



Parcours En quête de données

Livret enseignant – Cycle 4

Ce livret offre des suggestions pédagogiques, que chaque enseignant est libre d'adapter selon sa propre pratique et dans le respect de sa liberté pédagogique. A noter, les prérequis indiqués à la fin du premier temps sont à prendre en compte avant votre venue au Campus Numeria.

Préambule

Il est recommandé de réaliser les deux séances pédagogiques proposées en amont et en aval de la sortie au Campus Numeria (Futuroscope) pour profiter au mieux de l'expérience proposée.

Le **temps 1** est proposé pour balayer les concepts, donner les clés scientifiques et techniques utiles, et introduire le **temps 2** qui se déroule sur le site du Campus Numeria au Futuroscope. Une fois l'expérience vécue, le **temps 3** permet de structurer les concepts abordés et les compétences travaillées.

Afin de s'approprier les concepts et de mieux les transmettre, l'enseignant dispose d'une [ressource scientifique](#) d'appui à la compréhension du parcours.

Compétences travaillées (EMC – EMI)

Notions abordées	Contenus d'enseignement
Le respect d'autrui	Prendre conscience des enjeux civiques de l'usage du numérique et des réseaux sociaux.
Acquérir et partager les valeurs de la République	Identifier et connaître les cadres d'une société démocratique.
Construire une culture civique	• S'informer de manière rigoureuse. • Prendre part à une discussion, un débat ou un dialogue : prendre la parole devant les autres, écouter autrui, formuler et apprendre à justifier un point de vue. • Développer le discernement éthique.
Utiliser les médias de manière responsable	• Comprendre ce que sont l'identité et la trace numériques. • Se familiariser avec les notions d'espace privé et d'espace public.

Point scientifique : données et métadonnées d'une image

Une image est constituée de pixels qui définissent son contenu et notamment ce qu'elle montre lorsqu'elle est affichée dans n'importe quel logiciel capable de la visualiser. Cet ensemble de pixels constitue les données de l'image.

A une image peuvent être également associées des métadonnées qui donnent des renseignements complémentaires. Pour une photo prise avec un téléphone portable, par exemple, il est possible d'inscrire dans le fichier numérique contenant l'image, des informations sur l'appareil qui a pris la photo, sur la date et le lieu de la prise de vue. De manière générale, les métadonnées peuvent permettre de renseigner d'autres informations, comme le nom de l'auteur de l'image. La géolocalisation est une métadonnée qui permet d'enregistrer dans le fichier informatique de la photo, l'emplacement géographique de la prise de vue via sa latitude et sa longitude, coordonnées qui permettent de déterminer une position sur une carte.

Les métadonnées peuvent être créées en même temps que l'image (par exemple par le dispositif qui prend la photo) mais elles peuvent aussi être ajoutées ou modifiées ultérieurement. Ainsi pour les élèves qui n'ont pas encore la notion de latitude et longitude, les données de position peuvent être modifiées pour faire apparaître de simples coordonnées cartésiennes (type bataille navale par exemple) afin de leur permettre de travailler la localisation.

Les métadonnées peuvent être visualisées de différentes manières, soit dans l'explorateur de fichiers en demandant à afficher des informations ou propriétés d'un fichier image, soit en utilisant des logiciels de manipulation d'images, soit en utilisant des logiciels dédiés à la visualisation et à la modification de ces métadonnées.

Point d'attention : il existe des services en ligne qui proposent ce genre de services mais cela implique d'y déposer ses images. Les conditions d'utilisation du service et le degré de confiance à lui accorder doivent donc être soigneusement vérifiés pour garantir la protection des données transmises.

Premier temps du parcours (en classe) - Que racontent les images sur Internet ?

Objectifs

- Comprendre quelles informations sont contenues dans une image numérique (données et métadonnées).
- Développer l'esprit critique face aux images en ligne et aux intelligences artificielles (IA).
- Prendre conscience des traces informatiques laissées sur Internet.
- Sensibiliser à l'impact environnemental des données numériques.

Durée : 50 à 60 minutes.

Le matériel nécessaire (salle informatique)

- Vidéo-projecteur
- Ordinateurs/tablettes avec connexion Internet (au moins 1 pour 2 élèves)
- Outil de recherche inversée d'image
- [Graphique montrant l'augmentation exponentielle du stockage de données dans le monde](#)
- [Banque d'images](#)
- Livret élève.

Plan de la séance

1. La composition d'une image numérique.
2. Les traces invisibles laissées sur Internet.
3. La sobriété numérique et l'explosion des données.

Étape 1 (15 minutes) : La composition d'une image numérique

a) Qu'est qu'une image numérique ? (groupe classe, projection sur tableau, 5 min)

L'enseignant projette l'image « [1. La composition d'une image numérique > a\) Qu'est-ce qu'une image numérique](#) ». Il demande aux élèves de quoi est constituée une image.

Réponses attendues : on peut s'attendre à ce que les élèves partent de ce qu'ils voient directement et décrivent l'image ou bien listent des types d'image (ex. : logos, paysages, portraits, publicités...). L'enseignant doit les amener à formuler l'idée qu'une image est constituée de pixels (données).

Ensuite, l'enseignant oriente les élèves vers les données qui ne sont pas visibles directement (métadonnées). Il les interroge : « Une image est constituée d'autres éléments que l'on ne voit pas directement. Quels sont-ils ? »

Réponses attendues : date, heure, lieu si le GPS est activé, modèle d'appareil utilisé...

