VIE PRIVÉE ET SURVEILLANCE

Le développement des technologies numériques nous amène à questionner notre rapport à la sphère privée. Comment le numérique change-t-il l'**échelle et la nature de la surveillance**? Qu'est-ce qu'une **trace numérique**? Quels sont les arguments mobilisés par les défenseurs et les opposants aux pratiques de surveillance? Ce dossier propose des pistes pour répondre à ces interrogations.

Objectifs

- Prendre conscience des nouveaux enjeux de la surveillance numérique
- Comprendre ce que recouvre la notion de «trace numérique»
- Saisir les implications des argumentaires construits autour de la surveillance

Enjeux

🕵 Les nouveaux enjeux de la surveillance

Si la surveillance n'est pas née avec l'informatique, l'avènement des technologies de l'information et de la communication (TIC) à partir des années 1980, puis des terminaux mobiles et des médias sociaux a considérablement reconfiguré l'échelle et la nature de cette pratique, soulevant de nouveaux enjeux sociaux et politiques.

On peut aujourd'hui identifier trois formes de surveillance numérique. La première, d'ordre économique, est liée au modèle commercial des plateformes. Le but de cette surveillance est d'extraire et analyser les traces laissées par les utilisateurs afin de leur proposer des services personnalisés ou de vendre à des annonceurs des audiences publicitaires.[1] Pour la chercheuse Shoshana Zuboff, il s'agirait d'un nouveau modèle économique, qu'elle nomme «**capitalisme de surveillance**». Ce système mise sur la captation et le traitement des traces numériques afin de prédire et orienter les comportements au plus près des objectifs des annonceurs. Facebook est l'illustration parfaite de ce modèle.

Un second type de surveillance est d'ordre politique, elle concerne les pratiques exercées par les États. Cette forme de surveillance a été mise en lumière en 2013 par Edward Snowden. Cet ancien employé de la CIA et de la National Security Agency (NSA) révéla, documents à l'appui, la façon dont les services de renseignements américains et britanniques surveillent massivement les communications mondiales. Le dévoilement du programme de surveillance PRISM a mis au jour la collaboration entre la NSA et de grandes entreprises du numérique (dont Google, Facebook, Microsoft et Yahoo!). Celles-ci permettaient aux services de renseignement de disposer d'un accès aux données des utilisateurs. L'ampleur des informations collectées démontre un changement dans la nature de la surveillance : il ne s'agit plus de cibler un individu ou un groupe selon des critères précis. La surveillance s'exerce de manière massive sur l'ensemble de la population.

Un troisième type de surveillance se déploie de façon horizontale, entre individus. Internet, et, davantage encore, le **Web social**, a permis à chacun de voir et d'être vu. Cette veille de tous par tous est parfois désignée par le terme de «sousveillance» (voir encadré en page 4), soit une surveillance «par le bas».

🐾 Traces numériques

Ces diverses formes de surveillance se développent au cours des années 2000, à un moment où les pratiques numériques, tout comme les dispositifs permettant de recueillir les «**traces**» de ces activités, se multiplient. De nouvelles données d'une ampleur inédite sont ainsi produites, tandis que les capacités de stockage et de traitement de ces informations augmentent considérablement. Cette articulation entre une production massive de données complexes et des techniques permettant leur analyse est communément nommée **big data**.

Les traces concernées peuvent résulter de partages intentionnels (*tweets*, *likes,* publications sur les réseaux sociaux), mais une grande partie d'entre elles proviennent d'un enregistrement automatique de différents paramètres liés à nos activités en ligne (géolocalisation, adresse IP, historique de recherche et de navigation,..). Individuellement, ces traces n'ont que peu de sens. Mais lorsqu'elles sont centralisées et agrégées, elles permettent d'obtenir de précieuses informations sur les profils et comportements des individus.

[1] 👉 Voir dossier «Économie du numérique».

