DOSSIER ENSEIGNANTS

Acti Média

#1 PIXEL Mag

À la trace des données personnelles dans le numérique

Un dossier pédagogique pour (re)prendre le contrôle sur nos données personnelles

csem

FÉDÉRATION WALLONIE-BRUXELLES

rtbf.be

Autorité de protection des données

Cette brochure est le fruit de la collaboration de membres du CSEM, de l'Autorité de la protection des données (APD) et de la RTBF.

Rédaction :
Cassiopée Henaff

Comité d'accompagnement :
Romane Bomal - APD
Véronique Desloover - CECP
Sébastien Grau- CSEM
Damien Haenecour - CSEM
Alyson Hernalesteen - UNamur
Stéphane Hoebeke - RTBF
Delphine Mignon - WBE
Anne-Charlotte Recker - APD
Jade To Thanh - APD
Patrick Verniers - CSEM

Éditrice responsable :
Claire Berlage - CSEM

CSEM
Boulevard Léopold II, 44 – 6E630
1080 Bruxelles
csem.be
Mail : csem@cfwb.be

Août 2025 - Les références des ressources proposées dans cet ouvrage sont correctes à la date de parution.

conseil supérieur de l'éducation aux médias
csem

FÉDÉRATION WALLONIE-BRUXELLES

rtbf.be

Autorité de protection des données

Sommaire

La collection

Actimédia est une collection d'outils produite par le Conseil Supérieur de l'éducation aux médias. Elle propose des outils qui s'adressent directement aux élèves de l'enseignement obligatoire, fondamental et secondaire.

Actimédia vient en complément de la collection « Tronc commun » qui propose des activités pour travailler les attendus d'EAM présents dans l'ensemble des référentiels

Le format d'Actimédia est hybride : outre une version imprimée de l'outil, à exploiter dans un mode « débranché », le site internet du CSEM (csem.be), contient un certain nombre d'activités liées à la thématique. Enfin, des contenus audiovisuels, créés en collaboration avec la RTBF, peuvent également venir compléter l'exploitation de la thématique.

Cette collection est également le fruit de collaborations nouées entre le CSEM et des acteurs experts dans la thématique abordée par chacun des numéros.

Ainsi, le numéro pilote sur la protection des données a été réalisé en collaboration avec l'Autorité de la protection des données (APD).

Nous espérons que cette collection rencontrera les besoins du terrain et répondra au mieux aux attendus d'éducation aux médias à travailler avec les élèves.

Bienvenue dans PIXELMag, le journal où les élèves deviennent de véritables reporters !

Ce dossier propose une série d'activités immersives et interactives pour explorer les traces laissées en ligne, comprendre la collecte et l'utilisation des données personnelles et analyser les mécanismes derrière le ciblage des profils.

À travers des missions ludiques et participatives, les élèves enquêteront, recouperont des indices et produiront du contenu journalistique autour du numérique et de la protection des données personnelles.

Mais ce dossier va bien au-delà de la sensibilisation ! Il s'inscrit dans une véritable démarche de conscientisation, donnant aux jeunes les moyens de reprendre le contrôle sur leurs données personnelles et leurs usages du numérique. Apprendre à maîtriser ses données personnelles, ce n'est pas seulement protéger ses mots de passe ou refuser les cookies. C'est aussi et surtout comprendre comment et pourquoi les informations sont collectées, faire des choix éclairés et développer une posture critique sur ce que l'on partage, avec qui et dans quel but.

Grâce aux différentes missions de cet outil, les élèves développeront des réflexes concrets pour une navigation plus autonome et plus responsable.

Note préliminaire

La protection des données : un droit fondamental, un droit humain !

Le droit à la protection des données personnelles est un droit fondamental garanti par la Charte des droits fondamentaux de l'Union européenne ou encore par la Convention européenne des droits de l'Homme. Il relève plus généralement du droit au respect à la vie privée.

S'agissant d'un droit fondamental, il n'est pas absolu, c'est-à-dire qu'il peut être restreint ou encadré dans certaines situations. Il doit donc être mis en balance avec d'autres droits fondamentaux comme la liberté d'expression ou la liberté de religion par exemple.

La protection des données personnelles ne relève pas seulement des données personnelles contenues dans le numérique. Elle concerne toute information qui permet d'identifier directement ou indirectement une personne physique. Cela peut être le nom, le prénom, le pseudonyme, l'adresse IP, la carte d'identité, l'empreinte digitale, la photo, la vidéo, la plaque d'immatriculation, les habitudes alimentaires ou encore la religion.

Le Règlement Général sur la Protection des Données (RGPD) est un des textes réglementaires européens qui harmonisent le droit fondamental à la protection des données dans toute l'Union européenne.

Protection pour qui, responsabilité de qui ?

L'objectif principal du RGPD est de protéger les données personnelles de toute personne concernée (par exemple, les enseignant·e·s, les parents, les enfants, etc.), avec une protection spécifique pour l'utilisation des données personnelles des enfants.

Ce règlement indique qu'une protection spécifique pour les jeunes est nécessaire car ils·elles sont moins conscient·e·s des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel.

La responsabilité d'une conformité au RGPD et au droit à la protection des données repose en amont sur toute personne qui traite des données personnelles. On pense par exemple aux responsables du site ou des réseaux sociaux utilisés, aux écoles, aux autorités publiques, etc. En cas de non-conformité aux obligations, ce sont ces responsables qui risquent des sanctions, par exemple des amendes élevées.

Considération sur l'âge

Cet outil est à destination d'un public jeune de 6e primaire et de 1re secondaire. Cependant, en Belgique, l'âge légal pour s'inscrire sur des réseaux sociaux ou des plateformes de jeux vidéo (qu'on appelle aussi sous le terme générique de services de la société de l'information), est fixé à 13 ans. Ce n'est donc qu'à partir de cet âge qu'un·e enfant peut s'inscrire **seul·e** sur ces plateformes. Avant cet âge, l'enfant pourra s'inscrire uniquement moyennant l'accord du titulaire de l'autorité parentale (parents ou tuteurs).

Il est aussi à noter que l'âge de 13 ans ne vaut que pour l'inscription auprès des services de la société de l'information. Bien entendu, s'il s'agit de signer un contrat d'achat, un contrat à la souscription d'un abonnement,

l'âge légal reste en règle générale 18 ans. Le·la jeune ne pourra donc conclure un contrat que moyennant l'accord des titulaires de l'autorité parentale (parents ou tuteur·rice·s).

La responsabilité de la vérification de l'âge revient aux responsables qui traitent les données personnelles. Ceux-ci doivent mettre en place tous les moyens garantissant que le jeune ait l'âge requis pour s'inscrire et pour le protéger en ligne.

PIXEL Mag, c'est quoi ?

- **Une immersion narrative et journalistique :** les élèves ne sont pas de simples apprenant·e·s, mais plutôt des reporters du *Pixel Mag*, un journal scolaire consacré aux enjeux du numérique. À travers des missions journalistiques, les jeunes mènent l'enquête sur la collecte de données, analysent des indices et produisent du contenu pour éclairer leurs lecteurs et lectrices.

  D'ailleurs, toutes les investigations menées par les élèves aboutissent à la création d'un véritable journal, où se retrouveront des articles, analyses et conseils sur la protection des données personnelles. Cette production peut être réalisée sur papier ou en version numérique.

- **Un apprentissage actif et positif de la maîtrise des données personnelles :** ce dossier adopte une approche équilibrée loin de dramatiser ou culpabiliser, il met en lumière les opportunités et les risques du numérique. Chaque mission engage les élèves dans une démarche active permettant de reprendre le contrôle sur leurs données personnelles, de paramétrer leurs outils numériques et de naviguer en ligne de manière plus consciente et éclairée.

- **Une déconnexion avant tout, avec des liens vers le numérique :** toutes les activités peuvent être réalisées sans matériel numérique complexe, ce qui facilite leur mise en œuvre en classe. Cependant, certaines missions invitent les élèves à utiliser des outils numériques existants, notamment pour explorer leurs propres traces en ligne ou expérimenter la gestion de leurs données.

- **Un lien école-maison pour prolonger les apprentissages :** les réflexions amorcées en classe peuvent se poursuivre à la maison, en famille et avec les proches, grâce à des activités de prolongement qui permettent d'élargir la discussion sur la protection des données et le numérique.

- **Un format flexible et adaptable :** L'approche de cet outil repose sur une structure pédagogique modulaire qui permet aux enseignant·e·s d'adapter les activités en fonction du temps disponible et des besoins de leur classe. L'activité de base dure 100 minutes (mission 1) et constitue le cœur du dispositif. Les missions suivantes abordent chacune un aspect clé de la collecte et de l'exploitation des données. D'une durée de max. 45 min., elles peuvent être réalisées dans l'ordre souhaité, selon les intérêts des élèves ou le temps disponible.

- **Une mission = une production :** chaque mission aboutit à une production concrète qui s'intègre dans une rubrique spécifique du *Pixel Mag* permettant aux élèves de construire un journal collectif, enrichi par leurs analyses, leurs conseils et leurs découvertes sur le numérique. Au fil des séances, les élèves créeront plusieurs rubriques, chacune correspondant à un format journalistique différent (interviews, tests, courriers des lecteurs et lectrices…)

Objectifs de l'outil sous l'angle de la protection des données

Cet outil n'est pas un exposé juridique du RGPD. Il a pour but de faire prendre conscience de la notion de donnée personnelle au sens large, de prendre conscience de son empreinte numérique, des conséquences et risques du partage de ses données personnelles et, ainsi, d'accompagner les jeunes à adopter de bons réflexes.

Le projet s'adresse principalement aux élèves de 6e primaire et 1re secondaire, en les considérant comme de futur·e·s acteur·rice·s du numérique, utilisateur·rice·s et personnes dont les données sont collectées, et non comme des responsables de la gestion des données.

Dans certains cas, pour faciliter la compréhension du cadre juridique, des obligations légales qui incombent aux responsables de sites internet seront brièvement présentées.

Enfin, le vocabulaire utilisé a été simplifié pour le rendre accessible à la fois aux enseignant·e·s et aux jeunes. Par exemple, on utilise le mot « donnée personnelle » tandis que le RGPD utilise la notion « donnée à caractère personnel ».

Objectifs d'éducation aux médias

Durant ce parcours, les élèves seront amené·e·s à :

- **Comprendre ce qu'est une donnée personnelle** et comment elle est collectée et utilisée, aussi bien en ligne que dans la vie quotidienne.
- **Se préparer à l'autonomie dans la gestion de leurs données personnelles en ligne**, avant l'âge légal pour s'inscrire sur un service de la société de l'information comme un réseau social (13 ans en Belgique).
- **Identifier les lieux et les mécanismes de collecte de données**, que ce soit sur Internet, via des applications, ou à travers des documents administratifs et des objets connectés.
- **Expérimenter les effets concrets de la collecte de données** (ex.: publicités ciblées, recommandations personnalisées, bulles de filtre) et analyser leur impact sur leurs données personnelles et leur vie privée.
- **Développer un regard critique sur les pratiques numériques** et leurs influences, en adoptant une approche journalistique et analytique.
- **Connaître leurs droits pour protéger leurs données personnelles et leur vie privée** et comprendre les obligations des plateformes et des organisations en matière de traitement de leurs données personnelles.
- **Collaborer et réfléchir collectivement** en échangeant leurs analyses et en construisant des connaissances partagées sur ces enjeux.
- **Exercer leur autonomie numérique en adoptant des réflexes concrets** pour sécuriser leur profil en ligne et protéger leurs données personnelles, limiter la collecte excessive et faire des choix éclairés sur ce qu'ils·elles partagent en ligne.