En conclusion, l'enseignant vérifie que les élèves ont compris qu'une image numérique est un ensemble de données et de métadonnées.

b) Enquête sur images (groupe de 2 ou 3 élèves, 10 min)

L'enseignant propose aux élèves de réfléchir, par le biais d'une enquête, sur ce que peut nous apprendre la consultation d'un fichier image.

Il projette trois images numériques (« 1. La composition d'une image numérique > b) Enquête sur images ») :

- Image A : une photo contenant des métadonnées complètes (appareil, lieu, date).
- Image B : une photo identique sans métadonnées (modifiée volontairement via un service en ligne gratuit ou une capture d'écran).
- Image C : une image modifiée par IA, sans aucune métadonnée.

Il répartit la classe en groupe de deux ou trois élèves et leur demande de répondre aux questions suivantes à partir des images fournies :

- Où ont-elles été prises ?
- Quand ?
- Par qui ?
- Sont-elles fiables ? Sincères ?

Réponses attendues :

Image A : les métadonnées indiquent que la photo a été prise devant une aire de pique-nique du Futuroscope, le 22/05/2025 par Audrey.

→ Image sincère

Image B : les métadonnées indiquent que la photo aurait été prise devant une aire de jeu, le 05/06/2004 par Arun. Le copyright indique « ville de Chauvigny » et peut induire en erreur sur le lieu de la prise de vue.

→ Image insincère

Image C : aucune métadonnée. L'image originelle a été modifiée : les coussins ont été effacés sur l'image.

→ Image insincère

L'enseignant regroupe ensuite ses élèves et projette les trois photos ainsi que leurs métadonnées. Il mène ensuite les échanges à partir des questions suivantes :

- Qu'avez-vous réussi à deviner ?
- Qu'est-ce qui vous a manqué ?
- Peut-on toujours se fier aux métadonnées ?
- Pourquoi certaines images n'en contiennent-elles pas ?

Pour terminer, l'enseignant interroge les élèves sur les raisons qui pourraient expliquer l'absence de métadonnées sur une image lorsqu'on modifie ou télécharge celle-ci depuis certaines plateformes.

Réponses attendues :

Les métadonnées peuvent être supprimées volontairement pour **protéger la vie privée** (ex : géolocalisation). Ainsi, certains services en ligne retirent les métadonnées **automatiquement**, ou bien **réutilisent les images** sans ces informations (par exemple les agences immobilières en ligne).

Certaines métadonnées peuvent être modifiées, par exemple la localisation pour faire croire qu'une photo a été prise ailleurs. Quand le nom de l'auteur de la photo est changé pour s'approprier une image, c'est une violation du droit d'auteur et c'est également répréhensible.

Des images créées de toutes pièces via une application spécialisée (synthèse d'images, IA...) ne contiennent pas nécessairement de métadonnées.

Cela montre que même si les métadonnées sont utiles, **elles ne suffisent pas toujours pour garantir l'authenticité** ou la sincérité d'une image. Cependant quand elles sont sincères, elles constituent des traces numériques qui permettent d'obtenir des informations sur le contexte d'une image.

Étape 2 (30 minutes) : Les traces invisibles laissées sur Internet

a) Comment laisse-t-on des traces en ligne ? (réflexion collective, 5 min)

L'enseignant interroge ses élèves : **Quelles traces numériques un site web ou une application en ligne collectent-ils lors de votre navigation ?**

Réponses attendues : il y a plusieurs niveaux de collecte :

- sur votre navigateur (quelle application, quelle langue, quelles extensions sont installées...) et sur l'appareil que vous utilisez pour vous connecter (quel système d'exploitation, quelle résolution d'écran...).
- sur votre position via votre adresse IP (celle-ci permet de savoir qui est le fournisseur d'accès à Internet et d'avoir des informations approximatives de localisation).
- sur votre comportement sur le site ou l'application (temps passé sur une page, mouvements de la souris, clics, données saisies dans les champs même s'ils ne sont pas envoyées...).

Si vous autorisez les cookies, un site web ou une application peut en savoir bien davantage sur votre navigation et peut suivre vos activités sur plusieurs pages d'un même domaine. Si vous êtes connecté à certains services comme des réseaux sociaux, tout site qui contient des boutons d'intégration (like, share) est susceptible d'envoyer des informations à ces réseaux sociaux même sans que vous le lui demandiez.

Références :

- <https://amiunique.org/fr> pour découvrir l'empreinte de votre navigateur
- <https://www.cnil.fr/fr/definition/cookie> pour comprendre ce que sont les cookies.

Existe-t-il un moyen de ne laisser aucune trace numérique ? Si oui, avez-vous des exemples ?

Réponses attendues :

- Une option de navigation privée est disponible sur tous les navigateurs. Aucune donnée de navigation n'est alors stockée sur votre machine : ni historique des pages visitées, ni cookies persistants, etc. Vous êtes déconnecté de vos comptes par défaut (notamment vos comptes sur les réseaux sociaux). Cela permet de limiter les traces, pas de les faire complètement disparaître toutefois.
- Un réseau privé virtuel (communément appelé VPN pour Virtual Private Network) offre une protection plus importante en masquant l'adresse IP et en chiffrant les données.

En conclusion, l'enseignant vérifie que les élèves ont compris qu'un site Internet ou une application en ligne enregistre souvent **l'adresse IP, l'appareil utilisé, et d'autres données**, même si on ne laisse aucun commentaire ou publication. Il existe des manières de réduire les traces numériques : navigation privée, utilisation d'un VPN. Voir annexe « Lexique des termes techniques ».