Ce nouveau pouvoir de surveillance, qui repose sur la capacité à collecter, traiter et analyser les traces numériques, est concentré entre les mains de quelques grands acteurs qui disposent des capacités techniques et de l'infrastructure nécessaire à son déploiement: Google, Facebook, la NSA, et les intermédiaires que sont les **data brokers**. Cette forme de surveillance est particulièrement opaque et asymétrique : les entreprises (ou États) cherchent à obtenir un maximum d'informations sur les individus, tout en dissimulant le plus possible leurs méthodes et processus qui s'apparentent à des «**boîtes noires**». Les atteintes à la vie privée peuvent dès lors être à la fois omniprésentes et invisibles.

Malgré la puissance de ces nouveaux outils et leur capacité à révéler des régularités (ou *patterns*) qui seraient imperceptibles autrement, il est important de souligner que les traces ne fournissent qu'une information partielle sur le monde. En les considérant comme des données opérationnelles, le risque est alors de prendre des décisions de façon automatisée, sur la base de simples «signaux». Si les données peuvent renseigner en partie sur le passé, leur aptitude à prédire des comportements futurs demeure limitée. Les calculs et prédictions effectués par les algorithmes sur la base des traces recueillies s'avèrent parfois erronés et peuvent conduire à des décisions arbitraires ou discriminantes sur lesquelles les individus n'ont que peu de prise.

🙈 Rien à cacher ?

L'un des arguments les plus couramment avancés pour justifier les pratiques de surveillance est l'idée selon laquelle «si vous n'avez rien à cacher, vous n'avez rien à craindre». A priori, cela semble en effet relever du bon sens : une personne qui ne commet aucun délit ne sera pas affectée par des dispositifs de surveillance. Dans les discours populaires sur la surveillance, cette affirmation est souvent présentée sous la forme d'une pesée d'intérêts entre vie privée et sécurité. L'argument a par exemple été utilisé comme slogan d'une campagne d'information lors du déploiement d'un programme national de vidéosurveillance en Grande-Bretagne. Selon ce principe, la surveillance ne serait qu'un faible prix à payer pour garantir la sécurité de chacun.

LA SOUSVEILLANCE

La notion de «sousveillance» décrit un dispositif inverse à celui de la surveillance, soit un système dans lequel les personnes surveillées observent à leur tour les surveillants. Il s'agit donc de regarder «par le bas» ce qu'il se passe en haut en s'appropriant les mêmes outils.

Le concept recouvre une forte dimension politique, car il suppose une action visant à contrôler les différentes formes de pouvoirs étatiques ou commerciaux. Ce dispositif peut être perçu comme une action citoyenne, dans le sens où il permet à chacun de médiatiser certaines dérives et ainsi prendre part au débat public. La captation et la publication de scènes de violences policières, par exemple, s'inscrivent dans cette perspective.

Plus généralement, la notion de sousveillance s'applique également à nos activités en ligne qui nous placent dans la position de potentiels observateurs et «surveillants» des comportements de chacun.

Ce discours est également repris par les entreprises dont le modèle économique repose sur la collecte et l'analyse des traces numériques. Ainsi, Eric Schmid, ancien PDG de Google, a déclaré en 2009 : «Si vous voulez que personne ne soit au courant de certaines choses que vous faites, peut-être que vous ne devriez tout simplement pas les faire». Pourtant, la problématique de la surveillance est bien plus complexe.

Tout d'abord, le principe de l'argument «si vous n'avez rien à cacher, vous n'avez rien à craindre» est réfutable. En effet, tout le monde à quelque chose à cacher. Même s'il ne s'agit pas d'actes répréhensibles ou illégaux, chacun a le droit à une vie privée. Selon le contexte (professionnel, familial, amical, etc.) nous partageons certains éléments de notre vie et pas d'autres.

Ensuite, cet argument minimise les implications de la surveillance en termes de libertés et

droits fondamentaux. Voici quelques-uns des points qu'on peut lui opposer.