Attendus disciplinaires travaillés (Domaines d'apprentissage)

Cet outil s'adresse principalement aux élèves de 6e primaire et 1re secondaire.

Les attendus listés ci-après figurent dans les référentiels du Tronc commun et sont travaillés dans les différentes missions.

Discipline	Année(s)	Savoir/Savoir-Faire/Compétence	Attendu
Éducation à la philosophie et à la citoyenneté	**P3 à S3**	Préserver son intimité, en ce compris son intégrité (S-F)	Questionner et dégager des pratiques pour préserver sa sécurité, son identité numérique et son intimité sur Internet et les réseaux sociaux
Formation historique, géographique, économique et sociale	**S1**	Les rapports sociaux. L'identité numérique (S)	Identifier des modes de présentation de soi et de relation aux autres sans l'espace numérique et leurs effets sur soi et sur les autres.
Formation manuelle, technique, technologique et numérique	**P6**	Vocabulaire spécifique à la protection des données (S)	Utiliser adéquatement les termes de sauvegarde, cookie, hameçonnage, spam, piratage, cyberattaque, antivirus, mot de passe, authentification
		Effacer les traces sur un document partagé (S-F)	Effacer ses fichiers personnels sur un document partagé
		Prévenir et limiter les risques relatifs à la protection des données (C)	Adopter un comportement responsable relatif à la protection des données
	S1	Vocabulaire spécifique à la protection des données (S)	Utiliser adéquatement, en contexte les termes de profil, protection de la vie privée
		Effacer les traces sur un document partagé (S-F)	Effacer toute trace de connexion sur un équipement partagé
		Paramétrer les options de confidentialité d'un compte (S-F)	Paramétrer les options de confidentialité d'un compte
		Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles (S-F)	Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles

Listes des missions (timing, objectifs, durée)

Discipline	Durée	En termes d'éducation aux médias, l'élève est amené à…	Quelle rubrique dans le Pixel Mag ?
Mission 1 : Portraits connectés	**2 x 50 min**	▪ Analyser ses traces numériques et celles des autres ▪ Comprendre ce qu'est une donnée personnelle. ▪ Comprendre la collecte des données à partir des usages numériques. ▪ Questionner les enjeux de l'identité numérique. ▪ Préparer le jeune à son autonomie dans la gestion de ses données personnelles ▪ Avoir conscience de la valeur de ses données personnelles et de leur réutilisation.	**Rubrique** « Interviews - focus » **Description :** Les élèves, en groupe, reconstituent et complètent l'interview d'un·e élève volontaire, en reliant des indices numériques collectés à ses usages quotidiens.
Mission 2 : Quand c'est gratuit, c'est toi le produit	**50 min**	▪ Adapter son comportement en ne partageant que les données personnelles nécessaires. ▪ Avoir conscience de la valeur de ses données personnelles et de leur réutilisation. ▪ Distinguer les informations personnelles à protéger de celles partagées. ▪ Adopter une posture critique face aux formulaires et aux conditions d'utilisation. ▪ Se positionner et prendre des décisions éclairées selon son profil numérique.	**Rubrique :** Test interactif de type magazine **Description :** Les élèves complètent un test permettant aux lecteur·rice·s de découvrir leur profil numérique et de recevoir des conseils adaptés.

Discipline	Durée	En termes d'éducation aux médias, l'élève est amené à…	Quelle rubrique dans le Pixel Mag ?
Mission 3 : Tu as des droits… Utilise-les !	**50 min**	▪ Pouvoir rechercher la politique de confidentialité d'un site. ▪ Identifier ses droits en matière de protection des données et les obligations des plateformes. ▪ Formuler des réponses argumentées à des situations réelles. ▪ Exercer une démarche citoyenne en revendiquant ses droits à la protection des données.	**Rubrique :** Le courrier des lecteurs et des lectrices **Description :** Les élèves reçoivent des courriers fictifs de jeunes ayant des problèmes liés à leurs données personnelles et y répondent en mobilisant les droits et obligations des plateformes.
Mission 4 : Forteresse numérique	**50 min**	▪ Détecter les faiblesses dans les paramètres des comptes en ligne. ▪ Expérimenter des stratégies concrètes pour sécuriser ses comptes en ligne et protéger ses données personnelles. ▪ Visualiser et représenter les risques numériques à travers une météo de cybersécurité. ▪ **Développer une posture critique face aux paramètres des plateformes.**	**Rubrique :** bulletin météo **Description :** Les élèves analysent des profils numériques fictifs et identifient leurs failles de sécurité. Ensuite, ils·elles attribuent un bulletin météo de prévisions du web.
Mission 5 : Réinvente ton feed	**50 min**	▪ Comprendre le fonctionnement des algorithmes et leurs impacts. ▪ Expérimenter des stratégies pour diversifier son fil d'actualité. ▪ Produire un guide interactif pour sensibiliser aux bulles de filtres et au ciblage publicitaire.	**Rubrique :** Lifestyle **Description :** Les élèves conçoivent un challenge en 7 jours pour sortir de sa bulle algorithmique.

Impliquer pour conscientiser

L'objectif de ce dossier est de permettre aux élèves d'analyser leurs usages numériques, de comprendre les mécanismes de collecte des données et de développer une posture active et critique face à ces enjeux. Le rôle de l'encadrant·e n'est pas d'interdire ou d'alarmer, mais de les guider dans cette réflexion, en créant un espace de dialogue et d'expérimentation.

Quelques repères pour animer les missions :

- **Poser des questions plutôt que donner des réponses :** au lieu d'affirmer « *Les réseaux sociaux collectent trop d'infos* », demandez « *Pourquoi Snapchat veut-il ton numéro de téléphone ?* ». Laisser les élèves faire leurs propres déductions renforce leur esprit critique.
- **Encourager une réflexion sur leurs propres pratiques :** plutôt que d'imposer une bonne conduite numérique, aidez-les à identifier ce qu'ils·elles acceptent ou refusent en fonction de leurs propres valeurs et besoins.
- **Jouer sur l'expérimentation :** les missions ne sont pas des leçons théoriques. Elles permettent de tester, observer, comparer. Suggérez-leur d'explorer un feed sans algorithmes, de naviguer en mode privé, ou de modifier leurs paramètres pour en mesurer l'impact.
- **Créer un climat de confiance et éviter le jugement :** certain·e·s partagent beaucoup en ligne, d'autres sont très prudent·e·s. L'important est de ne pas stigmatiser, mais d'amener chacun·e à prendre conscience des risques et des alternatives.
- **Accepter que les usages des jeunes soient différents des vôtres :** ne partez pas du principe que les élèves « *ne font pas attention* ». Leur rapport au numérique est différent mais pas forcément naïf : écoutez-les, échangez et adaptez le dialogue à leurs réalités.

Votre rôle est celui d'un·e médiateur·rice, pas d'un juge ni d'un·e donneur·euse de leçons, mais bien un·e guide qui aide les élèves à décoder le numérique, à prendre conscience que leurs données personnelles ont de la valeur, à reprendre le contrôle sur celles-ci. La conscientisation sur la maîtrise des données personnelles leur permet de mieux protéger leurs comptes, leur identité et leurs traces numériques en particulier en cas d'abus dans l'utilisation future de leurs données personnelles.

Certaines actions dans ce dossier demandent peu d'effort, tandis que d'autres nécessitent une réflexion plus approfondie et une invitation à questionner ses pratiques numériques. Les missions proposées couvrent un large éventail d'actions, allant d'ajustements simples (modifier ses paramètres de confidentialité) à des choix plus radicaux (utiliser un réseau social qui respecte la vie privée). L'objectif est de leur faire prendre conscience de leur marge de manœuvre et de leur permettre d'agir à leur propre rythme.

Des parcours d'apprentissage adaptables

L'enseignant·e peut personnaliser le parcours en fonction du niveau et des connaissances de ses élèves. Chaque mission est pensée pour être autonome, tout en s'appuyant sur les acquis de la mission 1.

Même si chaque mission peut être réalisée individuellement après la mission 1, l'ensemble des missions forment un tout cohérent et progressif, permettant aux élèves d'élargir progressivement leur compréhension des enjeux liés aux données personnelles et à la vie numérique.

Exemples de parcours

Parcours	Quelles missions ?	Durée	Objectifs
Parcours complet	**Missions 1, 2, 3, 4 et 5**	**6 x 50 min**	Offrir une vision globale des enjeux de la protection des données Comprendre les mécanismes de collecte des données personnelles, leurs usages (publicité, algorithmes, recommandations…), ainsi que les moyens concrets de sécuriser leurs informations et de reprendre le contrôle sur leur navigation en ligne.
Comprendre ses empreintes numériques, le sort de ses données personnelles en ligne	**Missions 1 et 2**	**3 x 50 min**	Amener les élèves à prendre conscience des traces numériques laissées en ligne : ce parcours leur permet de comprendre comment leurs informations sont collectées et utilisées, et de développer un regard critique sur leur propre empreinte numérique.
Exercer ses droits	**Missions 1 et 3**		Comprendre comment les données personnelles sont collectées et exploitées. Exercer les droits numériques et les obligations des plateformes et découvrir comment agir.
Sécuriser ses comptes et protéger ses données personnelles	**Missions 1 et 4**		Sensibiliser à la collecte des données personnelles et aux bonnes pratiques numériques : les élèves identifient les principales failles de sécurité sur les réseaux sociaux et les plateformes en ligne. Expérimenter des stratégies concrètes pour mieux protéger leurs comptes et données personnelles.
Comprendre la réutilisation des données personnelles et trouver des moyens pour stopper les contenus ciblés	**Missions 1 et 5**		Décrypter le rôle des algorithmes dans la personnalisation des contenus. Prendre conscience de l'influence des algorithmes et expérimenter des stratégies pour diversifier le fil d'actualité et élargir les sources d'information.

Prolongations

Les missions en classe permettent aux élèves de découvrir comment leurs données personnelles sont collectées et utilisées. Mais comprendre, c'est aussi agir ! L'éducation aux médias numériques ne s'arrête pas à la prise de conscience : elle passe aussi par la capacité à reprendre le contrôle sur ses propres données et à faire des choix éclairés dans un monde où tout est tracé, analysé et souvent monétisé.

La conscientisation sur la maîtrise des données personnelles dans le numérique, c'est l'ensemble des réflexes et stratégies qui permettent de protéger sa vie privée et de garder une autonomie face aux outils numériques. Cela permet d'être capable de choisir en conscience ce que l'on partage et avec qui, de savoir où chercher les informations, comprendre les mécanismes qui influencent nos usages et de tester des alternatives.

Cette conscientisation vise à impliquer les élèves :

- Au niveau individuel → Prendre des habitudes simples : sécuriser ses mots de passe, ajuster ses paramètres de confidentialité, questionner ses usages.
- Au niveau collectif → Sensibiliser ses proches, partager ses connaissances, aider d'autres à mieux protéger leurs données.
- Au niveau citoyen → Interroger les pratiques des plateformes, comprendre ses droits, s'informer sur les lois qui régissent la protection des données et les pratiques commerciales du numérique.

Les défis proposés, à la suite de chacune des missions, sont conçus pour expérimenter des actions concrètes, seul·e ou en famille, et prolonger la réflexion amorcée en classe. Ils permettent d'appliquer les notions abordées à des situations réelles, en explorant ses propres usages et ceux de son entourage.

