

Épisode Traces numériques

Ce document est destiné aux médiateurs éducatifs souhaitant mener des actions d'Éducation aux Médias et à l'Information et / ou des ateliers pour mieux gérer ses traces numériques. Il contient :

- 1) Une piste d'atelier de 50 minutes (EMI-LAB)
- 2) Un petit précis de base sur les désordres de l'information (EMI-BASES)

L'ATELIER LIBERTE D'EXPRESSION EMI-LAB

Thématique : Empreintes / traces numériques

Âge : 12-18 ans (collège, lycée)

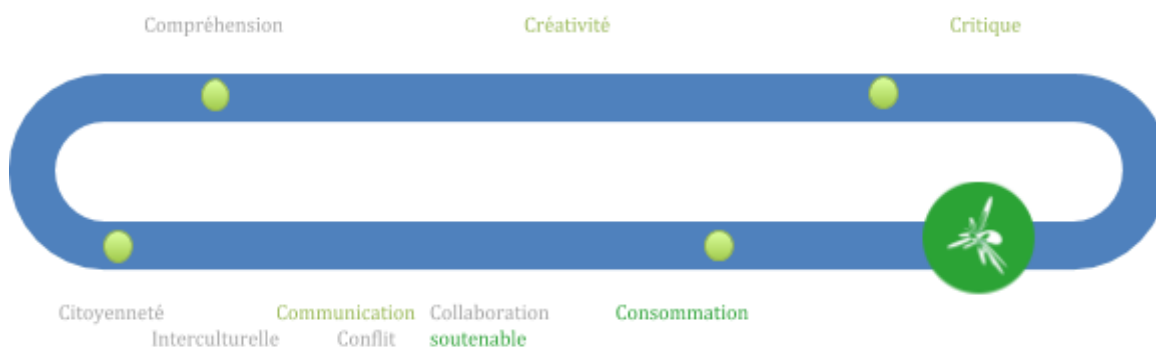
Disciplines concernées : Toutes matières, et en particulier géographie, histoire, enseignement moral et civique, sciences numériques et technologie, sciences numériques et sociales

Durée : 50 minutes

Matériel requis : Un vidéo projecteur / ordinateur connecté

Pour visionner la vidéo [CLIQUEZ ICI](#)

Les COMPÉTENCES EMI concernées



LE DÉROULÉ

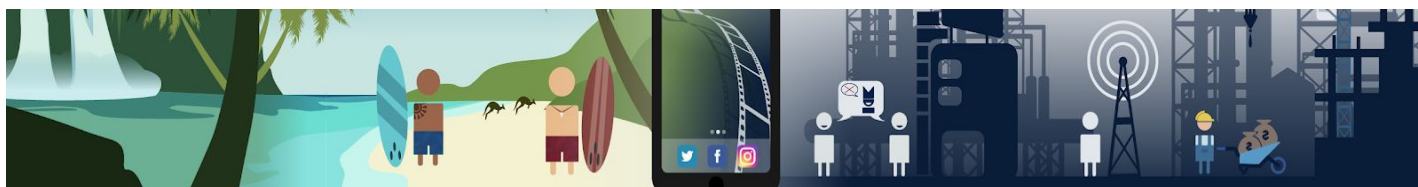
1) Débattre avec le groupe sur...

Suggestion de questions :

- Qu'évoque pour vous le terme de trace numérique ?
- Protéger sa vie privée, c'est important pour vous ? Et l'intimité ?
- Quelles sont les données que vous ne souhaitez pas partager avec la planète entière ?
- Savez-vous quelles sont les données qui sont protégées par la loi ?
- A votre avis, que font les plateformes numériques de vos données ?
- Et l'Etat ?
- Pensez-vous que votre liberté peut être mise en danger par la collecte de vos données ?

2) Faire visionner la vidéo dans son intégralité

- *Qu'en pensez-vous ? Notez les réactions spontanées des jeunes.*



3) Analyser, interpréter et réagir : reprendre la vidéo avec le groupe, en mode débat