1. **On ne peut être certain que ce que l'on fait aujourd'hui ne sera pas interdit demain, ou ailleurs.** Notre situation peut évoluer, tout comme l'environnement politique et social dans lequel nous vivons. Il n'est pas sûr que ce qui est toléré aujourd'hui le sera encore dans le futur. De la même manière, un acte admis dans un pays peut faire l'objet d'une répression dans un autre. Cette situation est particulièrement délicate pour les journalistes, avocat·es ou militant·es des droits humains, dont les libertés peuvent être menacées. Pour ces raisons, certaines de ces professions sont déjà davantage protégées.

2. **On n'agit pas de la même façon lorsque l'on se sait surveillé.** La surveillance peut ainsi limiter la liberté d'expression, de création et d'action.

3. **On ne décide pas de ce qui est surveillé et comment.** Avec la surveillance numérique, il est très difficile de se rendre compte du type de données qui sont collectées et de l'usage qui en est fait. Le risque est que certaines décisions soient prises à notre insu (refus d'octroi d'un prêt, détermination du montant d'une assurance, etc.), en s'appuyant sur nos traces numériques, sans que nous puissions en comprendre la raison. La transparence des processus de prise de décision est une condition fondamentale de la démocratie.

4. **Notre rapport personnel à la surveillance n'engage pas que nous.** Notre vie est faite de relations sociales. Lorsqu'une personne est placée sous surveillance, son entourage l'est également. Les données «personnelles» ne concernent rarement qu'un individu.

Cette liste - non exhaustive - montre que la question de savoir si nous avons «quelque chose à cacher» n'est pas pertinente. Cet argument conçoit la vie privée comme un droit individuel qui viendrait s'opposer au bien commun (en particulier, à la sécurité). Or, comme le souligne le juriste américain Daniel Solove, intérêts individuels et collectifs ne sont pas nécessairement opposés. Le respect de la vie privée garantit un espace de liberté et une confiance nécessaires à la vie en société.

🔐 La fin de la vie privée?

Les entreprises dont le modèle économique repose largement sur la captation des traces numériques ont tenté d'imposer l'idée selon laquelle le rapport à la vie privée aurait évolué avec le développement des technologies numériques. Celle-ci n'aurait désormais que peu d'importance et les utilisateurs des services numériques accepteraient cette forme de surveillance s'ils peuvent en tirer des bénéfices. Selon cet argumentaire, on se dirigerait donc vers «la fin de la vie privée». Lors d'une interview donnée en 2010, Mark Zuckerberg affirmait ainsi que l'on assistait à l'émergence d'une nouvelle «norme» sociale de transparence et que Facebook ne faisait que s'ajuster à cette évolution. Ce discours légitimait la pratique d'extraction des données en l'associant à une dynamique sociale prétendument en cours.

Or, les travaux de recherche sur les pratiques en ligne montrent que le rapport des utilisateurs à leur vie privée ne correspond pas au discours des plateformes. Les individus n'acceptent pas cette surveillance de bon gré. Selon leurs compétences, ils développent diverses stratégies pour tenter de maîtriser les contenus qu'ils partagent et les données qui sont collectées à leur sujet : obstruction de la webcam, installation de bloqueurs de publicité, suppression des cookies, utilisation de plusieurs comptes, pseudonymes et adresses e-mail. Mais ces stratégies sont inégalement efficaces et il demeure impossible de contrôler l'ensemble des informations transmises, forçant ainsi les utilisateurs à un consentement résigné.

Les grandes entreprises du numérique et certains États détiennent ainsi un pouvoir considérable que les différents scandales (régulières fuites de données, révélations d'Edward Snowden, affaire Cambridge Analytica) n'ont que peu ébranlé. Cependant, la problématique de la protection de la vie privée fait l'objet d'une attention politique et citoyenne grandissante et les pressions sur les entreprises concernées sont toujours plus fortes.