NB. : Il est possible de faire réfléchir les élèves par analogie. Naviguer sur Internet c'est comme laisser une empreinte de pas : même si on ne peut pas deviner ni la marque de la chaussure ni qui l'a laissée, on sait que quelqu'un est passé par là et on peut soit le retrouver en suivant le chemin inverse, soit continuer à le suivre, soit le reconnaître lorsqu'on recroise la même trace de pas ailleurs.

b) Jeu de piste informatique (groupe de 2 élèves, 10 min)

Dans un premier temps, l'enseignant divise sa classe en binômes et fournit à chacun une banque d'images « [2. Les traces invisibles laissées sur Internet > b\) Jeu de piste informatique](#) ». Il donne la consigne : « Nous allons jouer à un jeu de piste informatique. Vous aurez sur votre poste informatique, une banque d'images du Futuroscope et l'objectif est de trouver l'endroit de chacune des photos. Pour cela, vous pouvez utiliser plusieurs méthodes :

- Consulter les métadonnées comme ce que nous avons fait précédemment.
- Utiliser des outils comme OpenStreetMap ou la recherche inversée d'image.

Correction :

Image A : il n'y a pas de réponse précise, cette photo est une introduction. Les métadonnées ci-blent sur une zone proche de Poitiers.

Image B : Entrée Sud de l'aire d'activités économiques des Portes du Futur (métadonnées + visuel).

Image C : Arobase 4, Canopé, Technopole du Futuroscope (métadonnées + visuels).

Image D : morceau du mot "aqu**ASCOpE**" visible + panneaux de signalisation propre au Futuroscope.

Image E : sur le panneau à droite on aperçoit une partie du logo Futuroscope ainsi que le plan du parc. En zoomant, on peut voir "Entrée Futuroscope".

Image F : allée d'entrée aperçue dans l'horizon d'un bâtiment typique du Futuroscope, lettres géantes formant mot visible : **FutUROSCOpe**.

Image G : dans l'arrière-plan à droite : bâtiment typique du Futuroscope, panneau du rond-point qui indique le Futuroscope si on zoom dessus.

Image H : entrée C du Futuroscope (métadonnées + visuels).

A travers cet exercice, les élèves comprennent qu'ils vont se rendre au Futuroscope. L'enseignant informe la classe sur le contenu de leur visite et plus particulièrement sur l'expérience au Campus Numeria.

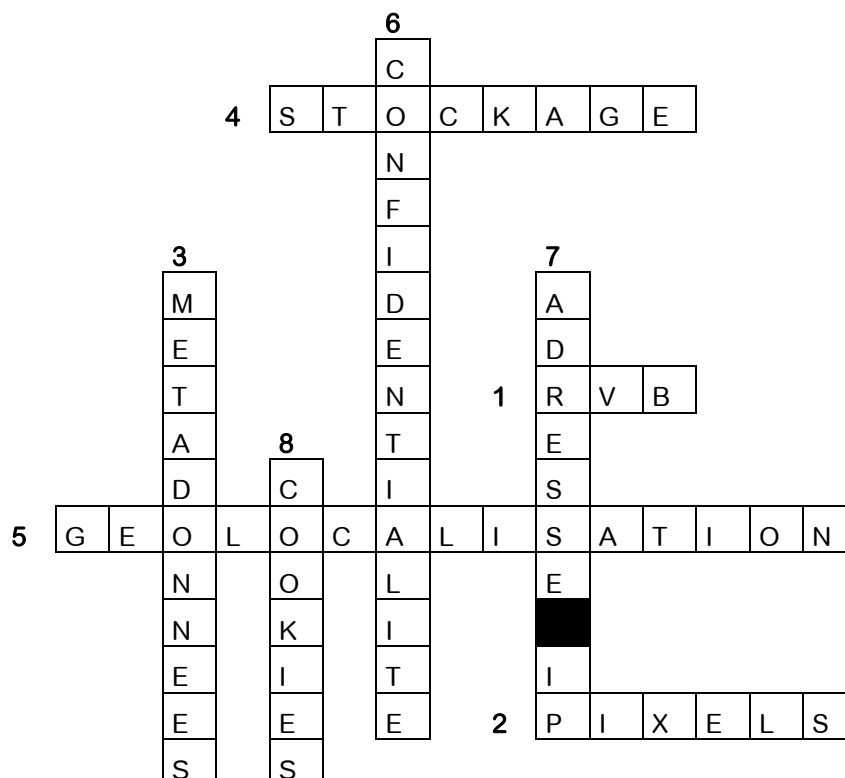
Dans un second temps, l'enseignant questionne les élèves sur le poids des fichiers contenant les images étudiées, et les invite à identifier les différents formats utilisés.

Réponses attendues :

- Taille des images.
- Formats : JPEG haute qualité, JPEG compressé, PNG.

c) Fixation du lexique (travail individuel, entre 5 et 10 min)

A partir du [glossaire](#) distribué par l'enseignant, les élèves complètent les mots croisés, dont la **correction** est la suivante :



Etape 3 : Mes usages numériques (40 minutes)

Ce qui est recherché dans cette étape est une prise de conscience qui pourra amener, après le passage au Campus Numeria, à une modification concrète des pratiques des élèves, dans le sens d'une meilleure protection de la vie privée et d'un usage raisonné des outils numériques.

a) Quelles données numériques est-ce que je laisse en ligne ? (travail individuel, 10 minutes)

Le livret élève contient un tableau vierge nommé « Utilisation quotidienne du numérique » : le remplir permet aux élèves de prendre conscience de manière plus personnelle du temps qu'ils passent en ligne et des informations qu'ils déposent involontairement sur Internet.

