DIGCITY

Cofinancé par l'Union européenne

GAME-BASED DIGITAL CITIZENSHIP

Guide sur les compétences de citoyenneté numérique

LogoPsyCom PENS digiQ YuzuPulse

Ce guide fait partie des ressources du **projet DigiCity**.

Pour en savoir plus, consultez le site web du projet : **https://projectdigicity.eu/**

Leader du projet

Omladinski savez udruženja 'OPENS' (Serbie)

Organisations participantes

Digitalna Inteligencia (Slovaquie)

YuzuPulse (France)

Logopsycom (Belgique)

Table des matières

I. INTRODUCTION

Dans le monde interconnecté d'aujourd'hui, le paysage digital fait partie intégrante de nos vies quotidiennes, autant que les paysages physiques. Des plateformes de réseaux sociaux aux ressources éducatives, internet offre des possibilités infinies de connexion, d'apprentissage et de créativité. Cependant, naviguer à travers ce grand et dynamique espace requiert bien plus que des compétences techniques, cela demande un set de valeurs, de comportements et connaissances collectives connu sous le nom de citoyenneté numérique.

Ce guide est créé de sorte à équiper les jeunes avec des compétences essentielles de citoyenneté numérique, leur donnant les moyens de participer responsablement, éthiquement et efficacement dans le monde numérique. Cela traite de sujets clés comme la confidentialité en ligne, une utilisation responsable des réseaux sociaux, la désinformation et comment la reconnaître, et ce qu'est une empreinte digitale. Ce ne sont pas juste des compétences, mais des leçons de vie qui aideront les jeunes à prospérer dans une société numérique croissante.

Pourquoi avons-nous fait ce guide ?

Le Guide sur les compétences de citoyenneté numérique est un pilier fondateur pour atteindre certains de nos objectifs, en particulier favoriser des citoyens numériques informés et responsables. Il met systématiquement en valeur les aspects critiques de la citoyenneté numérique que les formateurs et les organisations de jeunesse doivent acquérir/comprendre. En offrant une vue d'ensemble compréhensive des sujets comme la confidentialité en ligne, l'utilisation responsable des réseaux sociaux, et le discernement de la désinformation, ce guide équipe les formateurs et éducateurs avec les connaissances essentielles pour guider de manière efficace les jeunes apprenants.

Avec des conseils pratiques et des activités inclusives, ce guide met l'accent sur l'esprit critique, le comportement éthique et la communication numérique responsable. Cela permet d'établir un système théorique en définissant des concepts clés et en fournissant des stratégies concrètes pour intégrer les principes de la citoyenneté numérique dans les pratiques éducatives.

Pourquoi la citoyenneté numérique est-elle importante ?

Internet est un outil puissant, mais il peut aussi poser des difficultés. Les jeunes rencontrent souvent des problèmes avec le cyberharcèlement, le manque d'information, l'atteinte à la vie privée, et l'impact à long terme de leurs actions en ligne. Sans guidage approprié, ces défis peuvent non seulement entraver leur développement professionnel mais aussi académique et personnel.

Ce guide cherche à réduire cet écart en mettant à disposition des conseils pratiques et des activités engageantes accessibles à tous. En mettant l'accent sur l'esprit critique, un comportement éthique, et une communication responsable, le guide vise à aider les jeunes apprenants à prendre des décisions réfléchies et à formuler des interactions positives dans des espaces numériques.

À qui est destiné ce guide ?

- **Les jeunes** : Pour les aider à prendre confiance et acquérir des compétences pour naviguer dans un environnement numérique de manière sécurisée et responsable.
- **Les éducateurs et formateurs** : Pour mettre à disposition des outils et des stratégies pour aider les jeunes à développer des compétences numériques citoyennes fortes.
- **Les organisations jeunesse** : Pour améliorer leurs pratiques éducatives en intégrant les principes de citoyenneté numérique à leurs programmes.

À quoi faut-il s'attendre ?