Face à ce constat, certains acteurs ont tenté d'esquisser des solutions. En 2020, Google, sous la pression d'Apple, déclarait abandonner les **cookies** tiers. Quant à Facebook, l'entreprise affirme se réorienter vers un espace d'échange davantage privé et limité à un cercle

de connaissances restreint. Cette stratégie semble pourtant peu pertinente, car les inquiétudes des usagers concernent avant tout l'utilisation qui peut être faite des données par Facebook et des entités tierces, et non le degré de visibilité des publications, déjà largement paramétrable. Cependant, le modèle économique de Facebook est difficilement compatible avec une limitation du traçage. On comprend alors la colère du réseau social, lorsque Apple annonce désormais limiter l'accès à l'IDFA, cet identifiant unique à chaque appareil qui permet aux applications de traquer l'utilisateur pour lui proposer de la publicité ciblée.

Les solutions initiées par les entreprises, toujours dépendantes de leur modèle économique, ne peuvent offrir une réponse satisfaisante aux préoccupations grandissantes de la population. Quant aux initiatives individuelles, elle restent tributaires des compétences des individus et ne garantissent pas une protection optimale dans un environnement numérique qui cherche à capter toujours plus de traces de nos comportements.

Seule une approche collective de la protection de la vie privée permet d'envisager des solutions concrètes. La mise en place du règlement général sur la protection des données (**RGPD**) est un premier et important pas dans cette direction. Entré en vigueur dans l'Union européenne en 2018, il vise à garantir aux citoyens le respect de leurs droits fondamentaux en imposant un cadre légal précis aux entreprises qui collectent des données.

La Chine et le crédit social

Lorsque l'on parle de surveillance de masse, le «**système de crédit social**» chinois est souvent mobilisé pour illustrer les dérives possibles d'une telle pratique. Ce dispositif visant à évaluer les comportements des citoyens et des entreprises a été mis en place par l'État chinois dans le but d'inciter les individus à davantage respecter les nombreuses lois du pays.

Le système de crédit social est présenté comme un moyen d'accroître l'intégrité morale de la population et de rétablir la «confiance» au sein de la société face à une application arbitraire, voire corrompue, des lois chinoises, avec pour conséquences des troubles à l'ordre public et des entraves au développement économique. Pour mettre un terme à ces problèmes endémiques, l'État chinois a instauré un système de «capital de points», qui peut augmenter ou diminuer selon les agissements de chacun, menant à des sanctions ou des récompenses.

Cependant, contrairement aux imaginaires couramment véhiculés, le contrôle des comportements s'effectue au travers de dispositifs de surveillance qui demeurent relativement rudimentaires. En effet, la collaboration entre les autorités et les entreprises du numérique reste complexe et la plupart des informations sont encore collectées par des moyens humains lors de procédures administratives ou contrôles policiers. Si le secteur technologique chinois est en plein développement et que les entreprises ont largement recours à des dispositifs numériques (telle que la reconnaissance faciale), ceux-ci ne sont, pour l'instant, pas intégrés à un système de surveillance étatique global.

Par ailleurs, le système de crédit social est encore expérimental et loin d'être déployé de façon systématique et unifiée. Le big data est peu exploité dans ce cadre et il n'existe pas, à l'heure actuelle, de base de données centralisée ni de score de crédit unique qui serait automatiquement majoré ou diminué suite à chaque action enregistrée par un dispositif de surveillance. Les mises en œuvre se font à l'échelle locale et les priorités, tout comme les méthodes, peuvent diverger. Pour l'État central, le crédit social permet d'alimenter un système de *blacklists* qui existait déjà auparavant. Ces listes visent à identifier et sanctionner les individus qui ont commis des délits ordinaires, souvent d'ordre économique (arnaques, dettes impayées).