Afin que les élèves répondent de la manière la plus complète possible, l'enseignant précise que les rubriques proposées dans le tableau ont pour but d'identifier les pratiques et usages réels pour dépasser les intuitions ou les représentations, qu'il s'agit d'une réflexion personnelle pour préparer l'activité suivante et les réponses ne seront partagées que si l'élève en est d'accord.

b) Mes données, tes données, nos données... (travail en classe entière, 10 minutes)

L'enseignant demande aux élèves à mettre en regard leur tableau individuel et celui qui est complété à titre d'exemple dans le livret élève, et de partager leurs observations : quels points communs ? quelles différences ?

Il anime la discussion et rappelle à cette occasion d'une part l'âge limite à l'utilisation de certains réseaux ou plateformes et d'autre part les bonnes pratiques d'hygiène de vie numérique (cf. : <https://www.elysee.fr/em-manuel-macron/2024/04/30/remise-du-rapport-de-la-commission-dexperts-sur-limpact-de-l'exposition-des-jeunes-aux-ecrans>) Il prend en note au tableau ce qui pourrait constituer des lignes de force afin que les élèves puissent visualiser celles-ci.

NB. Afin d'amorcer l'étape 4 le cas échéant, l'enseignant s'assure en fin d'activité que les élèves ont bien compris la nature diverse et la quantité importante de données collectées à l'échelle individuelle, de la classe, et par extension de leur établissement scolaire, de la commune de celui-ci, du département, de la région, du pays...

c) Une habitude que je voudrais faire évoluer pour mieux protéger mes données (travail individuel, 5 minutes)

L'enseignant invite les élèves à prendre quelques minutes pour repérer une de leurs habitudes qu'ils voudraient faire évoluer, et pourquoi, en lien avec la question des données et les discussions qui ont eu lieu. Il leur demande d'écrire leur réponse dans le livret élève.

d) Que disent nos traces numériques ? (travail individuel, 10 minutes)

Les élèves sont maintenant invités à compléter la première colonne du tableau d'auto-évaluation proposé dans le livret élève dans la partie Troisième temps.

Etape 4 (10 minutes) : Prolongement possible : La sobriété numérique et l'explosion des données

L'enseignant montre le graphique de l'augmentation exponentielle du stockage de données dans le monde, [« activité 4 – sobriété numérique »](#).

Pour aller plus loin sur ce sujet, d'autres données sont consultables en suivant ce lien : How much content is uploaded to the internet per second? - Spectralplex

a) Pourquoi stocke-t-on autant d'images ? (en classe entière, 5 minutes)

La question est posée de façon ouverte aux élèves par l'enseignant. Cette phase sert à ouvrir le questionnaire.

b) Quels sont les impacts du stockage de cette grande quantité d'images sur l'environnement ? (en classe entière, 5 minutes)

On a besoin d'outils numériques pour stocker ces données (serveurs, disques durs, ordinateurs etc...) qui ont besoin de métaux rares (appelés « Terres rares » pour qualifier l'ensemble d'un groupe de métaux) et d'énergie pour fonctionner. Il est possible de prendre appui sur l'une des propositions suivantes :

- La pollution numérique | Minute MAJ, Youtube, Radio Canada 2:38min.
- Cliquer, c'est polluer – Décod'actu, Youtube, Lumni, 3:10min.

Maintenant que les élèves sont prêts et ont acquis les bases, ils vont pouvoir profiter pleinement de l'expérience qu'ils vont vivre au Campus Numeria, où il leur sera demandé d'aider le parc du Futuroscope à retrouver la photographie du parc qui a disparu ! Afin d'introduire le temps 2, la vidéo de présentation du parcours est diffusée en classe...

Prérequis pour la visite au Campus Numeria

- Savoir ce qu'est une métadonnée (information supplémentaire visant à enrichir la donnée elle-même stockée dans le fichier contenant les données) et comment y accéder.
- Connaître la composition d'une image numérique.
- Développer l'esprit critique pour douter méthodiquement de la sincérité d'une image.
- Compléter la première colonne du tableau auto-évaluation du livret élève.
- Avoir constitué les groupes d'élèves (voir tableau dans le temps 2).
- Avoir visionné la vidéo de présentation du parcours pour lancer l'enquête.



Deuxième temps du parcours (au Campus Numeria) : la photographie du Futuroscope a disparu ! Menez l'enquête pour la retrouver.

Objectifs de la séance

- Sensibiliser les élèves aux métadonnées et aux traces que chacun laisse sur Internet.
- Développer son œil critique face à une image (sincérité, véracité, fiabilité...).

Durée totale de l'activité : 2h (accueil, expérience, conclusion).

Ce que vous allez vivre

À votre arrivée au Campus Numeria, vous serez accueillis par un médiateur numérique : il accompagnera la mise en œuvre pédagogique. L'enseignant de la classe et les accompagnateurs seront mobilisés par le médiateur numérique dans le cadre de l'animation des sous-groupes d'élèves (*a minima, 5 adultes sont nécessaires : le médiateur numérique, l'enseignant, et trois accompagnateurs. La présence d'accompagnateurs supplémentaires, si elle n'est pas obligatoire, peut aider à fluidifier la mise en œuvre des ateliers*).