Ce guide est structuré en chapitres clairs, faciles d'utilisation dont chacun se focalisant sur un aspect important de la citoyenneté numérique :

- **Comprendre la citoyenneté numérique** : Introduction aux principes et valeurs qui définissent la participation responsable dans le monde numérique.
- **Les compétences numériques de base** : Vue d'ensemble des compétences essentielles requises pour un engagement effectif sur et numérique.
- **L'éducation aux médias:** Compréhension, reconnaissance et gestion de la désinformation ; outils et stratégies pour identifier des sources fiables et éviter la propagation de mauvaises informations.
- **L'utilisation responsable des réseaux sociaux :** Risques, bénéfices, et e-réputation ; idées sur comment naviguer de façon responsable sur les réseaux sociaux, en équilibrant leurs avantages et risques potentiels.
- **Comprendre et gérer votre empreinte numérique** : Conseils sur la façon dont les actions en ligne forgent les réputations personnelles et les opportunités d'avenir ; conseils pratiques pour protéger les informations personnelles et gérer les paramètres de sécurité.
- **Glossaire** : Section de référence utile définissant les termes et concepts clés liés à la citoyenneté numérique.

Chaque chapitre inclut des conseils pratiques, des exemples concrets, et des activités inclusives pour engager les apprenants de différents milieux. Le guide est fait de sorte à être à la fois informatique et pratique, en s'assurant que les principes de la citoyenneté numérique peuvent être appliqués dans un contexte réel.

Que voulons-nous accomplir ?

Ce guide est bien plus qu'un outil éducatif, c'est un engagement à favoriser une génération de citoyens numériques prévenants, éthiques et responsables. Ensemble, nous pouvons créer un environnement numérique plus sûr, plus inclusif, où tout le monde a l'opportunité d'apprendre, de grandir, et de se connecter.

Embarquons pour ce voyage vers la citoyenneté numérique et donnons le pouvoir d'agir aux jeunes apprenants pour devenir des leaders dans l'ère numérique.

II. COMPRENDRE LA CITOYENNETÉ NUMÉRIQUE

La citoyenneté numérique fait référence à une utilisation responsable et appropriée de la technologie pour quiconque s'engageant dans l'environnement numérique. Cela inclut différents comportements, compétences, et connaissances, tels que protéger les informations personnelles, s'engager dans une communication respectueuse, et contribuer positivement aux communautés en lignes, nécessaires pour naviguer à travers le monde numérique de manière sûre et effective.

Le concept de citoyenneté numérique est crucial dans le monde interconnecté d'aujourd'hui, où les interactions numériques sont d'importantes parties de la vie quotidienne. La citoyenneté numérique peut influencer significativement votre comportement en ligne de plusieurs manières différentes, comme vous encourager à vous comporter de manière responsable en ligne à travers une communication respectueuse. Les utilisateurs en ligne sont plus à même de s'engager dans des interactions polies et considérées, réduisant les cas de cyberharcèlement et d'harcèlement en ligne. Il permet également le partage et la création de contenu éthique à mesure que tout le monde prend conscience des lois sur les droits d'auteur et les droits de propriété intellectuelle.

En suivant les principes de la citoyenneté numérique, vous devenez plus prudent sur la manière de protéger votre confidentialité et apprenez à gérer votre empreinte numérique et protéger vos informations personnelles, réduisant les risques d'usurpation d'identité et d'exploitation en ligne. Les citoyens numériques sont mieux équipés pour identifier et éviter les arnaques en ligne, la désinformation, et potentiellement, du contenu dangereux.

D'autre part, l'éducation à la citoyenneté numérique améliore votre culture numérique en développant des compétences telles que l'esprit critique. Vous apprenez à évaluer une information en ligne, ce qui conduit à faire des choix et à avoir des opinions plus informées, et rend la prise de décision plus facile.

La citoyenneté numérique promeut aussi la participation active dans les communications en ligne. Vous êtes plus à même de vous engager dans un activisme en ligne positif, contribuer de manière constructive à des communautés numériques, et comprendre l'impact des actions en ligne. Cela promeut l'empathie et la considération des autres dans les espaces numériques.