Impuissant face à certains problèmes structuraux (pauvreté, surendettement, manque accès au soin, spéculation immobilière), le gouvernement chinois multiplie les mécanismes coercitifs dans l'espoir que le respect des règles permettra de garantir la stabilité sociale, le développement économique et la crédibilité du régime. Ces mesures politiques, prises dans le contexte du rapide développement des technologies numériques, renforce la perception d'un État chinois qui surveille et évalue chaque fait et geste de ses citoyens.

Ressources

- Un article de la chercheuse Shoshana Zuboff sur la notion de «capitalisme de surveillance» (*Le Monde diplomatique*)
- Un podcast qui propose de mieux comprendre le fonctionnement des traqueurs intégrés aux applications mobiles (France Inter, *Le code a changé*)
- Un dossier qui analyse le rapport quotidien des individus à leurs données personnelles et leur vie privée (Laboratoire d'innovation numérique de la CNIL)
- Le livre du journaliste Olivier Tesquet : *À la trace. Enquête sur les nouveaux territoires de la surveillance* (Premier Parallèle, 2020)
- Le livre de l'informaticien et philosophe Jean-Gabriel Ganascia qui explore la notion de sousveillance : *Voir et pouvoir : qui nous surveille ?*
- Le film documentaire *Nothing to Hide* de Marc Meillassoux et Mihaela Gladovic (2017)
- Un entretien avec la sinologue Séverine Arsène sur le pouvoir numérique chinois (revue *Esprit*)

Glossaire

- Trace numérique
- Cookie
- Capitalisme de surveillance
- RGPD
- Data broker
- Boite noire
- Système de crédit social (Chine)
- Web social ou Web participatif

Fiches / Dossiers complémentaires

L'AFFAIRE SNOWDEN | ÉCONOMIE DU NUMÉRIQUE

1 Suivre à la trace

Objectifs Comprendre la notion de «trace numérique»

Prendre conscience des nouveaux enjeux liés à la surveillance des pratiques numériques

A Sur Internet, tout le monde sait qui tu es

🕓 20 min ✍ débranché

Montrer les deux images en page 8 et poser les questions suivantes :

a) Comparez les deux dessins. Quel est le message de chacun?

Publié en 1993, au moment où l'on commence à parler d'Internet dans la presse grand public, ce premier dessin met en évidence l'anonymat (ou le pseudonymat) qui caractérisait la navigation en ligne à ses débuts. Il souligne aussi qu'Internet est un espace où chacun peut évoluer sans être jugé.

Le second dessin propose une version actualisée de cette caricature. Aujourd'hui, chaque activité sur le Web laisse des traces et les comportements des internautes sont pistés par toutes sortes de traqueurs, essentiellement à des fins commerciales (bien que ces données puissent également être utilisées dans un objectif de surveillance politique, comme l'a montré Edward Snowden). Par ailleurs, certaines plateformes, telles que Facebook - et donc tous les services qui utilisent son système d'authentification - ont réussi à imposer aux utilisateurs l'usage de leur vrai nom. Il devient ainsi de plus en plus difficile de dissimuler son identité.

b) Que s'est-il passé entre les deux dessins?