Après une présentation rapide, quatre ateliers éducatifs tournants, d'environ 10 minutes chacun, permettront de confronter les élèves à l'analyse critique des images et de leurs métadonnées. Le professeur de la classe et les accompagnateurs contribuent à l'animation proposée. Chaque atelier se compose de deux activités complémentaires : l'une mobilise du matériel numérique, l'autre s'appuie sur des objets physiques issus du monde physique. Ces deux approches permettent d'illustrer ensemble un même concept.

À mesure de leur progression, les groupes découvrent des indices : à chaque atelier, un caractère spécifique est remis à chaque groupe, distinct selon la couleur du groupe, mais identique pour les deux sous-groupes associés à cette couleur. Cette redondance permet de vérifier la conformité de l'indice. L'ensemble des caractères collectés permettra, une fois réunis, de résoudre le mystère de la disparition de la photographie.

Préparation des groupes avant votre arrivée au Campus Numeria

Groupe 1 (Bleu)	Groupe 2 (Rouge)	Groupe 3 (Jaune)	Groupe 4 (Vert)
Groupe 1a : - - - - -	Groupe 2a : - - - - -	Groupe 3a : - - - - -	Groupe 4a : - - - - -
Groupe 1b : - - - - -	Groupe 2b : - - - - -	Groupe 3b : - - - - -	Groupe 4b : - - - - -

Déroulement des ateliers

Ateliers	1e rotation	2e rotation	3e rotation	4e rotation
Géolocalisation : <u>Objectif</u> : Comparer des sources. <u>Consigne</u> : Replacer des photographies de lieux célèbres sur un planisphère à l'aide des données de géolocalisation. Repérer l'image contenant des données erronées.	Groupe 1a : atelier « physique » Groupe 1b : atelier « numérique »	Groupe 2a : atelier « physique » Groupe 2b : atelier « numérique »	Groupe 3a : atelier « physique » Groupe 3b : atelier « numérique »	Groupe 4a : atelier « physique » Groupe 4b : atelier « numérique »
Vidéo-surveillance : <u>Objectif</u> : Analyser des métadonnées telles que la date et l'heure de la prise de vue. <u>Consigne</u> : Retracer le parcours de la photographie à partir de données temporelles.	Groupe 2a : atelier « numérique » Groupe 2b : atelier « physique »	Groupe 3a : atelier « numérique » Groupe 3b : atelier « physique »	Groupe 4a : atelier « numérique » Groupe 4b : atelier « physique »	Groupe 1a : atelier « numérique » Groupe 1b : atelier « physique »
Stéganographie : <u>Objectif</u> : Exercer son esprit critique face à des métadonnées. <u>Consigne</u> : Mener l'enquête pour trouver des indices cachés dans les photos.	Groupe 3a : atelier « physique » Groupe 3b : atelier « numérique »	Groupe 4a : atelier « physique » Groupe 4b : atelier « numérique »	Groupe 1a : atelier « physique » Groupe 1b : atelier « numérique »	Groupe 2a : atelier « physique » Groupe 2b : atelier « numérique »
Archivage : <u>Objectifs</u> : Comprendre une arborescence numérique. Comprendre l'organisation et le classement d'archives physiques. <u>Consigne</u> : Mener l'enquête en s'appuyant sur les archives numériques et physiques de la photographie.	Groupe 4a : atelier « numérique » Groupe 4b : atelier « physique »	Groupe 1a : atelier « numérique » Groupe 1b : atelier « physique »	Groupe 2a : atelier « numérique » Groupe 2b : atelier « physique »	Groupe 3a : atelier « numérique » Groupe 3b : atelier « physique »

À la fin des quatre ateliers, le médiateur regroupe la classe pour découvrir ensemble où se trouve la photographie disparue.



Troisième temps du parcours (en classe) – Que disent nos traces numériques de nous et de nos proches ?

Objectifs

- Consolider les apprentissages sur les métadonnées et la fiabilité des images.
- Amener les élèves à une réflexion sur leurs propres traces numériques.
- Sensibiliser aux enjeux de vie privée et de maîtrise des données personnelles.
- Explorer des solutions pour un usage plus responsable du numérique.

Durée : 50 à 60 minutes

Matériel nécessaire

- Vidéoprojecteur.
- Accès à Internet et moteurs de recherche (*facultatif*).
- Livret élève.
- Tableau blanc ou application pour afficher des notes.

Déroulé de la séance

1. Retour sur l'expérience au Futuroscope.
2. Mes propres traces numériques.
3. Vers un usage plus responsable du numérique.

Étape 1 – Retour sur l'expérience au Futuroscope (5 min)

L'enseignant demande aux élèves de se rappeler les grandes notions abordées lors de la séance 1 et de les appliquer aux activités du Futuroscope. Il organise un brainstorming :

- Lister les concepts : métadonnées (leur présence ou non), codage des images, adresse IP, cookies, données personnelles.
- Qu'ont-ils appris sur les métadonnées et la manipulation des images ?

Nos traces en ligne peuvent être utilisées pour nous retrouver, voire pour craquer nos mots de passe (cf. mot de passe de la photographie craqué au Campus Numeria).

Conclusion : On laisse des traces au travers de notre navigation. Pour aller plus loin, même sans rien poster soi-même, il existe des données (traces) numériques à notre nom (données administratives, adresse mail liée à l'ENT, données médicales...).

