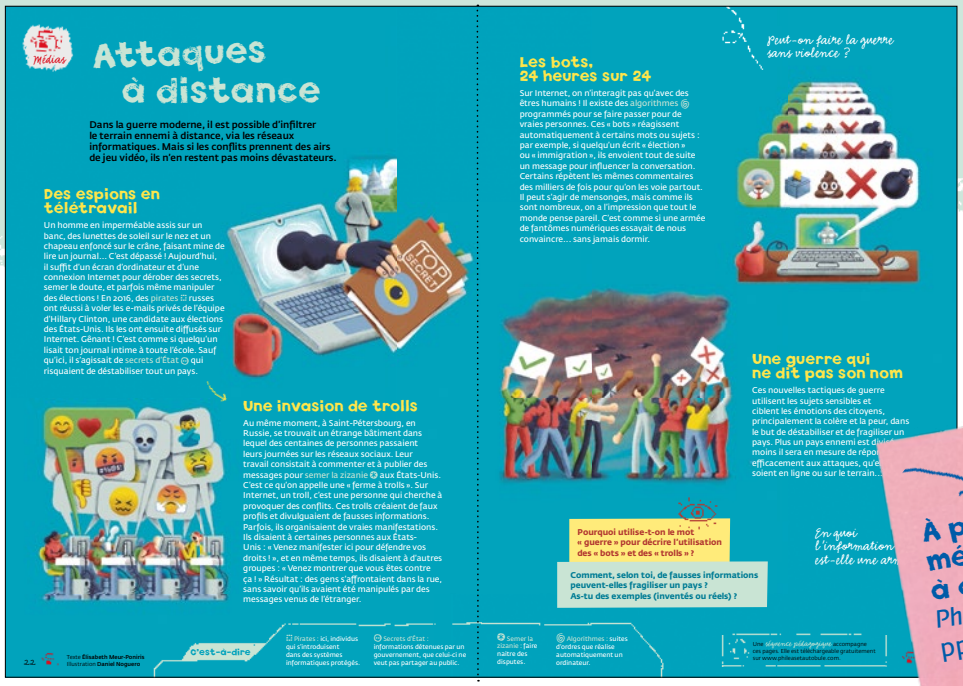
Séquence médias

Bataille de données : touchées… ou protégées ?

Autrice : Élisabeth Meur-Poniris (institutrice primaire et animatrice en éducation aux médias)



Attaques à distance

Dans la guerre moderne, il est possible d'infiltrer le terrain ennemi à distance, via les réseaux informatiques. Mais si les conflits prennent des airs de jeu vidéo, ils n'en restent pas moins dévastateurs.

Des espions en télétravail

Un homme en imperméable assis sur un banc, des lunettes de soleil sur le nez et un chapeau enfoncé sur le crâne, faisant mine de lire un journal… C'est dépassé ! Aujourd'hui, il suffit d'un écran d'ordinateur et d'une connexion internet pour dérober des secrets, semer le doute, et parfois même manipuler des élections ! En 2016, des pirates ☒ russes ont réussi à voler les e-mails privés de l'équipe d'Hillary Clinton, une candidate aux élections des États-Unis. Ils les ont ensuite diffusés sur internet. Gênant ! C'est comme si quelqu'un lisait ton journal intime à toute l'école. Sauf qu'ici, il s'agissait de secrets d'État ⓒ qui risquaient de déstabiliser tout un pays.

Une invasion de trolls

Au même moment, à Saint-Pétersbourg, en Russie, se trouvait un étrange bâtiment dans lequel des centaines de personnes passaient leurs journées sur les réseaux sociaux. Leur travail consistait à commenter et à publier des messages pour semer la zizanie ❷ aux États-Unis. C'est ce qu'on appelle une « ferme à trolls ». Sur Internet, un troll, c'est une personne qui cherche à provoquer des conflits. Ces trolls créaient de faux profils et divulguaient de fausses informations. Parfois, ils organisaient de vraies manifestations. Ils disaient à certaines personnes aux États-Unis : « Venez manifester ici pour défendre vos droits ! », et en même temps, ils disaient à d'autres groupes : « Venez montrer que vous êtes contre ça ! » Résultat : des gens s'affrontaient dans la rue, sans savoir qu'ils avaient été manipulés par des messages venus de l'étranger.