Chaque prolongation suit une même structure :

- Observer : Identifier ses propres pratiques et celles de son entourage.
- Analyser : Comprendre les implications et les enjeux liés aux données personnelles.
- Agir : Adopter des réflexes concrets pour limiter la collecte de données et renforcer son autonomie numérique.

Mission 1

Portraits connectés

Cadre théorique sur la protection des données personnelles

Qu'est-ce qu'une donnée personnelle ?

Chaque jour, des milliards d'informations sont partagées sur Internet. Parmi celles-ci, il y a des données qui permettent de nous identifier directement ou indirectement. Ce sont nos données personnelles. Cela peut être notre prénom, nom, date de naissance, visage, voix, adresse IP, etc. D'autres données personnelles peuvent être collectées également à travers notre navigation, nos commentaires ou nos likes sur les réseaux sociaux.

Il y a aussi des données personnelles dites « données sensibles », à savoir la religion, l'état de santé, les opinions politiques, l'appartenance syndicale, l'orientation sexuelle ou encore des données biométriques (comme l'empreinte digitale, l'ADN, l'iris de l'œil). La collecte de données sensibles est interdite sauf dans certains cas, par exemple moyennant le consentement explicite de la personne.

Toutes ces données que nous partageons renseignent sur notre identité, nos valeurs, nos passions, nos proches, etc.

Contexte de la mission

Aujourd'hui, chaque geste en ligne laisse une trace, qu'il s'agisse d'un simple like sur Instagram, d'un achat sur un site ou d'un trajet enregistré sur une application de navigation. Pourtant, nous avons rarement conscience de la quantité de données personnelles que nous partageons au quotidien, volontairement ou non.

En Belgique et en Europe, il existe un cadre à la protection de ces données personnelles : le Règlement général sur la protection des données (RGPD). Ce dernier prévoit une protection accrue des jeunes car ils sont moins conscient·e·s des risques du partage de leurs données personnelles.

Contexte de la mission

Dans cette mission, les élèves reçoivent une lettre d'Isabelle Moreau, rédactrice en chef du Pixel Mag. Elle leur explique que l'équipe du journal a rencontré un problème technique : plusieurs interviews d'élèves volontaires ont été partiellement effacées à la suite d'un bug. Pour sauver l'article, les journalistes en herbe vont devoir mener l'enquête et reconstituer ces interviews en analysant les indices disponibles.

Durant cette mission, les élèves doivent donc explorer les traces numériques et physiques laissées par ces élèves pour compléter les informations manquantes. Ils découvriront que nos données sont collectées par une multitude d'acteurs, aussi bien en ligne (réseaux sociaux, applications) que hors ligne (écoles, magasins, lieux publics…). En recoupant toutes ces informations, l'objectif est de prendre conscience que chaque donnée, même anodine, contribue à dresser un portrait détaillé de notre identité et de nos habitudes.

Durant cette activité, l'élève sera amené·e à :

- **comprendre ce qu'est une donnée personnelle et comment elle est collectée :** identifier les différentes informations considérées comme des données personnelles et découvrir les mécanismes de collecte, en ligne et hors ligne ;
- **se préparer à son autonomie dans la gestion de ses données personnelles en ligne**, avant l'âge légal pour s'inscrire sur un service de la société de l'information (13 ans en Belgique) ;
- **prendre conscience de l'impact des traces numériques sur l'identité et la vie privée :** analyser comment des données, même anodines, peuvent être croisées pour dresser un portrait précis d'une personne ;
- **expérimenter des stratégies d'enquête et de reconstitution d'informations :** travailler comme de véritables journalistes en recoupant des indices pour reconstituer des interviews, renforçant ainsi leur capacité d'analyse et de vérification de l'information ;
- **réfléchir sur ses propres usages numériques et sa responsabilité en ligne :** inciter les élèves à prendre du recul sur leurs propres habitudes, à adopter des réflexes plus conscients et à faire des choix éclairés sur ce qu'ils·elles partagent en ligne.

Rubrique visée : interviews - focus

Durée : 2 x 50 minutes

Matériel :

- **Dans le « dossier élèves » :**
  - Le mail d'Isabelle Moureau
  - Interviews de chaque élève

Documents numériques (disponible sur le site du CSEM) :

- Indices numériques (8 par élève)
- Cartes « lieux de collecte » (4 cartes par élève)

Déroulement (2 x 50 minutes)

Cette mission est construite comme une véritable enquête journalistique. À travers l'analyse d'indices numériques et physiques, les élèves découvrent comment les données personnelles sont collectées, croisées et exploitées.

L'activité suit cinq grandes étapes :

TEMPS 1

Découverte

20 min

L'enseignant·e divise la classe en 4 sous-groupes, chacun étant responsable d'un·e élève volontaire ayant fourni des données numériques fictives.

Chaque groupe reçoit :

- la lettre de la rédactrice en chef Isabelle Moreau expliquant leur mission ;
- une fiche vierge d'interview (format à trous) correspondant à un·e élève volontaire ;
- une série de captures d'écran liées aux activités numériques de cet·te élève (réseaux sociaux, plateformes utilisées, apps préférées, etc.) ;

Pour s'assurer que chacun·e a bien compris sa mission, l'enseignant·e peut réexpliquer le contexte : l'enregistreur de la rédaction a buggé, effaçant certaines parties des interviews. Les élèves doivent donc reconstituer des interviews à trous en analysant les indices fournis.

Remarque : le nombre de sous-groupes dépendra du nombre d'élèves. Pour que chacun·e puisse prendre une part active à l'activité, les groupes ne dépasseront pas 4 élèves. S'il le faut, deux groupes peuvent traiter les données d'un même profil d'élève.

TEMPS 2

Analyse et reconstitution des interviews ⏳ 30 min

Les élèves commencent par examiner attentivement les captures d'écran et les indices disponibles pour identifier les habitudes numériques de leur élève (réseaux sociaux utilisés, applications favorites, lieux fréquentés, etc.). À partir de ces indices, les élèves complètent la fiche d'interview en formulant des réponses crédibles qui correspondent aux informations disponibles.

L'enseignant·e peut passer entre les groupes pour poser des questions et les aider à faire des liens entre les indices et les questions posées dans l'interview.

TEMPS 3

Distribution des cartes « Lieux de collecte » ⏳ 15 min

Après 30 minutes d'analyse, les traces numériques ne suffisent pas toujours à reconstituer un portrait complet. En effet, de nombreuses données personnelles sont également collectées hors ligne, par exemple dans les administrations, les hôpitaux, les magasins ou encore les centres sportifs.

L'enseignant·e distribue donc à chaque groupe 4 cartes « Lieux de collecte » tirées au hasard. Ces cartes représentent différents endroits où des informations personnelles sont recueillies. Les élèves ont donc 15 minutes pour :

- Analyser les cartes reçues et déterminer si elles correspondent aux habitudes et au profil de leur élève volontaire.
- Échanger leurs cartes avec d'autres groupes, si nécessaire, afin d'obtenir les 4 cartes liées au lieu le plus pertinent pour leur élève.
- Examiner les indices au verso des cartes pour identifier les nouvelles informations collectées dans ces lieux.
- Compléter l'interview en intégrant ces nouvelles données issues de la vie hors ligne.

TEMPS 4

Collaboration et mur des données

20 min

Ce moment permet aux élèves de conscientiser l'impact de la collecte de données à grande échelle. Si, individuellement, certaines informations peuvent sembler insignifiantes, analysées collectivement, elles révèlent des tendances et des corrélations intéressantes. Ce principe est justement utilisé dans des domaines comme la publicité ciblée, la politique ou l'influence numérique par exemple.

Pendant que les élèves finalisent de compléter leur interview, l'enseignant·e affiche les 6 catégories de données, chacune sur une feuille, afin de différencier les catégories de données personnelles collectées :

- Le genre de l'élève
- L'âge de l'élève
- La ville où l'élève habite
- Les deux applications préférées de l'élève
- Les deux activités ou hobbies principaux de l'élève
- Les deux lieux les plus fréquentés par l'élève

Une fois les interviews finalisées, l'enseignant·e invite chaque groupe à tour de rôle à partager ses découvertes pour compléter les feuilles, construisant ainsi une visualisation collective des données.

L'enseignant·e invite ensuite la classe à prendre du recul et à observer l'ensemble des données collectées et guide la réflexion avec des questions :

- **Quels sont les points communs entre les élèves ?** Y a-t-il des tendances qui se dégagent ?
- **Quelles informations, mises en commun, permettent de deviner d'autres éléments sur un groupe ?** Par exemple, les hobbies et les applications préférées peuvent donner des indices sur le mode de vie d'un élève.
- **Les données personnelles collectées en ligne sont-elles les mêmes que celles collectées hors ligne ?** Quels types de données sont accessibles sans même utiliser Internet ?

Cette discussion permet aux élèves de comprendre qu'en croisant plusieurs sources d'informations, il est possible de dresser un portrait détaillé d'une personne ou d'un groupe, et ce, sans qu'il·elle s'en rende compte.

TEMPS 5

Discussion

15 min

Si cette mission amène les élèves à se glisser dans la peau d'un·e autre et à analyser des traces numériques extérieures, il est essentiel qu'ils·elles puissent ensuite recentrer la réflexion sur eux-mêmes. Ce temps de discussion leur permet d'examiner leur propre rapport aux données personnelles et de prendre conscience des traces qu'ils·elles laissent, volontairement ou non, dans leur usage quotidien du numérique.

L'enseignant·e est invité·e à susciter le débat en se référant au cadre théorique sur la notion de données personnelles.

Pour garantir un cadre bienveillant et favoriser une discussion ouverte, une fois le cadre bienveillant posé avec le groupe (voir « impliquer pour conscientiser » dans l'introduction), l'enseignant·e peut lancer la discussion à partir des questions suivantes. Elles permettent de lancer une (ou toutes les) activité(s) du dossier :

- Pour voir si vous avez bien compris cette mission 1, pouvez-vous me donner une définition de ce qu'est une donnée personnelle ?
- Dans cette mission, vous avez analysé les traces numériques de quelqu'un d'autre. Si vous aviez été à la place des élèves volontaires, auriez-vous été à l'aise avec le fait que vos propres données soient examinées ? Pourquoi ?
- Avez-vous déjà pris le temps de réfléchir aux traces que vous laissez en ligne ?
- Sur quelles plateformes ou applications pensez-vous partager beaucoup d'informations sur vous?
- Quelles données, parmi les vôtres, considérez-vous comme sensibles ou personnelles et ne voudriez-vous pas qu'on collecte ?
- À l'inverse, quelles données personnelles pourraient être récoltées sans que cela ne vous pose de problème ? Pourquoi ?
- Dans cette mission, nous avons vu que les données ne sont pas uniquement collectées en ligne. À votre avis, quelles traces laissez-vous dans votre vie quotidienne hors ligne ? (Exemple : carte de fidélité, abonnement de transport, badge scolaire, dossier médical, etc.)
- Avez-vous déjà été surpris·e par une publicité ou une suggestion de contenu qui semblait « trop bien vous connaître » ?

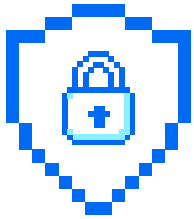
Notes


Une courte vidéo reprend les éléments essentiels à retenir de cette mission 1:

Mission 2

Quand c’est gratuit, c’est toi le produit

Contexte théorique sur la protection des données



Les données partagées

Dans un monde où l'échange d'information est omniprésent, les élèves partagent quotidiennement des données personnelles (voir mission 1). Que ce soit sur les réseaux sociaux, en s'inscrivant sur une plateforme ou même en remplissant un formulaire scolaire, ils·elles partagent une série d'informations qui les concernent et qui leur sont demandées et ne se rendent pas toujours compte de la quantité de données partagées. Pourtant, ces données ne sont pas toujours nécessaires et le partage n'est pas sans conséquence.