Timing [00,00 - 00,26 - 00 :39] **INTRODUIRE... EN DOUCEUR : LES TRACES**



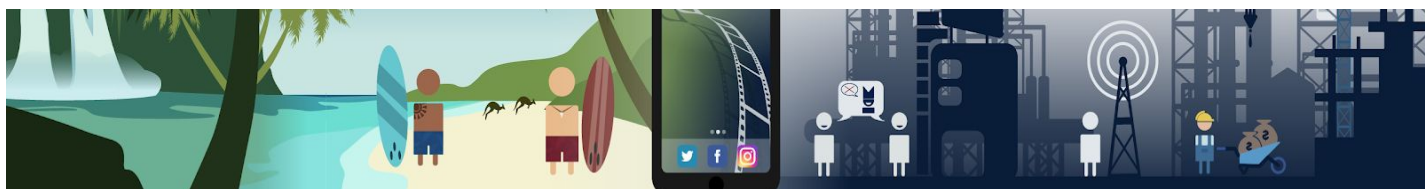
SCÉNARIO	MESSAGES CLÉS	ANALYSER	POUR DÉBAT
Vous déverrouillez le téléphone avec votre visage, faites des courses en ligne, comptez vos pas sur une appli, avez liké un post, pris un selfie... Souriez, vous êtes tracés !	Toute action en ligne laisse des traces.	Dès lors où nous effectuons une action en ligne, les systèmes informatiques peuvent la conserver en mémoire sous forme de donnée. La somme de ces données, qui peuvent sembler anodines, permet d'en savoir bien plus qu'on ne l'imagine sur les gens.	Pouvez-vous lister ce que Facebook sait de vous ? Et Google ?
Une fois agrégées, les données acquièrent de la valeur et modifient notre quotidien en nous donnant des suggestions de musique à écouter, de séries à voir, de personnes à rencontrer, de services à acheter...	Nos données servent essentiellement à nous proposer/ nous vendre des services personnalisés.	C'est la somme des traces laissées par une multitude d'utilisateurs qui fait la valeur de ces données et permet de mettre en place des stratégies commerciales. Ces pratiques sont parfaitement légales puisque ces données comportementales récoltées et traitées à notre insu ne sont pas des données personnelles et sont anonymisées.	Trouvez-vous cela bien que l'on vous propose des sélections personnalisées de produits ou services ?

Timing [0 :40 -00 :55 - 01 :15]

ENTRER DANS LE DUR : LES DÉRIVES



SCÉNARIO	MESSAGES CLÉS	ANALYSER	POUR DÉBAT
Outre les données que l'on donne, il y a celles que l'on nous « pique » : gare au hameçonnage, au profilage, ou encore au flicage, voire à l'espionnage !	Nos données valent de l'or (noir) ! Outre celles que nous fournissons, il y a toutes celles qui sont collectées à notre insu ou piratées à fins économiques ou politiques.	Dès lors où nous vivons dans une économie de la donnée, des dérives sont à attendre et se produisent. Le phishing a remplacé l'attaque de la diligence. Le problème, c'est que c'est invisible et que l'on ne s'en rend pas toujours compte.	Vous a-t-on déjà piraté vos données ? Que faites-vous pour sécuriser vos équipements et protéger vos données ?
Les plateformes numériques servent d'agents intermédiaires pour vous profiler avec des algorithmes de prédiction et autres analyses de sentiments rendues possibles par la captation de données par des mouchards.	Si c'est gratuit, c'est vous le produit : c'est le modèle d'affaires du numérique, identique au modèle des médias aux Etats-Unis (financé par la publicité et les données).	Le modèle de la gratuité, alimenté par des années d'habitude, est au cœur de la problématique des données.	Etes-vous prêt à payer pour les services que vous aimez et utilisez pour ne pas que l'on prenne vos données ?



Timing [1 :16-1 :32]

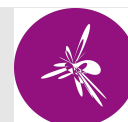
UNE SOCIÉTÉ DE SURVEILLANCE À L'HORIZON



SCÉNARIO	MESSAGES CLÉS	INTERPRÉTER	POUR DÉBAT
<p>Bonus malus pour bon comportement au travail en ville en voiture...</p> <p>Des régimes autoritaires et même des sociétés démocratiques collectent des données sensibles à des fins de surveillance subreptice ou d'incitation douce.</p>	<p>Le danger majeur lié aux traces numériques est l'instauration de sociétés de surveillance ou la manipulation politique des populations.</p>	<p>De nombreux scandales ont montré que la surveillance numérique des populations ou leur manipulation est loin d'être l'apanage des seuls régimes autoritaires.</p>	<p>A votre avis, que sait l'Etat de vous ?</p> <p>Y-a-t-il des risques de surveillance ?</p>

Timing [1 :32 – 2 :37]

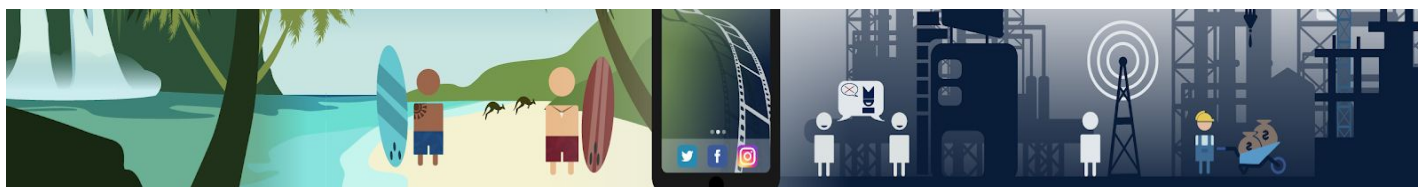
QUELLES SOLUTIONS ?