Les bots, 24 heures sur 24

Sur Internet, on n'interagit pas qu'avec des êtres humains ! Il existe des algorithmes ⓖ programmés pour se faire passer pour de vraies personnes. Ces « bots » réagissent automatiquement à certains mots ou sujets : par exemple, si quelqu'un écrit « élection » ou « immigration », ils envoient tout de suite un message pour influencer la conversation. Certains répètent les mêmes commentaires des milliers de fois pour qu'on les voie partout. Il peut s'agir de mensonges, mais comme ils sont nombreux, on a l'impression que tout le monde pense pareil. C'est comme si une armée de fantômes numériques essayait de nous convaincre… sans jamais dormir.

Peut-on faire la guerre sans violence ?

Une guerre qui ne dit pas son nom

Ces nouvelles tactiques de guerre utilisent les sujets sensibles et ciblent les émotions des citoyens, principalement la colère et la peur, dans le but de déstabiliser et de fragiliser un pays. Plus un pays ennemi est divisé, moins il sera en mesure de répondre efficacement aux attaques, qu'elles soient en ligne ou sur le terrain…

Pourquoi utilise-t-on le mot « guerre » pour décrire l'utilisation des « bots » et des « trolls » ?

Comment, selon toi, de fausses informations peuvent-elles fragiliser un pays ? As-tu des exemples (inventés ou réels) ?

En quoi l'information est-elle une arme ?

c'est-à-dire

☒ Pirates : ici, individus qui s'introduisent dans des systèmes informatiques protégés.

ⓒ Secrets d'État : informations détenues par un gouvernement, que celui-ci ne veut pas partager au public.

❷ Semer la zizanie : faire naître des disputes.

ⓖ Algorithmes : suites d'ordres que réalise automatiquement un ordinateur.

Une séquence pédagogique accompagne ces pages. Elle est téléchargeable gratuitement sur www.phileasetautobule.com.

Texte Élisabeth Meur-Poniris
Illustration Daniel Noguero

À partir des pages médias « Attaques à distance »
Philéas & Autobule n°97, pp. 22-23.

Objectifs

- Comprendre ce que sont les données personnelles
- Identifier les risques liés au partage d'informations en ligne
- Découvrir des stratégies de protection

Durée
2 x 50 minutes

Âge
De 10 à 13 ans

Matériel

- Une fiche « bingo des données personnelles » (annexe 1, p. 19) par enfant.
- Deux « plateaux de jeu » (annexe 2, p. 20) par groupe de 4 enfants.
- 6 jetons « données personnelles » et 3 jetons « boucliers » (annexe 3, p. 21) par groupe de 4 enfants.

Compétences du Conseil Supérieur de l'Éducation aux Médias[1]

Compétences techniques en écriture

- Choisir un dispositif technique en tenant compte des possibilités de confidentialité, de sécurité, de propriété intellectuelle, de pérennité, ... qui lui sont liées.

Compétences sociales en écriture

- Comprendre le contexte dans lequel l'utilisateur a écrit le message.
- Repérer les risques que l'utilisateur prend dans le contexte.
- Protéger son identité et ses données personelles quand c'est nécessaire.
- Faire la part des choses entre ce qui est recevable par les destinataires sur le plan privé, le plan public et le plan professionnel.

Compétences du référentiel d'Éducation à la philosophie et à la citoyenneté[2]

4. DÉVELOPPER SON AUTONOMIE AFFECTIVE

Savoir-faire

➲ **Préserver son intimité, son intégrité et celle des autres.**

- Questionner et dégager des pratiques pour préserver sa sécurité, son identité numérique et son intimité sur internet (P5 à S2).

Savoirs

➲ **Intimité**

- Questionner-expliciter ce qui révèle de l'intimité (P5 à S2).

1 Publiées dans *Les compétences en Éducation aux médias, un enjeu éducatif majeur*, édité par le Conseil Supérieur de l'Éducation aux Médias, 2016, www.csem.be. Notre sélection, non exhaustive, indique les principales compétences mobilisées dans cette séquence.

2 Issues du *Référentiel d'éducation à la philosophie et à la citoyenneté* publié par la Fédération Wallonie-Bruxelles (2022) sur le site www.enseignement.be. La numérotation correspond aux titres et sous-titres du référentiel. Notre sélection, non exhaustive, indique les principales compétences mobilisées dans cette séquence.