Mais finalement, pour quelles raisons les données personnelles sont collectées ? À quelles fins sont-elles utilisées ? Lorsqu'un·e élève s'inscrit sur un site ou une application, on lui demande souvent une série d'informations. Certaines sont obligatoires, mais d'autres sont facultatives, voire excessives. Par habitude, les jeunes (et nous aussi) remplissent tous les champs sans distinction. L'objectif de cette activité est donc de les sensibiliser à la protection et à la valeur des données personnelles ainsi qu'à la préservation de la vie privée.

Même si la plupart des plateformes sont d'apparence « gratuites », elles ne le sont pas vraiment. En échange d'un service gratuit, nous partageons nos données personnelles qui sont souvent très précieuses pour les plateformes et les publicitaires.

Un message clé : en dire le moins possible, ne partager que ce qui est strictement nécessaire et toujours réfléchir avant de communiquer une information. À travers des mises en situation et des exemples concrets, nous allons les aider à comprendre que la protection de leur vie privée passe également par le partage des informations personnelles : partager moins c'est aussi se protéger !

L'idée n'est pas de faire peur aux jeunes, mais de leur faire prendre conscience qu'ils·elles ont le pouvoir de limiter ce qu'ils·elles partagent notamment en adoptant le bon réflexe de se demander si une information est vraiment nécessaire avant de la communiquer.

Les bases de licéité, la finalité et le principe de minimisation des données

Tout traitement de données à caractère personnel doit reposer sur l'une des 6 bases légales prévues par le RGPD. Contrairement aux idées reçues, le consentement n'est pas la seule base de licéité possible. En effet :

- Soit la personne dont on traite les données a donné son consentement ;
- Soit, le traitement de données est nécessaire :
  - à l'exécution d'un contrat ;
  - au respect d'une obligation légale ;
  - à la sauvegarde des intérêts vitaux d'une personne ;
  - à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
  - aux fins d'un intérêt légitime.

Tout traitement de données doit répondre à une finalité précise et la base légale est déterminée en fonction de cette finalité.

Une fois que la finalité et la base de licéité sont déterminées, il y a également lieu de respecter les autres principes de protection des données dont le principe de minimisation des données. En vertu de ce principe, les données à caractère personnel doivent être utilisées de manière adéquate, pertinente, et limitée à ce qui est nécessaire pour atteindre la finalité.

Pour plus d'informations sur les bases juridiques : voir le site de l'autorité de la protection des données (autoriteprotectiondonnees.be).

Pourquoi certaines informations sont-elles obligatoires, facultatives et certaines même excessives ?

- Une donnée est obligatoire si elle est pertinente et strictement nécessaire pour atteindre l'objectif poursuivi. En d'autres mots, ce sont les données dont l'organisation (comme la plateforme en ligne ou l'école) a absolument besoin pour permettre à l'utilisateur·rice d'utiliser le service.
- Une donnée est facultative si elle n'est pas indispensable. On peut donc les fournir si on le souhaite comme par exemple fournir une photo de profil, communiquer nos centres d'intérêt. Le fait de ne pas fournir ces données ne nous empêche pas d'accéder au service.

Comment distinguer un champ obligatoire d'un champ facultatif ? Souvent, l'organisation le signifiera. Par exemple, elle peut marquer le champ d'une (*) et indiquer en bas du formulaire que ces champs sont obligatoires.

- Une donnée est considérée comme excessive lorsqu'elle n'est pas strictement nécessaire pour atteindre l'objectif du service, mais qu'elle est tout de même imposée à l'utilisateur·rice pour y accéder. On peut prendre l'exemple de l'obligation de fournir une photo de profil pour utiliser un réseau social.

Obligation de transparence et politique de confidentialité

Le RGPD impose une série d'obligations aux responsables de traitement, notamment une obligation de transparence. Les responsables qui traitent les données doivent toujours expliquer d'une façon accessible comment et pourquoi ils le font. Il y a différentes manières d'assurer cette information, notamment avec une politique de confidentialité. Avant de créer un profil, de finaliser une inscription ou encore avant de donner son consentement, il est toujours vivement recommandé de la lire.

En effet, en parcourant la politique de confidentialité, les personnes concernées (ici les jeunes) apprendront :

- qui collecte les données et comment contacter cette personne ;
- quelles sont les données collectées (nom, e-mail, localisation, historique de navigation, etc.) ;
- dans quel but les données sont collectées (publicité, administration, liste de membres, paiements…) ;
- si les données sont transférées à d'autres personnes (des tiers) ;
- la durée de conservation des données ;
- quels sont les droits des utilisateur·rices (comment faire rectifier ou supprimer des données erronées, comment retirer un consentement) ;
- comment porter plainte auprès de l'Autorité de protection des données.

En bref, la politique de confidentialité explique comment l'entreprise collecte, utilise et protège les données personnelles des utilisateur·rices. Celle-ci n'est pas à confondre avec la politique de cookies qui explique comment et pourquoi les cookies sont utilisés.

Les cookies, eux, sont des « mini fichiers » qui peuvent être placés sur un appareil connecté à Internet, comme un ordinateur, un téléphone, une tablette ou encore une télévision intelligente. Les cookies peuvent être utilisés pour recueillir ou stocker des informations sur la manière dont vous vous comportez sur (un site) Internet et/ou sur votre appareil. La « lecture » de ces cookies permet ensuite aux sites web qui les ont placés de récupérer les informations stockées. Les sites Internet ou les applications mobiles qui souhaitent installer et/ou lire des cookies sur un de vos appareils connectés à Internet doivent vous expliquer ce que font ces cookies et pourquoi ils veulent avoir recours à leur placement et/ou à leur lecture. Les sites ou les applications doivent vous demander votre consentement, sauf s'ils n'utilisent que des « cookies strictement nécessaires ».

Contexte de la mission

Cette mission se déroule en trois temps :

- **Un moment en grand groupe :** L'enseignant·e guide une réflexion collective à partir de deux cas concrets de formulaires à remplir (contact PMS et réseaux sociaux). L'objectif est de conscientiser les jeunes sur les données qu'ils·elles partagent : l'information partagée est-elle vraiment nécessaire ?
- **Un moment individuel :** chaque élève remplit un test magazine qui l'aide à identifier son propre rapport à la collecte de données personnelles. Une grille d'analyse permet ensuite de découvrir son profil : spontané·e (profil « téméraire »), stratège (profil « pragmatique ») ou furtif·ve (profil « prudent »).
- **Un moment en sous-groupes :** les élèves sont réparti·e·s en trois groupes, chacun chargé de rédiger la description d'un profil type. Ce travail leur permet d'explorer les avantages et les limites de chaque posture numérique, tout en produisant du contenu destiné à être publié dans *Pixel Mag*.

En fin de mission, les élèves auront acquis une meilleure compréhension de la collecte de données en ligne et pourront appliquer ces connaissances pour faire des choix éclairés au moment de remplir des formulaires ou de créer des comptes sur des plateformes numériques.

Durant cette activité, l'élève sera amené·e à :

- **prendre conscience que les données personnelles ont de la valeur ;**
- **comprendre la distinction entre les données obligatoires, les données facultatives et les données excessives :** identifier les différentes informations demandées lors d'une inscription et analyser leur pertinence en fonction du service proposé ;
- **prendre conscience des stratégies des plateformes numériques :** explorer comment certaines données facultatives sont collectées à des fins commerciales, publicitaires ou de personnalisation du service ;
- **développer une posture critique face à la collecte de données :** apprendre à questionner la nécessité des informations demandées et à faire des choix éclairés ;
- **rédiger un contenu pédagogique et engageant :** transformer les apprentissages en un outil de sensibilisation destiné aux lecteur·rice·s du *Pixel Mag* ;
- **encourager une réflexion sur le partage éclairé :** réfléchir à ses propres pratiques en termes de partage de données personnelles.

Rubrique visée : test magazine

Durée : 40 minutes

Matériel :

- Stylos, marqueurs, post-its de trois couleurs différentes, tableau ou TBI
- **Dans le « dossier élèves » :**
  - le mail d'Isabelle Moureau
  - le test magazine
  - la grille d'analyse
  - les profils à compléter

Documents numériques (disponible sur le site du CSEM via code QR) :

- Formulaire PMS
- Formulaire Snapchat

Déroulement (50 minutes)

TEMPS 1

Comprendre l'objectif du service

15 min

Deux cas concrets illustrent le fait que toutes les données personnelles collectées ne sont pas forcément nécessaires par rapport à l'objectif poursuivi.

L'enseignant·e propose au groupe d'analyser deux formulaires pour introduire la distinction entre données obligatoires, facultatives et excessives.

Analyse des deux formulaires :

L'enseignant·e divise le groupe classe en 4 sous-groupes et distribue à chaque sous-groupe 2 captures d'écran : un formulaire PMS et un formulaire d'inscription à Snapchat. Les 4 groupes travaillent donc sur les mêmes exemples.

Leur mission : classer chaque donnée demandée sur des post-its de couleur en fonction des catégories suivantes :

- Obligatoire (post-it vert) : c'est essentiel pour accéder au service.
- Facultatif (post-it orange) : c'est utile mais pas nécessaire, on peut s'en passer.
- Intrusif (post-it rouge) : ce n'est pas normal, c'est une collecte abusive de données.

À la fin du travail en sous-groupes, l'enseignant·e invite chaque groupe à venir placer ses post-it dans les différentes catégories au tableau. Ensuite, une discussion collective permet de comparer les choix des groupes, d'argumenter sur certaines décisions et de remettre en question certaines classifications si nécessaire. L'objectif est d'amener les élèves à justifier leur raisonnement et à prendre conscience que toutes les données demandées ne sont pas toujours légitimes ou nécessaires.

L'enseignant·e insiste sur un principe essentiel : avant de fournir une information ou de remplir un formulaire, il est important de s'interroger : Pourquoi cette donnée est-elle demandée ? Est-elle vraiment nécessaire pour utiliser le service ? Si la réponse est non, alors son partage ne devrait pas être obligatoire.

L'enseignant·e peut alors poser quelques questions :

- Que se passe-t-il si tu refuses de donner certaines informations facultatives ? Peux-tu quand même utiliser le service ?
- Pourquoi certaines applications demandent-elles des accès qui ne sont pas nécessaires à leur fonctionnement (ex. : contacts, caméra, géolocalisation) ?
- As-tu déjà rempli un formulaire sans trop réfléchir aux informations demandées ? Avec ces nouvelles connaissances, ferais-tu différemment ?

TEMPS 2

Le test magazine

⏳ 15 min

L'enseignant·e distribue à chaque élève le test magazine et la grille d'analyse. Chaque élève remplit le test pour mieux comprendre son propre profil numérique personnel et, à l'aide de la grille d'analyse, calcule son score et découvre s'il·elle se rapproche plutôt du profil spontané·e, stratège ou furtif·ve. Aucune description n'est encore disponible pour ces profils. Ce sera aux élèves de les rédiger.

L'enseignant·e divise alors la classe en trois sous-groupes, chacun chargé de rédiger une description pour l'un des profils :

- **Groupe 1 :** Le·la spontané·e → Téméraire, il·elle partage facilement ses informations sans trop y réfléchir.
- **Groupe 2 :** Le·la stratège → Pragmatique, cette personne fait attention à ce qu'elle partage.
- **Groupe 3 :** Le·la furtif·ve → prudent·e, il·elle limite au maximum la diffusion de ses données personnelles.