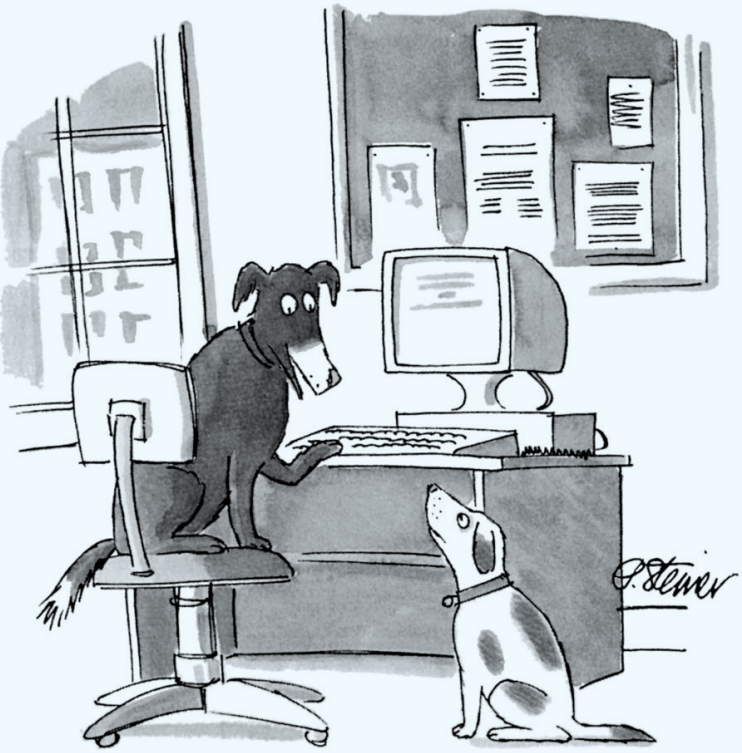
- *Avec l'émergence du Web participatif au début des années 2000, puis des réseaux sociaux, les internautes ont commencé à interagir en ligne, produisant ainsi - consciemment ou non - des traces numériques. Une fois collectées et agrégées, ces traces permettent d'obtenir des informations quant au profil des utilisateurs (données socio-démographiques, goûts, relations,...)*

- *Les plateformes en ligne ont perçu un intérêt commercial à capter toujours de plus de traces de ces pratiques pour proposer des services "personnalisés", ou se positionner comme intermédiaire et vendre à des annonceurs des espaces publicitaires ciblés.*

- *Les traces numériques des utilisateurs sont progressivement devenues l'invisible monnaie d'échange pour accéder à des services, souvent gratuits.*

- *La valeur grandissante de cette nouvelle masse de données a encouragé le développement de systèmes informatiques toujours plus performants et capables de stocker, traiter, et recouper d'immenses bases de données.*

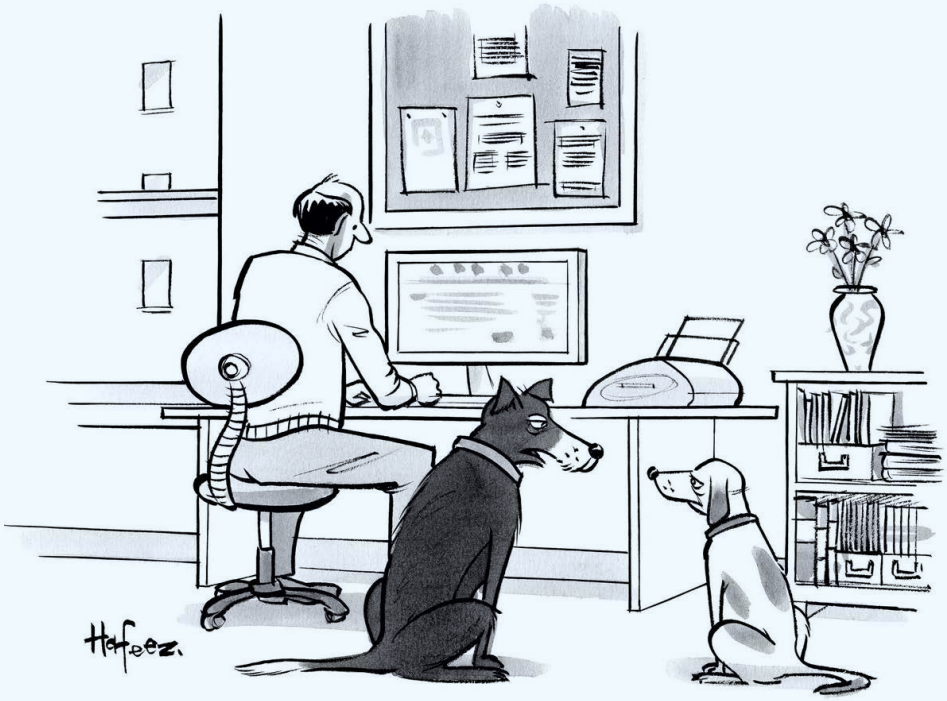
- *L'arrivée des smartphones et de nombreux «objets connectés» a encore ouvert le champ à la captation d'un nombre considérable de nouvelles traces, rendant l'évitement de cette forme de surveillance presque impossible.*



"On the Internet, nobody knows you're a dog."