PRÉPARATION

L'animateur lit l'article médias « Attaques à distance », ainsi que le déroulement présenté dans les pages qui suivent.

Il tente de réaliser lui-même les exercices et explore personnellement les questionnements qu'il s'apprête à proposer aux enfants.

L'animateur imprime et découpe les annexes à distribuer aux enfants.

DÉROULEMENT

1. DÉCOUVERTE DE L'ARTICLE ET FOCUS SUR L'ASPECT « DONNÉES PERSONNELLES » (SÉANCE 1 – 50 MIN)

1.1. Exploration (5 min)

À partir des pratiques numériques des enfants, l'animateur initie un brainstorming en leur posant les questions suivantes : *« Partagez-vous régulièrement des choses sur Internet ? Est-ce qu'un inconnu pourrait savoir des choses sur vous rien qu'avec ce que vous postez ou likez ? Vous renseignez-vous parfois sur ce que vos amis ou des personnes moins proches suivent ou likent ? »*

Si certains enfants se révèlent être peu connectés, voici quelques variantes permettant d'alimenter la conversation : *« Est-ce qu'il vous arrive de deviner des choses sur vos camarades rien qu'en observant leurs habits, leur sac ou ce qu'ils disent en classe ? Quand vous jouez à un jeu, est-ce qu'il vous est déjà arrivé de choisir un pseudo ou un avatar ? Que dit ce surnom sur vous ? Est-ce que vous gardez parfois des choses pour vous, que vous ne voulez pas partager avec tout le monde ? Pourquoi ? »*

1.2. Lecture de l'article et mise en perspective des risques d'exploitation des informations personnelles (20 min)

L'animateur interroge les enfants : *« Finalement, quel est le problème à parler de qui nous sommes ou de ce que nous aimons ? Quels risques pourrions-nous encourir ? »*

Conseil à l'animateur
Un enfant pourrait parler de pédocriminalité : un adulte malveillant pourrait utiliser des informations personnelles sur un enfant pour gagner sa confiance. L'animateur peut rebondir sur cet exemple en soulignant le fait qu'il s'agit également de manipulation : on crée un sentiment de proximité mais qui n'est ni sincère ni authentique.

Après avoir relevé quelques hypothèses éventuelles, l'animateur propose aux enfants de parcourir l'article ensemble.

Avant d'entamer la lecture, l'animateur note au tableau les mots du lexique suivant et s'assure que les enfants en aient une bonne compréhension. Durant la lecture, l'animateur pourra marquer un stop pour attirer l'attention des enfants vis-à-vis du lexique.

Lexique
- Dérober : prendre quelque chose en cachette, sans demander.
- Divulguer : révéler ou dire une information qui devait rester secrète.
- Interagir : agir avec quelqu'un, échanger ou réagir ensemble.
- Déstabiliser : troubler, surprendre ou mettre mal à l'aise.
- Fragiliser : rendre plus faible, moins solide.

L'animateur demande à tour de rôle à un enfant de lire le paragraphe. À la fin de chaque paragraphe, il demande au groupe de relever les mots-clés, qu'il note au tableau.

Mots-clés éventuels
- Paragraphe « Des espions en télétravail » : espions - pirates - secrets - publier
- Paragraphe « Une invasion de trolls » : réseaux sociaux - conflits - mensonges - affrontements
- Paragraphe « Les bots, 24 heures sur 24 » : robots - messages automatiques - nombreux
- Paragraphe « Une guerre qui ne dit pas son nom » : sujets sensibles - émotions - tactiques de guerre

Si nécessaire, l'animateur peut expliquer aux enfants ce qu'est un mot-clé : *« Dans une phrase, on pourrait dire que le mot-clé est celui qui - comme une clé - permet d'ouvrir la porte pour ensuite comprendre ce dont on parle. Le mot-clé résume l'essentiel de ce qu'il faut retenir. »*

À la fin de la lecture de l'article, l'animateur repart des mots-clés relevés et demande aux enfants d'expliquer les informations importantes du texte.

Réponses éventuelles
- Les données personnelles d'une personne peuvent être utilisées contre elle comme une attaque : on peut ridiculiser quelqu'un, rabaisser ses opinions.
- On peut utiliser les données personnelles de quelqu'un pour la pousser à réagir : en agissant sur les sujets que l'on sait sensibles, on peut déclencher des émotions vives.
- Sur Internet, beaucoup d'interactions sont automatisées : le moindre message peut être détecté par un robot programmé pour y réagir d'une certaine manière.