Étape 2 – Mes propres traces numériques (25 min)

Les élèves complètent la deuxième colonne du tableau d'auto-évaluation présent dans leur livret. Ils comparent leurs réponses avec la première colonne. Les élèves volontaires peuvent s'exprimer sur l'évolution de leurs représentations. Cela peut amener à une discussion en classe sur les usages et peut permettre de rappeler les pratiques à prévenir. L'enseignant veille à guider la discussion de façon à faire ressortir les points suivants :

- Ne pas utiliser son identité réelle (nom, prénom, âge etc.).
- Ne pas publier en ligne des contenus de soi sans contrôler leurs visibilité (publics, restreints aux amis, etc.).
- Ne pas accepter les conditions d'utilisation de sites sans comprendre ce à quoi on consent.
- Télécharger, publier ou modifier des images en lignes sur des sites peut donner le droit d'utilisation de votre image à cette plateforme. (cf. point précédent).

- Navigation sans vigilance : les VPN et navigation privée ne suppriment pas totalement vos traces en lignes.
- Ne jamais utiliser le même mot de passe partout. UN service = UN mot de passe.
- Même une image « réaliste » peut ne pas être sincère.
- Supprimer un contenu ne l'efface pas définitivement.
- Stocker des documents sur un serveur en ligne n'est pas écologique.

Pour que ces mises en garde deviennent des habitudes pour les élèves, ils complètent dans leur livret élève les 5 bonnes pratiques à adopter :

1. Protéger son identité.
2. Vérifier ce que l'on voit.
3. Faire attention à ce que l'on partage.
4. Penser aux traces qu'on laisse.
5. Respecter les autres et la planète.

Discussion à la suite (15 min) : Des informations laissées en lignes peuvent-elles être exploitées par d'autres ? Peut-on les contrôler ?

Cette discussion peut prendre la forme d'un débat mouvant dont l'organisation est la suivante :

- Diviser la salle de classe en 2 zones : d'un côté OUI, de l'autre NON (ou « Je suis d'accord », « Je ne suis pas d'accord » avec le fait de mettre des photos en ligne). Les élèves se placent au milieu. La question est posée et les élèves se déplacent dans la zone OUI ou NON selon ce qu'ils pensent.
- L'enseignant questionne ensuite certains élèves sur leur choix.
- À tout moment ils peuvent se déplacer et changer de zone si l'argumentaire d'un de leurs camarades les a convaincus.
- Possibilité de nuance : plus ils se positionnent loin de la ligne du milieu, plus ils ont une position tranchée. Le milieu peut être une zone de neutralité.
- Prendre 1 ou 2 questions des élèves pour continuer le débat.

Réponses :

Pour pouvoir contrôler les traces laissées en ligne, on peut regarder les conditions d'utilisation.

Les traces laissées en ligne peuvent nous enfermer dans des habitudes définies par des préférences déterminées à partir de notre navigation et de nos usages.

On peut demander à récupérer ses données sur n'importe quel service en ligne. On peut saisir la CNIL si on n'arrive pas à les récupérer. Attention, les données récupérées de la sorte peuvent ne pas être intelligibles. Les données restent tout de même sur la plateforme.

Étape 3 - Vers un usage plus responsable du numérique : mise en situation (15 minutes)

Pour conclure ce parcours, une mise en situation sous forme de quiz est disponible dans le livret élève.

Le quiz et sa correction :

Question 1 : Lucie crée un nouveau compte sur un site de jeux en ligne. Elle décide de choisir "Lucie1234" comme mot de passe. Est-ce un bon choix ? Pourquoi ?

- A) Oui, c'est un mot de passe facile à retenir, et c'est suffisant pour protéger son compte.
- B) Non, ce mot de passe est trop simple et facile à deviner. Il est important d'avoir un mot de passe long qui ne veut rien dire pour mieux protéger son compte.
- C) Oui, mais il faut ajouter une question secrète pour renforcer la sécurité.

☒ Réponse correcte : **B**

→ Il ne faut jamais utiliser dans un mot de passe de données personnelles (comme son prénom) ou sa date de naissance... Plus largement, un mot de passe robuste doit être une succession de caractères de différentes natures (lettre minuscule, majuscule, chiffre, symbole) qui n'a aucun sens, que l'on ne peut pas déduire d'informations connues sur la personne qui l'a créé ou que l'on ne peut pas retrouver dans des dictionnaires. En outre, avec la quantité d'informations que l'on peut trouver sur le web concernant une personne, utiliser une question secrète ne permet pas de renforcer la sécurité : souvent la réponse à la question secrète a été mise en ligne par l'utilisateur lui-même ou par un de ses proches (par exemple, pour le nom de jeune fille de la mère, il suffit d'avoir identifié comme cousins des cousins du côté maternel qui ont le même nom de famille)

Question 2 : Iliès veut se connecter à une plateforme (réseau social, jeu en ligne, etc.) et décide de remplir toutes les informations demandées, y compris son adresse postale et sa date de naissance exacte. Pourquoi est-il risqué de partager trop d'informations personnelles, même sur un site que tu penses être sûr ?

- A) Parce que cela peut être utilisé pour du marketing ciblé ou des publicités.
- B) Parce que certaines informations personnelles peuvent être utilisées à des fins malveillantes, comme le vol d'identité.
- C) Risque ou pas, de toute façon, Iliès n'a pas le choix s'il veut utiliser cette plateforme.

☒ Réponses correctes : **A et B et éventuellement C**

→ Ces informations peuvent contribuer à suivre l'internaute et donc à découvrir ses goûts, ce qui permettra de lui envoyer des publicités répondant à ses besoins supposés ou de le soumettre à des publicités liées à des besoins que des personnes avec des profils similaires peuvent avoir. Donner trop d'informations sur soi peut également permettre à un inconnu malveillant de se faire passer pour soi, auprès de proches (envoi de mails frauduleux crédibles) mais aussi pour réaliser des transactions (commerciales par exemple) ou autre action délictueuse.