SCÉNARIO	MESSAGES CLÉS	RÉAGIR	POUR DÉBAT
<p>La parade ? Mettre en place des stratégies pour gérer ses traces numériques en trouvant un juste équilibre entre partage et protection.</p> <p>Il existe des outils pour éviter les vols de données et les mouchards.</p> <p>Et le RGPD pour protéger notre vie privée.</p>	<p>Des traces, cela se gère. A chacun sa stratégie selon ses idées, sa vision du monde.</p> <p>Nos données peuvent faire avancer de belles et nobles causes. Il ne s'agit pas de tout garder pour soi mais de choisir à qui et pourquoi on les confie.</p>	<ul style="list-style-type: none"> ✓ Compartimenter privé et public ✓ Veiller à ses données sensibles ✓ « Donner » ses données à bon escient ✓ Choisir des services qui ne tracent pas, ou moins ✓ Utiliser des extensions sur vos navigateurs pour bloquer les mouchards ✓ N'utiliser la géolocalisation que lorsque nécessaire 	<p>Est-ce que vous seriez prêt à des politiques de « crédit social » comme en Chine ?</p> <p>Comment faire pour trouver équilibre entre partage et protection ?</p>

4) Conclure

Demander aux participants de tester un ou plusieurs extensions de navigateurs permettant de se protéger des mouchards et autres cookies.



LES EMI-BASES «LIBERTÉ D'EXPRESSION »

DÉFINITIONS

Données : se réfère à des informations codées qui peuvent prendre de nombreux formats tels que du texte, des images et des sons mais aussi des interactions, des événements, des transactions. Elles peuvent être utilisées comme descripteurs de base de la vie réelle d'une personne, dans sa forme numérique. Les Informations Personnelles Sensibles ou Sensitive Personal Information (SPI) peuvent inclure le nom de la personne, son numéro de sécurité sociale, sa date et son lieu de naissance, ses données biométriques. Pour l'EMI les débats sont centrés autour des utilisations tierces, qu'elles soient commerciales (marché de collecte et vente de données) ou criminelles (vol de données à des fins illégales). Cela peut entraîner des violations de la sécurité et de la vie privée. Voir Données massives, Vie Privée

Trace numérique : il s'agit d'un ensemble unique d'activités numériques traçables sur Internet (par exemple, vues de sites Web, commentaires, paiements). Elles se répartissent en deux catégories: passive et active, ou involontaire et volontaire. La première concerne les données collectées à l'insu du citoyen; la seconde concerne les données volontairement publiées pour partager et interagir en ligne avec les autres. En EMI, cela pose des problèmes de vie privée, de traçabilité et de sécurité. Voir aussi Sécurité, Vie Privée.

Cookie : un petit fichier stocké sur l'ordinateur d'un utilisateur, conçu pour contenir une quantité modeste de données spécifiques à un utilisateur particulier, dans la gestion des sites Web. Chaque fois que l'utilisateur accède à nouveau au site Web, le cookie est renvoyé au serveur sur lequel le site Web est stocké. Un cookie de suivi peut être intégré à un support publicitaire en provenance d'un site tiers et peut être utilisé pour signaler l'historique de navigation d'un utilisateur. Il peut ainsi faciliter des publicités ciblées et personnalisées. En EMI, les cookies peuvent être considérés comme une atteinte à la vie privée car ils permettent le profilage à l'insu de l'utilisateur. Ils nécessitent une réflexion critique pour éviter la propagande et les pratiques commerciales contraires à l'éthique. Voir aussi: Données, Vie Privée.