The New Yorker, 1993

Télécharger l'image



"Remember when, on the Internet, nobody knew who you were?"

The New Yorker, 2015

Télécharger l'image

Proposer aux élèves, par petits groupes, de réfléchir aux questions suivantes :

c) Qui collecte des données numériques (quel type d'entreprises/institutions) et pour quelles raisons?

Quelques éléments de réponses :

• Les fournisseurs d'accès à Internet, ainsi que de très nombreux services en ligne : réseaux sociaux, sites de e-commerce, Google et tous ses services (Gmail, Google Maps, Chrome, etc.), applications de rencontre, vidéo et musique en streaming, de musique, jeux en ligne. Pour ces entreprises, la collecte de données constitue un enjeu économique (cf question b.)

• Les États peuvent être amenés à collecter des données sur les citoyens. Cette forme de surveillance existait auparavant, mais avec le développement des technologies numériques, elle a changé d'échelle. Certains gouvernements ont désormais recours à une surveillance de masse, c'est-à-dire qu'ils ne ciblent plus seulement un individu ou un groupe suspect, mais l'ensemble de la population. Pour cela, ils s'appuient - entre autres - sur les données collectées par les grandes entreprises du numérique, comme l'a révélé le lanceur d'alerte Edward Snowden. Les pays concernés, justifient ces pratiques de surveillance à grande échelle comme le seul moyen de garantir la sécurité intérieure, en particulier suite aux attentats du 11 septembre 2001. Cette position est contestée par de nombreuses ONG et associations (dont La Quadrature du Net, Amnesty International, Privacy International), qui considèrent cette surveillance comme arbitraire et contraire au droit fondamental à la vie privée.

De quels types de données s'agit-il?

Deux catégories de données sont collectées : les informations publiées en ligne de façon consciente : tweets, likes, photos, commentaires ; et les données captées à l'insu des utilisateurs : adresse IP, langue, historique de recherche, localisation, temps de visionnage, clics, contenus des e-mails, (pour Gmail, notamment), etc. Nos activités en ligne laissent donc de nombreuses "traces numériques".

B Visualiser les traqueurs

🕓 30 min 🧑‍💻 branché

Le logiciel *CookieViz* (proposé par la CNIL) permet de visualiser en temps réel les traqueurs qui suivent notre navigation sur Internet.

Avant de démarrer l'activité, installer *CookieViz* sur les ordinateurs des élèves :

- Télécharger la version Mac ou PC depuis le compte GitHub de la CNIL
- Exécuter le fichier CookieViz (./ CookieViz, CookieViz.exe ou CookieViz.app, selon votre système)
- Sur Mac, il faut peut-être débloquer l'autorisation d'installation dans les paramètres «Sécurité et confidentialité»

a) En introduction, expliquer ce que sont les cookies et leurs différents usages.

b) Par petits groupes, proposer aux élèves de naviguer sur un ou deux sites et d'analyser le contenu du message relatif à l'utilisation des cookies. Que dit-il? Quelles sont les possibilités de paramétrage des cookies?

c) Ensuite, à l'aide de CookieViz, taper l'adresse du site dans la fenêtre de l'application et analyser les cookies présents sur le site (en cliquant sur l'œil). Quels types de traqueurs apparaissent? A quoi servent-ils?

d) Mettre en commun les réponses des différents groupes.

Exemple avec le site 24heures.ch

Une trentaine de traqueurs sont identifiés par CookieViz, dont Google, Facebook, Tiktok, Amazon et diverses régies publicitaires.