TEMPS 3

Rédaction des résultats du test

⏳ 20 min

Pour ce faire, les sous-groupes reçoivent :

- le mail de la rédactrice en chef Isabelle Moreau expliquant leur mission ;
- les feuilles de résultats à compléter pour le journal.

En s'appuyant sur la grille d'analyse, les élèves constatent que leur profil numérique suit des tendances précises et qu'il se distingue des autres. À partir de ces observations, les jeunes vont rédiger un portrait détaillé de leur profil numérique, à savoir « Le·la spontané·e – Le·la stratège – Le·la furtif·ve ». Il leur suffit de transformer ces observations en un texte structuré, mêlant description, conseils et réflexion sur les bonnes pratiques.

Pour construire la description des profils, il est également possible de demander aux élèves de rechercher (ou leur fournir) des descriptions du même type, issues d'autres tests et de les analyser et les décomposer ensemble pour identifier les invariants qui constitueront la description à rédiger.

Une fois leur texte final rédigé, les élèves le partagent avec le groupe lors d'une mise en commun. Chacun·e lit son portrait numérique à haute voix, permettant ainsi aux autres d'apporter des suggestions, de proposer des améliorations et de questionner certains choix. Cet échange permet d'enrichir les textes, d'affiner les formulations et de s'assurer que chaque profil est clair et percutant avant sa publication dans Pixel Mag.

Consigne	Explication	Exemple avec le·la spontané·e
Rédiger une phrase d'introduction engageante en utilisant « tu ». Cette phrase doit capter l'attention et résumer le comportement numérique de votre profil	Écrivez une phrase qui résume le comportement de cette personne avec le numérique. Imaginez une accroche engageante qui décrit comment elle gère ses données en ligne.	« *Tu es un·e explorateur·rice du web : curieux·se et toujours prêt·e à tester de nouvelles applis, tu ne perds pas de temps à lire les petites lignes… et encore moins à dire non aux cookies !* »
Comment cette personne interagit-elle avec le numérique ?	Décrivez son attitude : Partage-t-elle beaucoup d'informations sans trop y réfléchir ? Vérifie-t-elle avant d'accepter ? Se pose-t-elle des questions sur la collecte de ses données ?	« *Tu remplis les formulaires sans trop y penser, tu acceptes rapidement les conditions d'utilisation et tu ne vois pas trop pourquoi il faudrait tout vérifier. Après tout, si une appli demande tes infos, c'est sûrement qu'elle en a besoin, non ?* »
Quel est le principal point positif de ce comportement ?	Expliquez ce que cette manière d'interagir avec le numérique peut apporter de bénéfique. Est-ce que cette personne profite pleinement des services ? Est-elle bien protégée ?	« *Grâce à ton aisance avec les outils numériques, tu profites sans contrainte de toutes les fonctionnalités des applications et plateformes. Pas de prise de tête, tu es toujours dans l'instant et tu explores tout ce que le web a à offrir.* »
Quel est le principal point négatif ?	Décrivez un risque ou un problème potentiel lié à ce comportement. La personne peut-elle être trop exposée ? Est-elle trop méfiante ? Manipulée par les algorithmes ?	« *Le problème, c'est que tu donnes parfois plus d'infos que nécessaire. Résultat : ton profil est ultra-ciblé par la pub, et tes données personnelles peuvent être revendues sans que tu le saches.* »
Proposer un conseil clé	Rédigez une phrase qui pourrait aider cette personne à mieux gérer ses données personnelles. Comment pourrait-elle améliorer son comportement tout en gardant les aspects positifs ?	« *Avant de cliquer sur "J'accepte", pose-toi une question simple : est-ce que cette appli a vraiment besoin de toutes ces infos ? Parfois, un petit réglage dans les paramètres peut faire toute la différence !* »
Rajouter une touche d'humour	Trouvez une phrase amusante ou une métaphore qui illustre ce comportement. Cela peut être une comparaison avec un objet (ex. : « Tu acceptes les cookies plus vite qu'un robot affamé ! ») ou une blague sur son usage du numérique.	« *Tu remplis un formulaire plus vite qu'un·e influenceur·euse accepte une collaboration… Mais souviens-toi, sur Internet, tout ce que tu donnes peut rester à jamais !* »

Notes

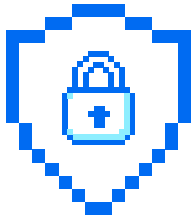
Notes


Une courte vidéo reprend les éléments essentiels à retenir de cette mission 2 :

Mission 3

Tu as des droits…
Utilise-les !

Contexte théorique sur la protection des données



Une fois que les élèves ont pris conscience de la quantité de données personnelles partagées, il est important de prendre conscience de ses droits en lien avec ces dernières. Connaître et utiliser ses droits, c'est déjà reprendre le contrôle sur ses données.

1. Les droits des jeunes en tant que personnes concernées

Les enfants sont des personnes concernées au sens du RGPD et, à ce titre, ils·elles disposent des droits prévus par le RGPD. L'enfant peut exercer lui·elle-même ses droits mais, en fonction de son âge et de sa maturité, il·elle devra se faire assister par un adulte, par exemple le·la titulaire de la responsabilité parentale. Le RGPD ne prévoit pas d'âge minimum pour que le·la mineur·e exerce l'un de ses droits.

Le droit à l'information (art. 13 et 14 RGPD)	Chaque personne concernée a droit à certaines informations lorsqu'une organisation traite des données personnelles la concernant. Le responsable du traitement a l'obligation d'informer la personne concernée de ce qu'il fait avec ses données et pourquoi ainsi que sur les droits de la personne concernée. Il doit le faire notamment au moyen d'une politique de confidentialité (voir mission 2).
Le droit d'accès (art. 15 RGPD)	Le droit d'accès permet à la personne concernée de contrôler la licéité (respect de la loi) de chaque activité de traitement. Le droit d'accès comporte trois volets : 1. La personne concernée a le droit de savoir si le responsable de traitement traite ou non ses données personnelles. 2. Si oui, la personne concernée a le droit d'obtenir une série d'informations telles que la finalité du traitement, les catégories de données concernées et le délai de conservation. 3. La personne concernée a le droit d'obtenir gratuitement une copie de ses données personnelles.
Le droit de rectification (art. 16 RGPD)	La personne concernée a le droit de faire rectifier des données personnelles inexactes ou de compléter des données personnelles incomplètes, Si le responsable de traitement a transmis ces données personnelles à des tiers, il doit les informer de la rectification qui a été apportée, à moins que cela se révèle impossible ou exige des efforts disproportionnés.

Le droit à l'effacement (art. 17 RGPD)	Chaque personne concernée peut s'opposer au traitement de ses données personnelles la concernant « pour des raisons tenant à sa situation particulière ». Le droit d'opposition peut exclusivement être exercé si le traitement repose sur une des bases juridiques suivantes : ▪ l'intérêt légitime du responsable de traitement ou d'un tiers ; ▪ l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ⚠ Une exception importante à cette mise en balance des intérêts existe en faveur de la personne concernée : en cas de marketing direct, la personne concernée a toujours le droit de s'opposer sans la moindre motivation. Cette opposition conduit donc automatiquement à l'arrêt du traitement pour cette finalité.
Le droit d'opposition (art. 21 RGPD)	Le droit à la portabilité des données personnelles permet à la personne concernée d'obtenir ses données personnelles et de les réutiliser pour d'autres services. La personne concernée peut, ainsi, déplacer ses données personnelles d'un environnement IT vers un autre.

Ces droits ne sont pas absolus. Pour plus d'informations sur les droits des personnes concernées et comment les utiliser, vous pouvez consulter le site de l'autorité de la protection des données : autoriteprotection-donnees.be

Dans le cadre d'un exercice de droits, le responsable de traitement dispose d'un délai d'un mois pour répondre à compter de la date de réception de votre demande. Le RGPD lui permet, dans certaines circonstances, de prolonger ce délai de deux mois. Dans ce cas, il devra toutefois informer la personne concernée de cette prolongation et de ses motifs dans le délai d'un mois précédemment mentionné.

Si le responsable de traitement ne répond pas dans le délai imparti ou fournit une réponse insatisfaisante, la personne concernée a la possibilité d'introduire une procédure de plainte ou de médiation auprès de l'APD.

2. Droit à l'image

Notion de droit à l'image

Le droit à l'image protège la personne concernée contre l'utilisation non-consentie de son image. Ce droit implique que pour prendre et pour diffuser une photo et/ou vidéo d'une personne physique, son consentement préalable est requis. Il existe des exceptions qui sont reprises ci-contre.

Ce droit est devenu d'autant plus important avec le développement du numérique et les réseaux sociaux. Le droit à l'image doit être respecté tant par les jeunes, notamment lorsqu'ils·elles publient des photos et/ou vidéos sur les réseaux sociaux que par les établissements scolaires (dont les enseignants) par exemple lorsqu'ils·elles prennent des photos et/ou vidéos lors d'activités scolaires.

Le droit à l'image est un droit impliquant que pour chaque image d'une personne mais aussi pour l'utilisation de cette image, le consentement de la personne apparaissant sur l'image est requis.

Principe du consentement

Le droit à l'image se divise en deux droits différents :

- le droit de prendre l'image ;
- le droit de diffuser l'image.

Dans les deux cas, il faut préalablement obtenir le consentement de la personne photographiée ou filmée.

Ce sont deux consentements différents. Ils doivent être demandés séparément : d'abord un consentement pour prendre l'image et ensuite un consentement pour diffuser l'image.

Pour pouvoir prouver le consentement, mieux vaut utiliser un document écrit dans lequel le consentement de la personne concernée est clairement exprimé.

Exceptions :

- Si la personne concernée n'est pas facilement identifiable sur l'image, elle ne peut pas exercer ses droits sur la prise de l'image ni sur la diffusion.

  Par exemple, pour une photo de foule, les personnes concernées dans cette foule ne peuvent pas refuser qu'on prenne leur image.

- Le consentement des personnes publiques (politiciens, chanteurs, sportifs, etc.) pour les images prises pendant qu'elles exercent leur fonction publique n'est pas nécessaire. On peut, dans ce cas, prendre, exposer et reproduire leur image sans leur demander leur consentement.
- Le droit à l'information permet de prendre et de diffuser une image sans le consentement des personnes concernées par l'événement d'actualité.
- Une photo à usage purement privé ou domestique (comme une photo prise avec un membre de sa famille qu'on ne publie pas sur les réseaux)

Il est essentiel que le jeune comprenne que le fait de consentir à être pris en photo ne signifie pas consentir à ce que cette photo soit publiée sur les réseaux.

Forme du consentement

Une personne photographiée ou filmée doit donner son consentement de manière claire et non-ambiguë.

Le responsable de traitement (photographe, personne qui diffuse l'image, etc.) doit pouvoir prouver que la personne a donné un consentement valable.

Le consentement ne doit pas nécessairement être écrit, mais il doit être certain. Il peut être oral ou même implicite. Ainsi, une personne prend la pose ou se laisse photographier sans s'y opposer.

Un consentement oral ou implicite est difficile à prouver. Par prudence, il vaut mieux utiliser un document écrit, appelé formulaire d'autorisation. Un consentement écrit est en effet recommandé pour prendre ou diffuser des images ciblées dans un cercle fermé : une école, un club sportif, une association, etc.