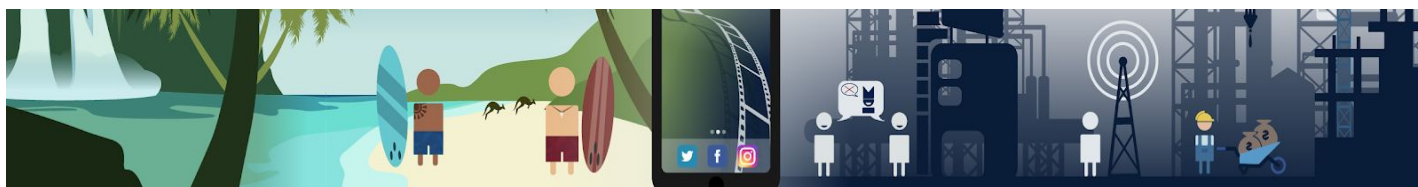
Phishing : combine les mots «phreaking» et «fishing» pour créer une image d'appât pour attirer une victime. Il s'agit d'une tentative des pirates de l'information et des pirates informatiques d'obtenir des données personnelles, en particulier des informations personnelles sensibles (SPI) en se déguisant en une personne de confiance (ami.e, collègue, banque, etc.) Le but est de diriger la victime vers de faux sites Web qui peuvent répandre des virus ou utiliser des données volées à des fins illicites. Voir aussi Cyber-sécurité, Données, Protection.

Profilage : processus consistant à examiner les données disponibles dans une base de données existante et à appliquer des statistiques pour fournir des métriques ou des prévisions sur les personnes ou d'autres activités en ligne. En EMI, les défis concernent la sensibilisation à la trace numérique et les abus possibles pour porter atteinte à la vie privée. Voir aussi Données massives; Données, Trace numérique; GDPR; Vie Privée.

DONNÉES PERSONNELLES ET SENSIBLES

Sont considérées données personnelles et protégées par la loi toute information ou groupe d'informations permettant d'identifier une personne : images, identifiants (nom, adresse, immatriculation, numéro de sécurité sociale...), infos santé, vie familiale, données bancaires...

Certaines sont en outre classifiées « données sensibles » et encore plus protégées : origine ethnique, religion, opinions politiques ou philosophiques, appartenance à un syndicat, orientation sexuelle, données génétiques et biométriques...



LE DROIT À LA VIE PRIVÉE, DROIT FONDAMENTAL DE LA PERSONNE

ARTICLE 12 DE LA DÉCLARATION UNIVERSELLE DES DROITS DE L'HOMME (ONU, 1948)

Droit à la vie privée

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

ARTICLE 8 DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME (1953)

Droit au respect de la vie privée et familiale

Toute personne a droit **au respect de sa vie privée et familiale**, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que **cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale**, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

CE QUE VOUS DONNEZ À FACEBOOK (LISTE NON EXHAUSTIVE !)

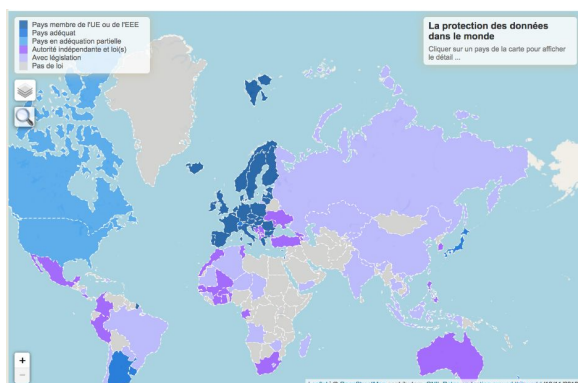
- Vos données publiques (A Tout Le Monde)
- La liste de vos amis
- Ce que vous aimez, ou pas
- Les sites que vous visitez
- Les groupes auxquels vous adhérez
- Les pages dont vous êtes fan
- Les cadeaux ou pokes que vous avez offerts
- Les événements auxquels vous avez participé
- Les vidéos que vous avez postées ou partagées
- Les applications que vous avez téléchargées
- La façon dont vous avez réagi à des pubs
- Des infos provenant de vos amis : qui vous a tagué, ce qu'ils ont dit de vous, les relations qu'ils indiquent avoir avec vous...
- Vos messages, y compris ceux du tchat même si effacés
- La liste complète des ordinateurs que vous avez utilisés pour vous connecter et la liste de toutes vos connexions depuis votre inscription
- Les contacts de votre smartphone si vous avez synchronisé ou que vous avez utilisé la fonctionnalité de recherche d'amis à partir des contacts de votre boîte mail... qui peuvent alors recevoir des mails de Facebook sans même être inscrits.