Pour la réponse C, il faut bien regarder quelles sont les informations indispensables et les informations facultatives. Normalement lorsqu'on crée un compte sur une application, celle-ci ne doit exiger que des informations utiles pour rendre le service associé. Il est logique qu'une application donnant la météo cherche à savoir où l'on est ou qu'une application de généalogie demande le nom de famille. Par contre, il est plus curieux qu'elles demandent à accéder aux contacts de l'utilisateur. Lorsque des informations sont facultatives, il est conseillé de ne pas les fournir à moins d'avoir une bonne raison. Et si une application a des exigences qui paraissent disproportionnées, il est plus prudent de ne pas y créer de compte et d'en trouver une autre plus raisonnable et proposant un service similaire.

Question 3 : Sarah voit une vidéo sur les réseaux sociaux qui affirme qu'une célébrité a fait une déclaration choquante. Elle veut la partager sans attendre. Pourquoi est-il essentiel de vérifier les informations avant de les partager ?

- A) Parce qu'il est possible que la vidéo soit fausse ou manipulée, et la partager sans vérifier peut propager de fausses informations.
- B) Parce que Sarah peut perdre toute crédibilité en diffusant des informations erronées.
- C) Parce que tout le monde pourrait penser à tort que Sarah est bien informée si elle la partage.

✓ Réponses correctes : **A, B**

→ De nombreuses informations erronées circulent sur le web. Il peut s'agir d'erreurs innocentes, de rumeurs malveillantes, de tentatives de manipulation etc. Il faut être capable d'identifier des sources d'information de confiance et ne transmettre une information que lorsqu'elle est attestée par plusieurs sources fiables.

Lorsqu'on republie des informations erronées, il existe plusieurs risques. Le plus grave est de porter atteinte à des personnes et éventuellement de contribuer à les diffamer. Sans aller jusque-là, on risque de perdre soi-même la confiance de son cercle de connaissances si l'information se révèle fausse ultérieurement. Se construire une bonne réputation prend du temps, la perdre peut se faire en un claquement de doigts... ou plutôt en un clic d'un partage trop vite exécuté.

Question 4 : Aaron reçoit un message de son ami qui lui dit que son compte de jeu en ligne a été piraté et qu'il doit immédiatement cliquer sur un lien pour sécuriser son compte. Que devrait-il faire dans cette situation ?

- A) Cliquer sur le lien pour vérifier son compte, ça semble important.
- B) Ignorer le message et vérifier directement sur le site du jeu en ligne si son compte est en danger.
- C) Répondre à l'ami pour lui demander plus de détails avant de prendre une décision.

✓ Réponse correcte : **B**

→ La plupart du temps les mails anxigènes de ce type ne viennent pas d'un ami mais de quelqu'un qui se fait passer pour lui (sans nécessairement avoir eu besoin de pirater son compte). Lorsqu'on passe la souris sur le lien que l'on est supposé cliquer, l'adresse de la page web qui apparaît n'a généralement rien à voir avec le site dont on est supposé devoir protéger l'accès. Dans tous les cas, il ne faut jamais cliquer sur un lien dans un mail sans être absolument sûr de sa provenance.

Dans certains cas, non seulement le pirate se fait passer pour un ami mais il a réellement pris le contrôle de son compte mail. Dans ce cas, il ne sert à rien de lui répondre. Si on veut contacter l'ami en question, il vaut mieux utiliser un autre canal de communication (téléphone, rendez-vous dans le monde physique par exemple).

Si on veut vérifier que tout va bien sur son compte, il faut ouvrir un navigateur et accéder au site en saisissant soi-même l'adresse de la page ou bien en la récupérant dans ses favoris ou dans son historique.

Question 5 : Luna envoie une photo d'elle en maillot de bain sur une application de messagerie, mais la photo finit par être partagée dans un autre groupe. Que peut-elle faire pour éviter cela à l'avenir ?

- A) Partager des photos uniquement avec ses amis les plus proches.
- B) Toujours réfléchir à l'impact potentiel avant de partager des photos personnelles, et vérifier les paramètres de confidentialité.
- C) Mettre des filtres sur ses photos pour les rendre moins reconnaissables.

✓ Réponse correcte : **B**

→ Il faut considérer que toute information envoyée sur Internet peut devenir publique à un moment. Une photo partagée dans un petit cercle de personnes peut être rediffusée par une ou plusieurs d'entre elles volontairement ou par mégarde, avec ou sans intention de nuire.

Appliquer des filtres sur les photos pour les rendre moins reconnaissables ne garantit en rien qu'elles ne puissent pas être retravaillées ultérieurement pour reconstituer tout ou partie des informations modifiées.

Question 6 : Paolo joue régulièrement en ligne avec des amis. Chaque fois que Quentin perd, Paolo prend une capture d'écran et la partage dans un groupe privé pour se moquer de lui. Cette situation dure plusieurs semaines. Quels risques juridiques Paolo encourt-il en partageant cette capture d'écran ?

- A) Il peut être accusé de harcèlement moral en ligne, ce qui est punissable par la loi, et pourrait faire face à des sanctions judiciaires.
- B) Il enfreint la loi sur la protection de la vie privée, en partageant une image sans le consentement de la personne concernée, ce qui peut entraîner des poursuites.
- C) Il n'y a aucun risque juridique, car il est dans un groupe privé et cela ne concerne que des amis.

✓ Réponse correcte : **A et B** (les deux sont valides).