Les droits et devoirs des citoyens numériques

L'un des droits fondamentaux de la citoyenneté numériques et la protection des données personnelles. Le RGPD (Règlement Général sur la protection des données), mis en place par l'Union européenne en 2018, est un point de repère de réglementation qui cherche à protéger la confidentialité et les informations personnelles des individus au sein de l'UE.

LES ASPECTS CLÉS DU RGPD INCLUENT :

Protection des données
S'assurer que les informations personnelles sont collectées, transformées et gardées de manière sécurisée.

Droit à l'accès
Permettre aux individus d'accéder à leurs informations personnelles et en comprendre l'utilisation.

Consentement
Consentement clair et explicite des individus est requis avant de collecter leurs données.

Droit à l'oubli
Fournir aux individus le droit à demander la suppression de leurs informations personnelles sous certaines conditions.

Le RGPD fixe des normes élevées en matière de protection des données et de la vie privée, servant de modèle pour d'autres régions et renforçant les droits des citoyens numériques.

Plus d'information sur la page **GDPR.eu page "What is GDPR, the EU's new data protection law?" (Wolford B, n.d.)**

Il existe plusieurs manières de chercher de l'aide et de l'assistance en tant que citoyen numérique lorsque vous rencontrez des problèmes en ligne :

- **Communautés de soutien en ligne :** Rejoindre des forums et des groupes où les individus partagent leurs expériences et conseils pour gérer les défis numériques.
- **Ligne d'assistance et soutien téléphonique :** Utiliser des lignes d'assistance dédiées aux problèmes tels que le cyberharcèlement, le harcèlement en ligne ou les addictions numériques.
- **Mécanismes de signalement :** Utiliser les outils de signalement sur les plateformes de réseaux sociaux et sites web pour signaler du contenu inapproprié ou dangereux.
- **Ressources éducatives :** Accéder aux cours en ligne et tutoriels pour améliorer l'éducation numérique et la compréhension des droits numériques.

Les informations sur les ressources disponibles vous permettent d'aborder et de résoudre efficacement les problèmes en ligne. Pour plus d'informations, consultez le site **Find a Helpline**.

Le respect est la pierre angulaire de la citoyenneté numérique. Pour garantir un environnement en ligne respectueux, vous devriez :

Pratiquer l'empathie

Comprendre et considérer les perspectives et sentiments des autres dans les interactions numériques.

Communiquer poliment

Utiliser un ton et un langage respectueux, même en cas de désaccords ou de débats.

Respecter la confidentialité

Reconnaître et honorer la vie privée d'autrui en ne partageant pas d'informations personnelles sans leur consentement.

Être responsable

Assumer la responsabilité de ses actes et de ses paroles en ligne et être prêt à présenter des excuses et à corriger les erreurs.

Les citoyens numériques sont aussi responsables pour reconnaître et adresser la discrimination et les comportements dangereux en ligne. Cela implique :

IDENTIFIER LA DISCRIMINATION

Soyez conscient du contenu biaisé ou préjugé qui cible des individus ou groupes en fonction de l'origine, le sexe, la religion ou d'autres caractéristiques.

ÉDUQUER LES AUTRES

Faites prendre conscience de l'impact de la discrimination et promouvez l'inclusivité et la diversité en ligne.

SIGNALER LES CONTENUS DANGEREUX

Utilisez les outils des plateformes pour signaler et effacer du contenu abusif ou dangereux.

SOUTENIR LES VICTIMES

Offrez soutien et ressources aux individus qui ont fait face à la discrimination en ligne et au harcèlement.

En vous opposant activement à la discrimination et aux comportements préjudiciables, vous contribuez à créer un espace numérique plus sûr et plus équitable pour tous les utilisateurs.

III. LES COMPÉTENCES NUMÉRIQUES DE BASE

Définition des compétences numériques

Défini par le Cadre Européen des Compétences Numériques (**DigComp**), les compétences numériques sont essentielles pour s'engager de manière confiante, critique, et responsable avec les technologies numériques dans divers contextes, y compris l'éducation, l'emploi et la vie personnelle. Ils englobent un large éventail de compétences, allant de la maîtrise élémentaire de l'informatique aux capacités avancées en matière de résolution de problèmes numériques et d'utilisation éthique de la technologie.