Une image ciblée est une image individuelle ou une image pour laquelle une ou plusieurs personnes sont mises en évidence, comme une photo de classe ou d'équipe, ou une photo individuelle.

Pour des images non ciblées, il suffit d'informer les personnes concernées que :

- des images sont prises ;
- pour quelle finalité ;
- pour quelle publication.

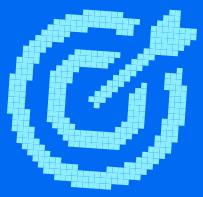
Une image non ciblée est une image qui donne une idée générale de l'ambiance, sans qu'une ou plusieurs personnes soient spécifiquement identifiées. Par exemple, une photo de groupe de la classe lors d'une balade en forêt ou d'une activité sportive. Dans la pratique, ce n'est pas toujours possible de demander préalablement un consentement. On peut alors anonymiser les images.

Consentement du mineur

Un·e mineur·e peut donner seul son accord s'il a la capacité de discernement. Dans ce cas, il ne doit pas être représenté par ses parents.

Généralement, on considère qu'un·e mineur·e a la capacité de discernement entre 12 et 14 ans. Toutefois cette capacité doit être évaluée au cas par cas, en tenant compte du contexte spécifique.

Contexte de la mission



Nous interagissons chaque jour avec des sites web et des applications, souvent sans prêter attention aux petites lignes des politiques de confidentialité. Pourtant, ces documents définissent ce que les plateformes font avec nos données personnelles. Cette mission vise à aider les élèves à comprendre leurs droits pour protéger leur vie privée en ligne et à développer une posture critique et active face aux pratiques des entreprises du numérique.

Dans cette mission, comme toutes les autres, les élèves se glisseront dans la peau de journalistes du Pixel Mag pour répondre aux nombreuses questions envoyées par les lecteur·rice·s. Leurs courriers reflètent des situations bien réelles : une photo non désirée est publiée, une avalanche de publicités non souhaitées ou encore un faux compte qui usurpe une identité.

Pour les aider à formuler des réponses précises et accessibles, les élèves devront explorer les droits dont ils disposent pour protéger et contrôler leurs données et comprendre les obligations des plateformes. Ainsi, les jeunes peuvent se rendre compte qu'ils·elles ne sont pas impuissant·e·s face aux plateformes du numérique. Ils·elles ont des droits pour protéger leurs données personnelles et leur vie privée, et ils·elles peuvent les faire valoir !

Durant cette activité, l'élève sera amené·e à :

- **Prendre conscience de ses droits** pour protéger ses données personnelles et sa vie privée.
- **Découvrir les obligations légales des plateformes** numériques.
- **Savoir comment agir pour modifier ou supprimer ses données personnelles** en ligne par l'exercice des droits prévus par le RGPD.
- **Développer un regard critique** et une posture active sur l'utilisation des données personnelles.
- **Développer des compétences rédactionnelles** en expliquant ces notions de façon accessible aux lecteur·rices du Pixel Mag.

Durée : 45 minutes

Matériel :

- Stylos, marqueurs, post-its
- **Dans le « dossier élèves » :**
  - le mail d'Isabelle Moureau
  - les courriers des lecteur·rice·s

Documents numériques (disponible sur le site du CSEM via code QR) :

- Les cartons « vrai ou faux »
- Les cartons des droits

Notes

Déroulement (50 minutes)

TEMPS 1

Données personnelles : vrai ou faux — 10 min

Dans ce premier temps, l'enseignant·e divise la classe en 6 sous-groupes et distribue à chaque sous-groupe les 13 cartes « Vrai/Faux ». Sur chaque carte, il y a une phrase écrite. Les élèves discutent pour classer les phrases en deux tas distincts : « Vrai » et « Faux ».

Une fois les affirmations classées, l'enseignant·e peut lancer une discussion :

- Qu'est-ce qui vous a surpris ?
- Savez-vous ce qu'est une politique de confidentialité et où la trouver ? L'enseignant·e peut aborder cette question en se référant au cadre théorique.

TEMPS 2

Utilise tes droits — 15 min

Toujours en groupe, les élèves reçoivent 8 cartons décrivant les droits dont ils·elles disposent, par exemple, quand ils·elles estiment qu'une organisation ou une personne utilise abusivement leurs données personnelles.

L'enseignant·e passe en revue les différents cartons pour que chaque élève ait bien compris le vocabulaire ainsi que le contenu.

TEMPS 3 (1/2)

Répondre aux courriers

25 min

Chaque sous-groupe d'élèves lit la lettre de la rédactrice en chef Isabelle et Moreau et se voit attribuer un des courriers des lecteurs.

L'enseignant·e explique qu'il faut les aider à trouver des solutions grâce aux cartons des droits. Il faut donc que les élèves rédigent une réponse aux inquiétudes exprimées par chaque lecteur·rice.

Lettre 1 - On m'a créé un faux compte Insta !

Quel(s) droit(s) peut-il·elle activer ?

Le droit à l'effacement. Comment ?

- Contacter Instagram : signaler le compte et lui demander de supprimer les données à caractère personnel ;
- Demander à la personne qui a créé le profil ayant violé la vie privée de supprimer le contenu et les images ;
- Contacter les services de police. En effet, il s'agit d'une infraction pénale (usurpation d'identité).

Lettre 2 - Je veux changer d'appli sans tout perdre !

Quel(s) droit(s) peut-il·elle activer ?

Le droit à la portabilité permet de récupérer ses données et de les transférer vers une autre plateforme (si elle le permet).

Lettre 3 - J'ai accepté un truc sans faire exprès

Quel(s) droit(s) peut-il·elle activer ?

Le droit de retirer son consentement (fait partie du droit à l'effacement) en allant dans la section « Gestion des cookies » sur le site. Si le site ne propose pas cette option, contacter directement le service concerné pour demander la suppression des données.

TEMPS 3 (2/2)

Répondre aux courriers

Lettre 4 - Pourquoi mon école garde mes infos ?

Quels droits peut-elle activer ?

Le droit d'accès : elle peut demander à voir les infos que l'école conserve sur elle. L'école est obligée de lui répondre et de lui fournir une copie des données si elle le demande.

Lettre 5 - J'ai dit oui aux pubs, mais maintenant j'en ai marre !

Quels droits peut-il activer ?

Le droit de retirer son consentement (fait partie du droit à l'effacement) en contactant directement le site. Mais en principe, il peut chercher le bouton « se désinscrire » sur la page. Si le site continue de lui envoyer des publicités, il peut contacter l'Autorité de Protection des Données (APD) pour demander une médiation ou introduire une plainte via le formulaire disponible sur son site. (autoriteprotectiondonnees.be/citoyen)

Lettre 6 - J'ai dit oui à une photo... mais maintenant je regrette !

Quels droits peut-elle activer ?

Le droit à l'effacement : elle peut demander à son amie de retirer la photo, même si elle avait dit oui au début. Son amie doit respecter sa demande, car elle a le droit de changer d'avis sur la diffusion de son image.

Si le temps le permet, l'enseignant·e peut aussi lire quelques exemples à voix haute et demander l'avis des élèves :

Situations	Que peux-tu faire ?
Mon école a publié une photo de la fancy-fair sur laquelle apparaît toute la classe sur son site Internet. Je ne souhaite pas être dessus.	Tu peux demander à l'école de ne plus être identifiable sur la photo (**droit à l'effacement**). Attention : Tu dois être reconnaissable sur la photo pour que ce droit s'applique.
J'ai envie d'installer une nouvelle application mais elle me demande beaucoup d'informations.	Avant de donner tes infos, vérifie : Lis la politique de confidentialité. Si ce n'est pas clair, exerce ton **droit d'accès** pour savoir quelles données sont collectées et pourquoi. Si ces infos ne sont pas nécessaires, tu peux demander **leur effacement**. Bon réflexe : Ne remplis que les champs obligatoires et laisse les cases facultatives vides.
J'ai été refaire ma carte d'identité à la commune. J'ai dû fournir une photo d'identité mais je ne veux pas que ma photo figure sur la carte.	Impossible ! La loi oblige à mettre une photo sur ta carte d'identité pour pouvoir t'identifier facilement.
Quand j'étais plus jeune, j'ai donné une fausse date de naissance pour m'inscrire sur un site. Maintenant, j'aimerais la corriger.	**Droit à la rectification** : Tu peux contacter le site et demander à modifier tes informations avec ta vraie date de naissance.
Le vendeur dans un magasin me demande de montrer ma carte d'identité. Suis-je obligé·e d'accepter ?	Non, sauf exceptions ! Un commerçant ne peut pas exiger ta carte d'identité. Exceptions : Il peut te demander une preuve d'âge pour acheter alcool, cigarettes, jeux d'argent, mais tu peux montrer un autre document (carte étudiante, MoBib…) qui permet de démontrer ton âge
Mon club de sport me demande d'utiliser ma carte d'identité comme garantie. Suis-je obligé·e d'accepter ?	Non, tu peux refuser ! Le club doit proposer une alternative, comme une caution en argent.
Un commerçant propose d'utiliser la carte d'identité comme carte de fidélité pour obtenir des réductions. Suis-je obligé·e d'accepter ?	Non ! Tu peux refuser. Le commerçant doit proposer une alternative pour bénéficier des réductions sans utiliser ta carte d'identité. Tu as aussi le droit de demander quelles données seront utilisées et pourquoi.

Notes


Une courte vidéo reprend les éléments essentiels à retenir de cette mission 3 :

Mission 4

Forteresse numérique

Cadre théorique sur la protection des données personnelles

Chaque jour, ce sont des milliards de données qui sont partagées sur Internet. Parmi ces données, il y a des informations qui permettent d'identifier notre identité, nos habitudes, nos passions. Ce sont nos données personnelles. En partageant nos données personnelles, nous partageons une partie de notre vie privée. Or, notre vie privée est un droit fondamental qui est protégé.

Une faille de sécurité, une vulnérabilité dans un système informatique permet à un·e attaquant·e (hacker) de porter atteinte à la confidentialité, l'intégrité et/ou la disponibilité du système informatique, et donc de porter atteinte aux données personnelles contenues dans ce système informatique. Lorsqu'une faille de sécurité se produit sur un système informatique, par exemple sur un réseau social, la responsabilité première incombe au propriétaire du site. Si la faille de sécurité a compromis les données personnelles d'un grand nombre d'utilisateur·rice·s, le site doit informer les personnes dont les comptes ont été exposés, et donc, leurs données personnelles violées.

Parallèlement, en tant qu'utilisateur·ice·s, nous nous exposons à des risques de voir nos données personnelles publiées via nos comptes en ligne qui sont à la merci de hackers et de cyberattaques.

L'objectif de cette mission est de proposer des bons réflexes qui permettent aux élèves de protéger proactivement leurs comptes en ligne. En sécurisant leurs comptes en ligne, ils·elles protègent leur identité en ligne, leurs données personnelles et donc leur vie privée. Si une cyberattaque se produit, leurs données personnelles seront donc moins vulnérables.

Quelques réflexes :

- Utiliser des mots de passe forts qu'on garde secrets pour sécuriser son compte et limiter sa vulnérabilité
- Sécuriser ses comptes en ligne en réglant les paramètres (ex : supprimer l'option de géolocalisation permanente ou encore l'enregistrement permanent du micro du téléphone) pour rester maître des informations qu'on partage
- Utiliser une connexion Internet sécurisée pour limiter l'accès facile de hackers à des données personnelles
- Limiter l'accès de son profil et de ses publications à des utilisateur·rice·s qu'on choisit et qu'on connaît.