1.3. Le bingo des données personnelles (15 min)

L'animateur distribue une fiche de bingo (annexe 1, p. 19) à chaque enfant et demande de la remplir avec les informations suivantes :
- Son plat préféré
- Sa chaîne YouTube préférée
- Son sport préféré
- Sa couleur favorite
- Son lieu préféré
- Son animal de compagnie / animal préféré

Cette fiche doit rester anonyme.

L'animateur relève les fiches, les mélange puis les redistribue aux enfants qui lisent individuellement la fiche reçue puis tentent à tour de rôle de deviner qui en est l'auteur, en mettant en avant les indices qui leur ont mis la puce à l'oreille.

L'animateur demande aux enfants d'imaginer une publicité dont l'auteur de la fiche pourrait être la cible.

Conseil à l'animateur
Si le temps est limité, l'animateur peut tirer lui-même au hasard quelques fiches et demander au groupe d'en identifier les auteurs.

2. JEU DE PLATEAU ET FOCUS SUR L'ASPECT « OUTILS POUR SE PROTÉGER » (SÉANCE 2 - 50 MINUTES)

2.1. Rappel de la séance précédente (5 min)

L'animateur demande aux enfants de rappeler les apprentissages importants de la séance précédente :
- Lorsque l'on poste du contenu sur Internet, on donne des informations sur qui nous sommes, ce que nous aimons.
- Ces informations sont appelées « données personnelles ».
- Certaines personnes peuvent utiliser nos données personnelles pour nous manipuler, nous amener à acheter des produits ou nous faire croire à des idées fausses.

L'animateur demande aux enfants si depuis la dernière séance, ils ont été confrontés à de nouveaux exemples de ciblage de données personnelles : « *Depuis la dernière séance, avez-vous remarqué des situations où vos données personnelles semblaient utilisées ?* »

Pour orienter les enfants, l'animateur peut proposer des exemples : « *une publicité qui correspondait exactement à ce que vous aviez cherché, une vidéo recommandée qui ressemblait beaucoup à ce que vous regardez, ou un message qui semblait fait pour vous.* »

2.2. Réflexion autour des actions possibles pour protéger nos données personnelles (5 min)

L'animateur oriente à présent la discussion sur la manière dont on peut protéger ses données personnelles et tente de dégager avec les enfants les premières connaissances qu'ils possèdent sur des stratégies de protection.

« *Maintenant, réfléchissons ensemble : connaissez-vous déjà des façons de protéger vos données personnelles sur Internet ? Quelles idées ou astuces pouvez-vous proposer ?* »

Les enfants proposeront probablement les moyens de protection les plus usités : un mot de passe, un code, limiter les paramètres de confidentialité aux amis les plus proches, faire attention à ce que l'on publie.

Conseil à l'animateur
La réalité est plus complexe : les paramètres de confidentialité ont un effet auprès du public mais pas sur les algorithmes publicitaires des réseaux sociaux, par exemple. À ce stade, l'animateur peut se contenter de ces stratégies de protection simples et décider de revenir par la suite plus en détails sur les nuances à apporter au sujet.

2.3. Lancement du jeu de plateau (20 min)

L'animateur informe les enfants qu'ils vont maintenant exercer leurs nouvelles connaissances à travers un jeu de plateau.

Il demande aux enfants de former des groupes de 4. Dans chaque groupe, il y aura deux équipes : deux enfants auront le rôle d'utilisateurs et deux autres auront le rôle de « bots ».

L'animateur demande aux enfants s'ils se rappellent ce qu'est un « bot » : « *c'est un robot programmé pour réagir d'une certaine manière à un message.* »

L'animateur distribue les plateaux et les jetons et détaille les règles du jeu :
- Les utilisateurs disposent de 6 jetons « données personnelles » avec différents types de données. Ils bénéficient également de 3 jetons « boucliers » pour protéger certaines de ces données.
- Comme dans le jeu bataille navale, les utilisateurs placent leurs données personnelles sur un plateau, caché par une séparation (farde, cahier ...). Ils disposent également les boucliers au-dessus des données qu'ils veulent protéger. L'autre équipe, qui joue le rôle de bots et dispose du même plateau, doit essayer de les trouver.
Les bots annoncent une case, par exemple *B4*. Si l'équipe des utilisateurs a placé une donnée sur cette case, elle dit « touché ! ». Si elle a un bouclier, la donnée est protégée. Si la case est vide, l'équipe des utilisateurs dit « dans l'eau ».
- Le but des bots est de récolter un maximum de données. Le but des utilisateurs est de les protéger.
- La partie se termine lorsque les utilisateurs n'ont plus de boucliers ou que toutes les données personnelles non protégées ont été trouvées par les bots.