Ce pistage sert tout d'abord à analyser le

profil et le comportements des internautes sur le site (localisation, clics, vues, temps passé sur un article). Il permet au journal de mieux comprendre les habitudes et préférences des utilisateurs. Il pourra ainsi adapter son contenu ou suggérer des offres personnalisées aux lecteurs. Mais certains cookies tiers permettent aussi à d'autres entreprises (essentiellement des régies publicitaires) d'accéder à ces informations et d'établir ainsi un profil le plus précis possible de l'utilisateur afin de lui proposer un contenu publicitaire ciblé en dehors du site du journal.

A noter que dans ses paramètres de confidentialité, le site du journal 24heures affiche une liste détaillée des cookies tiers. Ces derniers sont considérablement plus nombreux que ceux que le logiciel CookieViz est capable de détecter.

Options alternatives

- Possibilité de faire le même exercice en utilisant l'extension Kimetrak (disponible uniquement pour Firefox). La visualisation des traqueurs apparaît lorsque l'on clique sur l'icône orange de Kimetrak, en haut à droite de la fenêtre de navigation.

- Le site de l'association Exodus Privacy liste les traqueurs et les permissions présentes dans de nombreuses applications mobiles Android.

2 Rien à cacher?

Objectif Saisir les enjeux que pose l'argument «si vous n'avez rien à cacher, vous n'avez rien à craindre»

A L'importance de la sphère privée

🕓 30 min ✍️ débranché

Par petits groupes demander aux élèves de réfléchir aux questions suivantes :

a) Avec quelle personne ou groupe ci-dessous....

- Parents
- Amis
- Enseignant
- *Followers* sur Instagram
- Inconnus

.... partageriez-vous sans hésiter ces informations suivantes :

- Votre historique de recherche Google
- Les photos de votre smartphone
- Vos messages privés
- Le nom des personnes que vous avez cherchées sur les réseaux sociaux
- Les dernières vidéos que vous avez visionnées

Cet exercice permet de prendre conscience du fait que l'on partage des informations différentes selon la personne ou le public auquel on s'adresse.

b) Imaginez que tous les espaces de l'école (salles de classe, couloirs, espaces extérieurs) soient surveillés par des caméras et micros. Selon vous, est-ce que votre comportement changerait? Si oui, de quelle façon?

Note: On peut, par exemple, demander aux élèves s'ils/elles :

- raconteraient leur dernière soirée
- diraient du mal d'une personne
- copieraient leur devoir à la dernière minute avant d'entrer en classe
- partageraient une information confidentielle avec un·e ami·e
- enverraient des messages pendant les cours

Cette réflexion a pour objectif de montrer la nécessité d'un espace privé. Chaque jour, nous faisons des choses que nous n'aimerions pas afficher publiquement.

c) L'un des arguments que l'on entend souvent pour défendre la mise en place de dispositifs de surveillance est que "si nous n'avons a rien à cacher, nous n'avons rien à craindre". Que pensez-vous de cet affirmation?

Discutez les réflexions des élèves en amenant les contre-arguments proposés dans le paragraphe "Rien à cacher ?" en page 3. Deux d'entre eux sont déjà évoqués aux questions a) et b).

Lors d'une visio-conférence en 2016, Edward Snowden déclare ceci :

« *Affirmer que vous ne vous souciez pas du droit à la vie privée parce que vous n'avez rien à cacher, c'est comme dire que la liberté d'expression est inutile parce que vous n'avez "rien à dire".*»

d) Qu'entend-il par là?

Ce n'est pas parce que l'on ne fait pas usage d'un droit soi-même que l'on peut nier que d'autres puissent en avoir besoin. Selon Edward Snowden, il s'agit là d'un argument fondamentalement antisocial qui ne tient pas compte des risques que peuvent rencontrer certaines populations lorsque leurs droits sont bafoués.