D'autres stratégies sont possibles pour sécuriser ses comptes en ligne comme l'utilisation de pseudonymes ou la possibilité d'utiliser plusieurs adresses email différentes.

Le contexte pédagogique part de l'hypothèse de la sécurisation dans le paramétrage des comptes en ligne. Plus les stratégies proposées dans cette mission sont employées, moins les utilisateur·rice·s (les élèves, les enseignant·e·s, etc.) voient leurs données personnelles contenues dans leurs comptes en ligne exposées et vulnérables aux cyberattaques et aux failles de sécurité.

Contexte de la mission

Dans cette mission, les élèves vont examiner de près des captures d'écran issues des comptes des élèves volontaires (les mêmes que dans la Mission 1!). Leur but ? Repérer les faiblesses qui rendent ces profils particulièrement vulnérables et exposés aux regards indiscrets, aux failles de sécurité, aux cyberattaques… Un mot de passe trop simple ? Une géolocalisation activée en permanence ? Un compte public ? Tout est à analyser pour rédiger un article percutant.

Pour clôturer cette enquête numérique, les élèves rédigeront un bulletin météo du web. À travers des pictogrammes et une analyse ludique, l'objectif est de proposer une grille de lecture simple pour aider les lecteur·rice·s du *Pixel Mag* à adopter de meilleures pratiques pour protéger leurs comptes en ligne.

Durant cette activité, l'élève sera amené·e à :

- **comprendre les risques liés à la gestion des comptes en ligne :** analyser comment certaines pratiques numériques peuvent exposer les données personnelles et prendre conscience de sa responsabilité lorsqu'il·elle publie ;
- **identifier des stratégies pour mieux sécuriser ses comptes en ligne et protéger ses données personnelles :** à travers des exemples concrets, découvrir des outils et des réglages essentiels pour sécuriser ses comptes et préserver sa vie privée ;
- **développer une posture critique face aux paramètres des plateformes :** en examinant les options proposées par les sites, les réseaux sociaux et les applications, prendre conscience des choix à faire pour limiter l'exposition de leurs données personnelles.
- **expérimenter la mise en situation et le changement de perspective :** en passant du rôle d'enquêteur·rice à celui d'un·e « hacker » fictif·ve, prendre du recul sur ses propres habitudes numériques et comprendre l'importance d'une navigation éclairée ;
- **communiquer sur ces enjeux de manière claire et impactante :** grâce à la rédaction du bulletin météo du web, apprendre à synthétiser des recommandations et à sensibiliser son entourage avec un langage accessible et visuel.

Rubrique visée : bulletin météo

Durée : 40 minutes

Matériel :

- Stylos, marqueurs, post-its
- **Dans le « dossier élèves » :**
  - le mail d'Isabelle Moureau
  - le bulletin météo du web

Documents numériques (disponibles sur le site du CSEM via code QR) :

- Le set de cartes « paramètres de sécurité »
- Les descriptions des captures d'écran « comptes sécurisés »

Déroulement (50 minutes)

TEMPS 1

Audit de paramètres de sécurité des comptes en ligne — 15 min

L'enseignant·e divise la classe en 6 sous-groupes et distribue à chaque groupe un dossier de presse constitué de :

- la lettre d'Isabelle Moureau, la rédactrice en chef
- 2 descriptions de captures d'écran (liées à l'élève volontaire dont le groupe s'occupe). Ces profils sont les mêmes que ceux dans la Mission 1.

Dans ces 2 captures, les élèves sont invité·e·s à repérer 3 faiblesses de sécurité des comptes en ligne.

TEMPS 2 (1/2)

Forteresse numérique — 10 min

Une fois les failles identifiées, chaque groupe reçoit un set de 8 cartes « Paramètres de sécurité », comprenant des stratégies de protection. Les élèves posent sur les captures d'écran 3 cartes qui représentent les solutions concrètes pour améliorer la sécurité du compte. Ils·elles doivent choisir les 2 plus importantes à leurs yeux parce que plusieurs cartes sont utilisables.

Proposition de correctif

Clara

Capture 1 (Carte)

- Vérifier les autorisations des applications
- Paramétrer ses réseaux sociaux en privé

Capture 2 (Carte)

- Ne jamais partager ses mots de passe
- Choisir un mot de passe long et unique

TEMPS 2 (2/2)

Inès

Capture 1 (Carte)

- Désactiver la géolocalisation automatique
- Faire attention aux Wi-Fi publics

Capture 2 (Carte)

- Activer l'authentification à deux facteurs (2FA)
- Choisir un mot de passe long et unique

Gabriel

Capture 1 (Carte)

- Protéger ses comptes avec un gestionnaire de mots de passe
- Choisir un mot de passe long et unique.
- Activer l'authentification à deux facteurs (2FA)

Capture 2 (Carte)

- Vérifier les autorisations des applications

Yassir

Capture 1 (Carte)

- Choisir un mot de passe long et unique
- Paramétrer ses réseaux sociaux en privé.
- Vérifier les autorisations des applications

Capture 2 (Carte)

- Désactiver la géolocalisation automatique
- Vérifier les autorisations des applications

TEMPS 3

Défi « H@ck » ou Protège ?

10 min

Sur les captures d'écran, les sous-groupes ont identifié 3 faiblesses mais il y en a bien plus. Pour trouver une dernière faiblesse restante, chaque sous-groupe va changer de profil d'élève volontaire (en se levant et en se déplaçant, par exemple).

Les nouveaux groupes ont ainsi une nouvelle mission : jouer les « hackers » et tenter de trouver une faiblesse restante (un mot de passe encore trop faible, une information partagée trop facilement, etc.). Ensuite, chaque groupe propose une solution supplémentaire pour renforcer encore plus la sécurité du profil en choisissant une dernière carte (parmi les 6 restantes).

TEMPS 4

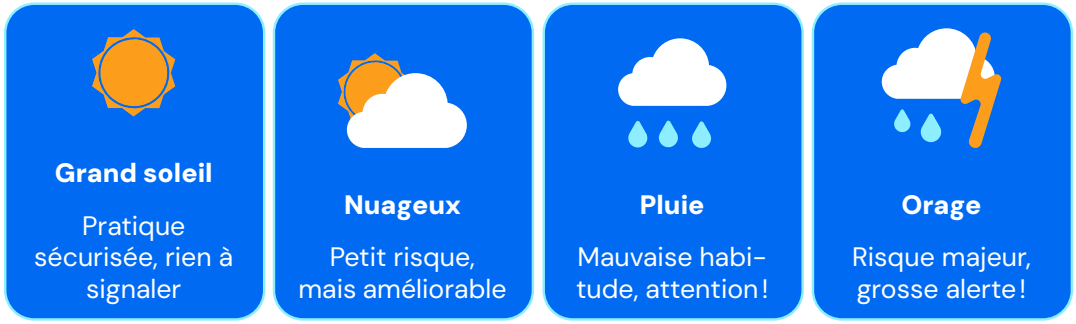
Rédaction du bulletin météo

15 min

Selon la lettre d'Isabelle Moreau, les élèves doivent rédiger un bulletin météo de prévisions du web. En grand groupe, l'enseignant·e note au tableau les situations ci-dessous.

- Se connecter à un Wi-Fi public
- Utiliser le même mot de passe pour tous ses comptes
- Partager ses identifiants Netflix/Spotify avec plusieurs amis
- Utiliser la géolocalisation permanente sur toutes ses applications
- Utiliser la date de naissance de son chien ou de sa sœur comme mot de passe
- Laisser son compte Instagram ou TikTok en mode public
- Activer la double authentification (2FA) sur ses comptes importants
- Mettre son compte Instagram en mode privé mais accepter des demandes d'inconnus
- Avoir un mot de passe solide mais le noter sur un post-it sur son bureau
- Refuser la géolocalisation pour certaines applications, sauf en cas de besoin
- Utiliser un gestionnaire de mots de passe sécurisé

L'enseignant·e invite les élèves à dessiner sous chaque situation le pictogramme adapté :



On remarque également dans cette fiche que 3 espaces libres sont disponibles pour que les élèves puissent y insérer eux-mêmes des situations vécues qui ne seraient pas proposées par la mission.

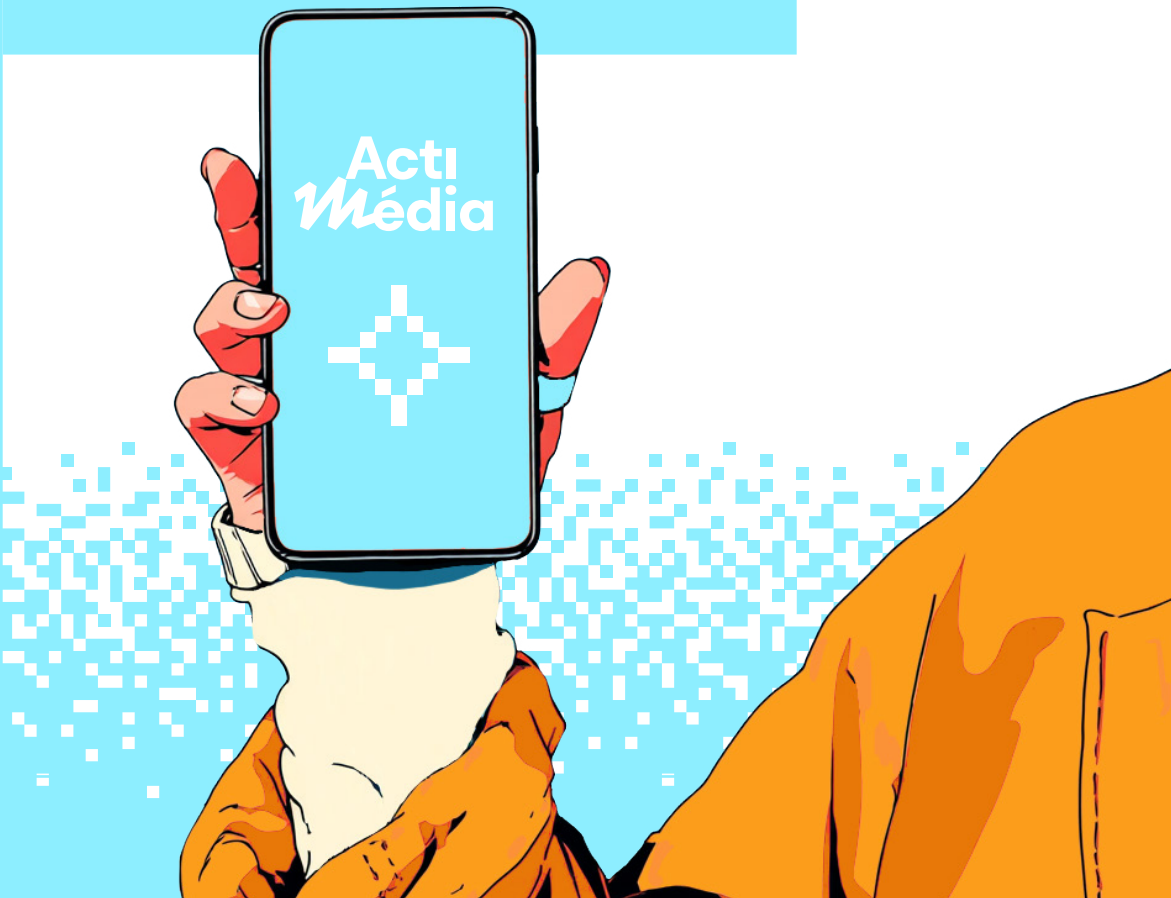
Notes

Notes


Une courte vidéo reprend les éléments essentiels à retenir de cette mission 4 :

Mission 5

Réinvente ton feed



Contexte théorique sur la protection des données

Les données que nous partageons en ligne révèlent notre identité, nos valeurs, nos habitudes, nos proches. Ce sont des données personnelles qui sont de l'ordre de la vie privée. Or, elles peuvent être utilisées à notre insu pour vendre des produits, des services ou promouvoir des idées.