→ Le cyberharcèlement est bien décrit ici : <https://www.service-public.fr/particuliers/vosdroits/F32239>.

Lorsqu'on pense être l'objet de cyberharcèlement, il faut absolument réaliser des captures d'écrans des messages échangés afin d'avoir des preuves et se manifester auprès d'un adulte de confiance ou s'adresser directement aux représentants de l'ordre.

Question 7 : Maïssane poste régulièrement des photos de ses vacances et de ses sorties avec des amis sur son compte Instagram. Un jour, elle décide de supprimer quelques anciennes publications, pensant qu'elles sont oubliées. Est-ce que les traces en ligne peuvent disparaître facilement ?

- A) Oui, dès que tu supprimes une photo, elle est effacée de partout.
- B) Non, même si tu supprimes des publications, elles peuvent avoir été enregistrées ou partagées par d'autres.
- C) Oui, mais seulement si tu les supprimes rapidement après les avoir postées.

✓ Réponse correcte : **B**

→ Il faut toujours lire les conditions des services en ligne que l'on utilise pour savoir comment est géré l'effacement de données, parfois le retrait de la donnée ne signifie pas sa suppression immédiate des serveurs.

Par ailleurs lorsqu'une donnée (une photo par exemple) est mise en ligne, elle peut être récupérée par une des personnes qui y a accès et être republiée indépendamment ailleurs. La suppression de la photo sur le compte de la première personne qui l'a postée n'a aucune incidence sur la copie de la photo présente sur le compte d'une autre personne.

Dès qu'une donnée est mise en ligne, elle échappe en partie au contrôle de celle ou celui qui l'a postée.

Question 8 : Léo reçoit un message sur un réseau social d'une personne qui se présente comme étant un de ses amis. Cette personne lui demande de partager son mot de passe ou de lui donner des informations personnelles, sous prétexte qu'elle a un "problème urgent" et qu'elle ne peut pas accéder à son propre compte. Quel risque Léo prend-il en partageant ses informations personnelles avec cette personne ?

- A) Léo risque de devenir victime d'usurpation d'identité, car quelqu'un pourrait se faire passer pour lui et utiliser ses informations à mauvais escient.
- B) Léo n'encourt aucun risque, car son ami a simplement besoin d'aide et il lui fait confiance.
- C) Léo doit simplement changer son mot de passe pour éviter tout problème, mais il n'y a pas d'autre danger.

✓ Réponse correcte : **A**

→ Si Léo n'a pas donné son mot de passe il n'a pas besoin de le changer.

On ne doit divulguer un mot de passe à personne ni d'ailleurs demander un mot de passe à quiconque. Lorsque quelqu'un dispose des identifiants de connexion d'un autre, il peut se connecter sur le service en ligne concerné avec ces identifiants et se faire passer pour l'autre. Toutes les actions qu'il fera seront attribuées à l'autre. Ainsi s'il commet un délit, par exemple en pratiquant du cyberharcèlement sur une tierce personne, c'est la personne dont il a volé l'identité qui sera poursuivie. Il est parfois difficile de prouver qu'il y a bien eu usurpation d'identité.

Question 9 : Ezio voit un post sur les réseaux sociaux où quelqu'un se moque d'un autre élève. Il se rend compte que cela peut blesser la personne visée. Comment peut-il réagir face à ce genre de situation pour montrer du respect envers l'autre ?

- A) Ignorer le post et passer à autre chose.
- B) Signaler le post comme inapproprié et exprimer son soutien à la personne moquée.
- C) Liker le post pour montrer qu'il est d'accord avec ce que la personne a écrit.

☒ Réponse correcte : **B**

→ Dans la vie numérique comme dans la vie « physique », il est important de venir en aide à celles et ceux qui sont victimes de moqueries, harcèlement ou autres actes malveillants. On ne sait jamais quel impact une agression en ligne peut avoir sur quelqu'un. Ne rien dire pourrait être assimilé à de la non-assistance à personne en danger. Lorsqu'on constate une situation anormale et potentiellement dangereuse pour la victime, il est indispensable de la signaler à un adulte de confiance.

Question 10 : Mélanie adore passer du temps à regarder des vidéos en ligne et à télécharger des séries. Un jour, elle apprend que le fait de regarder des vidéos en streaming ou de télécharger des fichiers consomme énormément d'énergie et a un impact sur l'environnement. Que pourrait faire Mélanie pour réduire son empreinte écologique tout en continuant à profiter de ses vidéos préférées ?

- A) Mélanie peut regarder des vidéos en streaming sans s'inquiéter de l'impact écologique, car cela ne lui coûte rien personnellement.
- B) Mélanie pourrait télécharger des vidéos et les regarder hors ligne pour limiter la consommation d'énergie à chaque lecture.
- C) Mélanie pourrait limiter son utilisation des écrans et privilégier d'autres activités pour réduire son empreinte écologique.

☒ Réponses correctes : **B et C**

→ Certains coûts ne sont pas visibles, soit parce qu'ils sont endossés par d'autres (l'abonnement au service de streaming a un coût financier supporté par les adultes du foyer), soit parce que ce sont des coûts indirects qui n'ont pas d'impact évident à court terme. L'explosion du numérique et notamment du transfert et du stockage de grands volumes de données (images, vidéos etc.) a un coût écologique que nos sociétés paieront tôt ou tard : coût en matériaux et en énergie pas tous renouvelables. Un usage raisonné du numérique laissant la place à d'autres types d'activités par exemple est un moyen pour chacun de contribuer à la protection de la planète.