à dresser un portrait précis basé sur l'ensemble des attributs qui pourraient nous définir (nos goûts, nos intérêts, nos activités, notre situation sociale et familiale, etc.) et à anticiper certains de nos besoins sans avoir à nous filmer ou à nous écouter à notre insu.

<p>Étape 2</p>	<p>Jouer à Cheesemaster</p> <p>Accès au jeu sur le site : https://www.cheesemaster.ch/</p> <p>Cette activité développée par la RTS permet de prendre conscience en quelques minutes des données récoltées à notre insu.</p> <ul style="list-style-type: none"> • Que pouvons-nous dire des résultats ? • Sommes-nous surpris ?
<p>Étape 3</p>	<p>Réfléchir à des pistes d'action pour laisser le moins de traces possibles</p> <p>En petits groupes, les élèves répondent à la question ci-dessous et présentent leurs idées à l'ensemble de la classe. Il s'agit de s'appuyer sur les connaissances des élèves, leurs expériences.</p> <p>Comment pouvons-nous laisser moins de traces sur Internet et les réseaux sociaux ?</p> <p>Les éléments de réponse suivants sont des exemples pour étayer les propos des élèves :</p> <ul style="list-style-type: none"> • Désactiver la localisation permanente Toutes les applications doivent demander notre accord pour avoir accès à notre localisation. Celle-ci peut être activée en permanence ou uniquement quand l'application est utilisée. • Prendre le temps de refuser les cookies Tous les sites Internet que nous visitons nous demandent d'autoriser l'utilisation de cookies (cf. lexique p.6). Bien souvent, nous ne prenons pas le temps de vérifier dans quel but ils sont utilisés et nous les acceptons sans nous informer. Nous pouvons cependant en désactiver certains (par exemple, ceux employés pour la publicité ciblée). • Limiter la publication des informations personnelles qui permettent de nous identifier (nom et prénom, adresse, date de naissance, numéro de téléphone, etc.) • Utiliser une navigation privée (cf. lexique p.8) • Choisir son navigateur Les navigateurs récoltent les données de manières différentes selon leurs conditions générales d'utilisation. Il est utile de prendre le temps de lire un comparatif sur la manière dont chacun traite nos données. De nombreux comparatifs sont disponibles en ligne.

	<ul style="list-style-type: none"> • Une solution plus technique est d'installer un VPN (cf. lexique p.8)
Étape 4	<p>Répondre au quiz « Internet te piste ! » de REPER</p> <p>Ce quiz a pour but d'évaluer les connaissances des élèves au terme de l'atelier.</p> <p>Pour y accéder, se rendre sur le site www.quiz-addict.ch. Dans la catégorie « ECRANS », choisir « Internet te piste ! ».</p> <p>Si vous souhaitez faire le quiz en groupe, choisir la fonctionnalité en haut de la page à droite.</p>
Messages à transmettre aux élèves	<ul style="list-style-type: none"> • Les services et plateformes en ligne gardent en mémoire et analysent ce que nous faisons. • Ils nous proposent des contenus selon nos goûts et centres d'intérêts, ce qui restreint l'accès aux informations qui nous sont présentées. • Nous pouvons réduire les traces numériques que nous laissons sur Internet.
Ressources	<ul style="list-style-type: none"> • Send_it - Boîte à outils pour faire face aux risques des médias sociaux et du cyberharcèlement : https://sendit.up-to-you.ch/fr/boite-a-outils • Site CIAO – Comment les réseaux sociaux gagnent de l'argent : https://www.ciao.ch/articles/comment-les-reseaux-sociaux-gagnent-de-largent/ • Site Jeunes et médias – Surfer en protégeant ses données personnelles et sa sphère privée : https://www.jeunesetmedias.ch/themes/surfer-en-protectant-ses-donnees-et-sa-sphere-privee
Lexique	<ol style="list-style-type: none"> 1. Algorithme : Un algorithme, ou plus précisément, un algorithme de recommandation est une opération mathématique qui rassemble toutes les données récoltées et les analyse. Cette analyse va lui permettre de déterminer quel contenu correspond le mieux au profil de l'utilisateur·trice et ce qui va le plus l'intéresser. Ainsi certaines informations lui seront proposées et d'autres pas. 2. Cookie : Petit fichier texte déposé sur l'appareil et conservé un certain temps. Il en existe plusieurs sortes. Certains servent à améliorer la navigation, par exemple en préremplissant des formulaires d'achats avec nos informations personnelles, ou à proposer des publicités ciblées en se basant sur les articles consultés, voire mis en favoris, dans une boutique en ligne.