Aujourd'hui, le marché de la donnée est géré par de grandes entreprises qui stockent et revendent les informations dont nos données personnelles.

Les mécanismes de l'influence agissent sur les subtils rouages qui guident nos choix, attitudes et comportements, souvent de manière inconsciente. Ces mécanismes profitent de notre psychologie et de nos biais cognitifs, exploitant nos besoins d'appartenance, de conformité et de reconnaissance sociale. Les réseaux sociaux amplifient ces mécanismes. Certaines plateformes sociales exploitent la conformité sociale en mettant en avant le nombre de like, de partages et de commentaires pour valider l'importance d'une publication. Comprendre ces mécanismes de l'influence peut nous rendre plus conscient·es de nos choix et nous aider à prendre des décisions plus éclairées en toute indépendance.

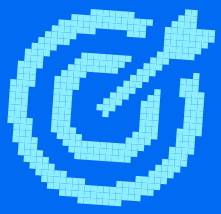
Les algorithmes utilisent les données collectées sur nos comportements passés pour anticiper nos préférences et nous présenter un contenu personnalisé. Cette personnalisation peut renforcer nos croyances existantes ou encore exploiter nos réactions émotionnelles en mettant en avant des contenus pouvant susciter des réponses émotionnelles fortes, ce qui peut renforcer nos engagements en ligne ou contribuer à la propagation de la désinformation.

Cette mission a pour objet la réutilisation des données personnelles. Cette dernière peut avoir une influence sur leur recherche d'informations et les publicités ciblées. Elle peut être liée à différentes thématiques :

- **Le profilage :** technique qui a pour objectif de nous faire correspondre à des schémas mis en place pour nous persuader, nous influencer, ou nous vendre des produits par exemple.
- **Les cookies :** mini-fichiers installés sur nos appareils connectés qui, au fil de nos navigations, permettent, par exemple, à des tiers de connaître nos navigations et d'en déduire nos goûts et nos préférences.
- **La bulle de filtre :** phénomène observé principalement sur les réseaux sociaux qui désigne le filtrage de l'information parvenant à l'internaute par différents filtres qui alimentent notamment les fils d'actualité des publications susceptibles d'intéresser les utilisateurs et qui peuvent parfois ne proposer que des contenus similaires entre eux.

La mission offre des méthodes pour adopter des réflexes afin d'avoir un profil moins soumis aux influences des bulles de filtre ou encore des publicités ciblées.

Dans les prolongations, on revient également sur une des stratégies clé du RGPD : exercer ses droits. Dans ce cas, il s'agit de l'exercice du droit d'opposition par la désinscription des newsletters.



Contexte de la mission

Cette fois, Pixel Mag s'intéresse à un phénomène invisible, mais qui façonne en grande partie notre expérience en ligne : les algorithmes. Ils façonnent en grande partie notre expérience numérique et celle des jeunes : que ce soit les vidéos regardées, les recommandations d'ami·e·s, les articles proposés ou encore les publicités ciblées. Ces systèmes s'appuient sur l'analyse de leurs données personnelles – historiques de navigation, interactions, centres d'intérêt, localisation… – pour leur suggérer des contenus adaptés à leurs profils numériques. Ce ciblage, bien que pratique, peut aussi les enfermer dans une « bulle de filtre » où ils·elles ne voient plus que ce qui correspond à leurs préférences passées, limitant ainsi leur accès à une diversité de points de vue et de découvertes.

Cette mission vise à leur faire prendre conscience de l'impact de ces algorithmes sur leur navigation et à leur montrer qu'il est possible d'en reprendre le contrôle. Il est proposé aux jeunes de :

- explorer le ciblage publicitaire en découvrant comment les données personnelles partagées sur le net influencent les annonces qu'ils·elles reçoivent ;
- comprendre le phénomène des bulles de filtres et discuter de son impact sur l'accès des jeunes à l'information ;
- passer à l'action en concevant une rubrique lifestyle intitulée « Réinvente ton feed : Explore au-delà de ta bulle numérique ! », où les élèves proposeront un challenge interactif de 7 jours pour diversifier leurs recommandations et reprendre du contrôle sur leurs fils d'actualité.

Durant cette activité, l'élève sera amené·e à :

- **comprendre l'influence des algorithmes sur les contenus affichés, à partir du profil numérique :** analyser comment les systèmes de recommandation façonnent leur expérience en ligne, influençant les publicités, les vidéos et les articles proposés ;
- **identifier les mécanismes des bulles de filtres :** en explorant le ciblage algorithmique, prendre conscience de son exposition à des contenus répétitifs et de l'impact de ces filtres sur son accès à l'information ;
- **décrypter les stratégies publicitaires :** en associant des publicités et des recommandations aux profils fictifs, découvrir comment ses données personnelles sont exploitées à des fins commerciales et marketing ;
- **développer une posture critique sur leur usage du numérique :** apprendre à questionner les suggestions de contenu et à réfléchir aux impacts de la personnalisation algorithmique sur ses choix et opinions ;
- **expérimenter des stratégies pour diversifier leur fil d'actualité :** en concevant un challenge de 7 jours, tester des actions concrètes pour « hacker » ses propres recommandations et élargir leurs horizons numériques ;
- **communiquer de manière engageante et accessible :** à travers la création de la rubrique lifestyle « Réinvente ton feed », développer sa capacité à formuler des conseils pratiques et à sensibiliser son entourage aux enjeux des algorithmes.

Rubrique visée : lifestyle « Réinvente ton feed »

Durée : 40 minutes

Matériel :

- Les interviews complétées de la mission 1
- **Dans le « dossier élèves » :**
  - La lettre d'Isabelle Moureau
  - Fiche « Challenge 7 jours »

Documents numériques (disponibles sur le site du CSEM via code QR) :

- Les publicités fictives
- Les recommandations et contenus informationnels personnalisés

Notes

Déroulement (50 minutes)

TEMPS 1

Ciblage publicitaire

20 min

L'enseignant·e affiche les 4 interviews complétées lors de la Mission 1, soit en les imprimant, soit en les projetant si l'équipement de la classe le permet. L'objectif est que tous les élèves puissent visualiser simultanément les 4 profils.

Ensuite, l'enseignant·e distribue au grand groupe, réparti en groupes de deux élèves, deux publicités. L'enseignant·e explique que les annonces publicitaires visibles en ligne ne sont pas affichées au hasard. Elles sont spécifiquement conçues pour cibler des utilisateur·rice·s en fonction de leurs données personnelles.

Les élèves disposent de cinq minutes pour analyser les publicités et décider à quel·le élève elles correspondent le mieux. Une fois leur choix fait, accrocher leur publicité sous le profil correspondant à l'aide de papier collant ou d'aimants.

À l'issue de cette phase, l'enseignant·e anime une discussion en revenant sur les associations effectuées et en posant les questions suivantes :

- Pourquoi pensez-vous que cette publicité intéresse ce profil en particulier ?
- Quelles données spécifiques de ce profil (âge, hobbies, applications préférées…) ont été utilisées pour concevoir cette publicité ?
- Pourquoi plusieurs publicités peuvent correspondre à plusieurs profils ?

TEMPS 2

Bulle de filtre

15 min

L'enseignant·e explique que les algorithmes ne se limitent pas aux publicités : ils influencent également les flux d'information en ligne, notamment à travers les recommandations de vidéos, d'articles ou de comptes à suivre.

Chaque groupe reçoit deux fois le même contenu informationnel sous forme d'une recommandation YouTube, d'un compte Instagram ou d'une vidéo TikTok. Les élèves doivent analyser ce contenu et déterminer à quels profils de la mission 1 ils correspondent le mieux.

Une fois leurs choix effectués, les élèves justifient leurs associations en expliquant pourquoi ces profils spécifiques pourraient être particulièrement exposés à ce type de recommandation.

L'enseignant·e engage ensuite une discussion collective en posant les questions suivantes :

- Est-ce que tout le monde voit la même chose ?
- Quels risques y a-t-il à être enfermé·e dans un même type de contenu ?
- A-t-on vraiment le choix dans ce que l'on regarde en ligne ?

TEMPS 3 (1/2)

Réinvente ton feed

15 min

Lors de ce dernier temps, les élèves passent à l'action en explorant des stratégies concrètes pour sortir de leur bulle de filtre. L'objectif est qu'ils·elles comprennent que leurs habitudes influencent les recommandations et qu'il est possible d'en reprendre le contrôle.

L'enseignant·e explique que les algorithmes ne sont pas figés : en modifiant leurs comportements en ligne, les élèves peuvent diversifier leur fil d'actualité et élargir leurs horizons.

Toujours en duo, les élèves reçoivent la lettre d'Isabelle Moreau, la rédactrice en chef du *Pixel Mag*. Celle-ci leur explique leur mission : concevoir une rubrique lifestyle pour le *Pixel Mag* intitulée « Réinvente ton feed : Explore au-delà de ta bulle numérique ! ». Cette rubrique prendra la forme d'un challenge sur 7 jours, avec des défis quotidiens à tester pour influencer leurs recommandations.

L'enseignant·e projette en grand la fiche à compléter avec les 7 jours de défis, qui servira à structurer le challenge (ou l'imprime en A3 pour l'afficher au tableau).

Chaque duo reçoit 2 post-its et inscrit une idée de défi par post-it (soit 2 idées en tout). Les post-its sont collés au tableau pour une mise en commun. L'enseignant·e regroupe les idées similaires et anime une rapide discussion collective pour affiner les propositions.

S'il y a beaucoup d'idées, un vote rapide peut être organisé. Les 7 défis retenus sont inscrits sur la fiche projetée (ou imprimée si le matériel ne permet pas la projection).

Si les élèves peinent à trouver des idées, quelques suggestions pour les guider se trouvent à la page suivante. Ces propositions ne sont là qu'à titre d'exemples : il ne s'agit ni d'une liste exhaustive ni d'un programme imposé, mais d'un point de départ pour nourrir les réflexions et les aider à formuler leur propre challenge.

TEMPS 3 (2/2)

- Chercher une vidéo sur un sujet totalement différent de leurs habitudes (ex. regarder un documentaire s'ils consomment surtout du gaming).
- S'abonner à un·e créateur·rice de contenu ou une page sur un sujet inconnu.
- Désactiver les recommandations automatiques sur *YouTube/TikTok* pendant une journée.
- Naviguer en mode privé et observer les différences dans les suggestions.
- Tester un moteur de recherche alternatif à *Google* (ex. *Qwant*, *Ecosia*, *DuckDuckGo*).
- Écouter une playlist ou un artiste complètement différent de ses goûts habituels.
- Se désabonner de 3 comptes et analyser comment cela impacte les suggestions.
- Regarder une vidéo ou lire un article venant d'un média qu'ils·elles ne consultent jamais.
- Chercher une information sur plusieurs plateformes différentes et comparer les résultats.
- Utiliser une application qu'ils·elles n'ont jamais testée et observer comment elle leur recommande du contenu.
- Etc.

Notes


Une courte vidéo reprend les éléments essentiels à retenir de cette mission 5 :

csem

FÉDÉRATION WALLONIE-BRUXELLES

rtbf.be

Autorité de protection des données