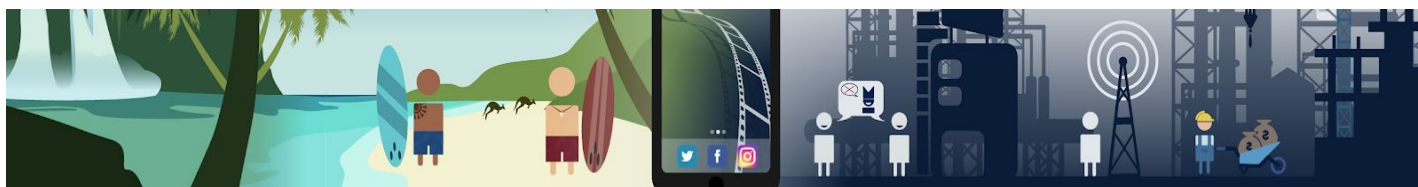
LES DIFFÉRENTS TYPES DE SOLUTION POUR PROMOUVOIR LA LIBERTÉ D'EXPRESSION

AUTO-RÉGULATION : solutions adoptées par les médias de masse et les médias sociaux eux-mêmes.

Dans le cas de la protection de la vie privée, les plateformes et entreprises européennes sont soumises au respect du RGPD. Elles peuvent en revanche prendre des dispositions pour limiter la collecte de données non personnelles (métadonnées) dans le cadre de bonnes pratiques. Peu le font... et pour ce qui est entreprises et plateformes américaines, elles se réfugient derrière le droit américain.

RÉGULATION :





www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

EDUCATION : solutions adoptées par les acteurs de la société civile, pour susciter des points de vue multiples, éveiller l'esprit critique, produire des contre-discours. C'est le rôle de l'Éducation aux Médias et à l'Information, et à la citoyenneté numérique, qui porte une attention toute particulière à la protection des données depuis 2018.

CITOYENNETÉ : solutions adoptées par tous pour établir les valeurs de diversité culturelle, la résolution de conflit et la consommation soutenable et avertie.

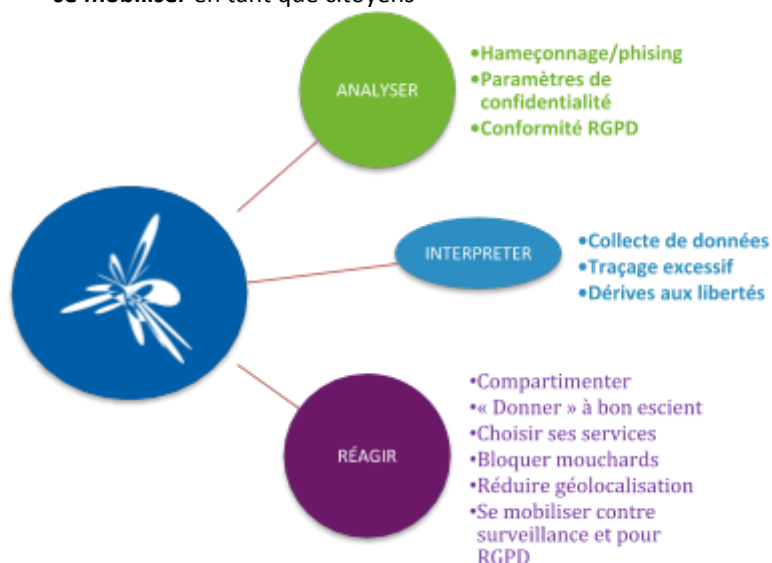
Construire l'esprit critique:

PRENEZ DE L'AIR (ANALYSER, INTERPRÉTER, RÉAGIR)

ANALYSER : se poser les questions du **Quoi** et du **Comment**

INTERPRÉTER : se poser les questions du **Qui** et du **Pourquoi** et avec quelles **Conséquences**

RÉAGIR : trouver des **solutions** politiques/ sociales/ culturelles/ économiques/ juridiques ;
se mobiliser en tant que citoyens



Pour aller plus loin...

[Le site de la CNIL \(cnil.fr\)](http://Le site de la CNIL (cnil.fr))

[- Ressources pédagogiques
- Textes de lois, Rapports, Etudes, Publications](http://Ressources Savoir Devenir (savoirdevenir.net/ressources/)<u>Ressources Savoir Devenir (savoirdevenir.net/ressources/)</u></p></div><div data-bbox=)

Ressources partenaires

- Pour les animateurs
[L'espace professionnel du site de la Bpi \(pro.bpi.fr/pro\)](http://La médiathèque éduc'active des Ceméa (yakamedia.cemea.asso.fr/)<u>La médiathèque éduc'active des Ceméa (yakamedia.cemea.asso.fr/)</u>• Pour les bibliothèques
<a href=)

Ce document et la vidéo sont sous licence Creative Common CC BY-NC-ND - Attribution – Réutilisation non commerciale – Pas de modification.



La série audiovisuelle *Médiatropismes* est une co-production **Savoir Devenir** et l'**INA** avec le soutien du **Ministère de la Culture**