2.4. Une règle d'or pour protéger ses infos (20 min)

Lorsque les deux équipes ont chacune mené une partie, l'animateur invite les enfants à une discussion collective. Ce moment permet de revenir sur les stratégies utilisées : quelles données ont été protégées en priorité, par quels moyens et pourquoi.

Pour clôturer la séance, l'animateur propose une activité créative permettant aux enfants de formaliser ce qu'ils ont appris. Chaque enfant est invité à imaginer une « règle d'or » pour protéger ses informations personnelles. Cette règle peut prendre différentes formes : un slogan accrocheur, une petite bande dessinée, une affiche colorée ou encore une phrase simple mais percutante.

L'animateur peut donner quelques exemples pour inspirer les enfants, comme : « Un mot de passe fort = une maison bien fermée ».

Les productions des enfants sont ensuite mises en valeur : affichées dans la classe, dans le couloir ou dans un espace commun de l'école, elles servent de rappel visuel et collectif des bonnes pratiques à adopter sur Internet.

PROLONGEMENTS

DÉBRIEF SUR LES RISQUES DE L'EXPOSITION ET LES RÉFLEXES À ADOPTER POUR SE PROTÉGER

Si l'animateur souhaite prolonger la problématique, il peut profiter d'une discussion collective pour complexifier le débat et l'ancrer dans la réalité. Il explique que, dans la vraie vie, la protection ne se limite pas à cocher quelques paramètres de confidentialité. Les algorithmes des réseaux sociaux parviennent parfois à contourner ces réglages et continuent de récolter des informations. De plus, un mot de passe simple ne suffit pas : il doit être complexe, et il est essentiel de ne pas utiliser le même mot de passe pour tous ses comptes.

Enfin, l'animateur attire l'attention sur des données encore plus sensibles, comme les empreintes digitales ou la reconnaissance faciale, souvent utilisées pour déverrouiller les appareils. Si ces données venaient à être piratées, les risques seraient particulièrement importants, car elles sont uniques et impossibles à changer.

ANNEXE 1
BINGO DES DONNÉES PERSONNELLES

Mon plat préféré	Ma chaine Youtube préférée
Mon sport préféré	Ma couleur favorite
Mon lieu favori	Mon animal de compagnie ou mon animal préféré

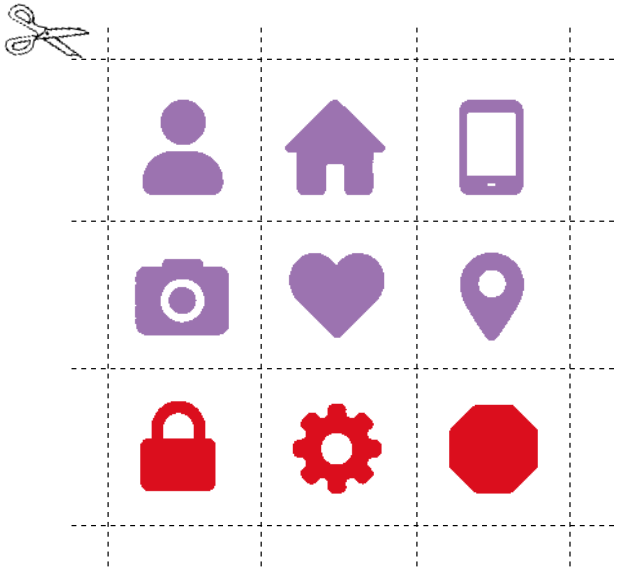
ANNEXE 2
PLATEAU DE JEU

	A	B	C	D	E	F
1						
2						
3						
4						
5						
6						

Données personnelles

- Nom et prénom
- Adresse
- Numéro de téléphone
- Photo personnelle
- Goûts et préférences
- Localisation

Boucliers

- Mot de passe
- Paramètres de confidentialité
- Vigilance

ANNEXE 3
JETONS