3. Bulle de filtres :
En analysant nos comportements en ligne pour nous proposer des informations, services et produits qui répondent à nos goûts et nos intérêts, les plateformes et réseaux sociaux nous enferment dans une bulle sans nous laisser la possibilité de découvrir autre chose. La notion de « bulle de filtres » illustre cette situation.
4. Identité numérique :
Il s'agit de la présentation personnelle, de ce que chacun·e présente et dit de soi sur Internet.
5. Empreinte numérique :
Il s'agit de l'ensemble des traces que nous laissons derrière nous sur Internet. Des traces qui peuvent être volontaires ou involontaires.

Traces volontaires : ce sont souvent les informations que l'on donne en s'inscrivant sur un site ou en devenant membre d'un réseau social. Il peut s'agir du nom, du prénom, de l'adresse, de l'âge, des loisirs, etc. Ce sont également les photos et les vidéos que l'on publie.

Traces involontaires : ce sont les informations ou les données personnelles que les services et plateformes en ligne collectent sans que l'on s'en rende compte. Il peut s'agir des sites consultés, des recherches sur un moteur de recherche, du volume réglé sur notre appareil, de notre vitesse de frappe sur le clavier, de l'endroit de l'écran où nous cliquons, etc... Les traces involontaires sont également ce que les autres publient sur nous.

Les traces volontaires et involontaires peuvent être utilisées pour définir notre profil d'utilisateur·trice et nous adresser des contenus ciblés.

Elles constituent notre empreinte numérique. À ce titre, elles sont la base de notre réputation en ligne.

6. Aspects légaux :
Au niveau européen il existe le Règlement Général sur la Protection des Données (RGPD). Entré en vigueur en 2018, il permet aux utilisateurs et utilisatrices des réseaux sociaux d'avoir accès aux données qui ont été récoltées sur eux/elles. Dans l'onglet confidentialité des réseaux sociaux, nous pouvons demander une copie des données qui ont été récoltées sur nous. Ce droit s'étend à la Suisse.

De plus, en Suisse, si nous sommes victimes d'une atteinte à la

protection de nos données, nous pouvons nous appuyer sur la Loi fédérale sur la Protection des Données (LPD). La dernière mise à jour rentrera en vigueur en 2023.

7. Navigation privée :

Lorsque que nous ouvrons une fenêtre dans notre navigateur, nous pouvons aller dans les paramètres pour choisir d'ouvrir une fenêtre de navigation privée. En navigation privée, nos cookies, notre historique de navigation et nos mots de passe ne seront pas enregistrés. Cela ne nous rend pas anonymes mais nous permet de laisser moins de traces.

8. IP :

L'Internet Protocol est la série de chiffres et de lettres qui identifie tout appareil qui se connecte à un réseau informatique.

9. VPN :

Acronyme de Réseau Virtuel Privé, un VPN est un système qui modifie l'adresse IP de notre appareil lors de nos connexions. Il rend ainsi plus difficile l'identification et la localisation de l'ordinateur/smartphone que nous utilisons et permet, par exemple, de contourner des restrictions géographiques imposées à certains contenus en ligne et d'accéder à ceux-ci.

Les VPN ne garantissent pas l'anonymat de l'utilisateur·trice car leur usage se fait généralement par le biais d'un service en ligne proposé par un fournisseur. Ce dernier dispose d'informations permettant d'identifier l'utilisateur·trice et peut collecter ses données de navigation.

Les VPN ont gagné en popularité auprès des élèves car certain·e·s· influenceurs·euses sont payé·e·s pour les promouvoir.

10. Darknet :

Le darknet, aussi appelé darkweb, est la partie cachée du web. Pour le rejoindre il faut utiliser un navigateur particulier (Tor Browser). Il est très connu pour ses activités bien souvent criminelles (par exemple : vente de drogues, vente d'armes à feu, données bancaires volées, pédopornographie, etc.). Bien que son fonctionnement vise à rendre ses utilisateurs·trices anonymes, les polices enquêtent sur le darkweb et démantèlent des organisations.

Il est possible que les élèves abordent ce thème qui est l'objet de vidéos sur Youtube et de publications sur les réseaux sociaux. Ils ou elles peuvent imaginer que le darknet ressemble à Internet alors qu'il est constitué de listes comme un annuaire.