Les cadres comme DigComp vous fournissent une approche structurée pour comprendre la nature multidimensionnelle des compétences numériques. Il souligne l'importance de l'accessibilité, en veillant à ce que les compétences numériques soient inclusives et applicables à tous les citoyens, indépendamment de leur formation ou de leurs capacités.

Source: Comprendre DigComp, European Commission

La maîtrise de l'information et l'esprit critique

Rechercher et gérer l'information

L'éducation sur l'information implique non seulement de trouver des informations mais aussi d'évaluer leur qualité et leur pertinence. Des techniques telles que l'utilisation d'opérateurs de recherche avancée, évaluer de manière critique les recherches et les résultats et reconnaître les sources fiables sont essentiels pour naviguer à travers les vastes quantités

d'informations disponibles en ligne. Des outils comme **Google Scholar**, des bases de données académiques, et les médias de presse réputés sont des exemples de ressources que vous pouvez utiliser pour obtenir des renseignements fiables.

En outre, la gestion de l'information comprend la compréhension des façons de stocker, de récupérer et de protéger les données. Cela comprend l'utilisation d'outils numériques pour organiser l'information, tels que les solutions de stockage en cloud, et la compréhension des principes de gestion des données, telles que les conventions de nommage des fichiers et les stratégies de sauvegarde des données. Cela implique également de reconnaître les implications éthiques de l'utilisation des données, telles que le respect des droits de propriété intellectuelle et de la vie privée.

Évaluer les sources

La désinformation est très répandue en ligne, ce qui veut dire que vous devriez développer la capacité à évaluer les sources d'informations que vous rencontrez de manière critique. Cela implique questionner les références des auteurs, l'exactitude de l'information et la présence de potentiels polarisation. La lecture latérale, la vérification d'informations avec plusieurs sources, et l'utilisation d'outils comme les sites de vérification de faits (i.e, **Snopes**, **FactCheck.org**) sont des stratégies concrètes qui vous aident dans ce processus d'évaluation.

De plus, il est important de comprendre l'impact des algorithmes et la diffusion de contenu personnalisé, qui peut fausser l'information qui vous est présentée basée sur vos comportements précédents et préférences. Apprendre sur l'influence des algorithmes sur votre environnement d'information peut vous aider à chercher d'autres perspectives et d'éviter d'éternelles répétitions.

La résolution de problèmes et l'évaluation critique

La résolution de problèmes dans les contextes numériques est plus que le dépannage technique ; elle exige un état d'esprit d'évaluation critique et une pensée adaptative. Les compétences en résolution de problèmes

numériques comprennent l'identification des besoins numériques, l'analyse des solutions potentielles et le choix des stratégies les plus efficaces. Par exemple, lorsque vous faites face à une menace de sécurité en ligne, comme l'hameçonnage, vous devez évaluer la situation, reconnaître la menace et prendre les mesures appropriées, telles que signaler l'incident et renforcer vos mesures de sécurité.

Les approches éducatives qui intègrent des simulations numériques, des jeux de rôle et des activités interactives de résolution de problèmes peuvent aider les jeunes à développer ces compétences d'une manière engageante et pratique. En fournissant des scénarios concrets qui nécessitent une évaluation critique et la prise de décisions, les éducateurs peuvent mieux préparer leurs élèves aux complexités du monde numérique.

La communication et création de contenu

Les compétences de communication numérique

La communication numérique est la pierre angulaire de la compétence numérique, incluant les compétences requises pour interagir efficacement dans de nombreux environnements en ligne. Des communicateurs numériques efficaces sont capables d'adapter leurs messages à leur audience, choisir les canaux appropriés pour la communication, et maintenir le professionnalisme et le respect dans leurs engagements digitaux.

Acquérir des compétences en communication inclut explorer le concept de « netiquette », c'est-à-dire les lignes directrices pour un comportement courtois et respectueux en ligne. Cela implique aussi des discussions sur l'empreinte numérique et la permanence des actions en

ligne, surlignant combien il est important de réfléchir avant de poster et de comprendre les effets à long terme de la communication numérique.

Les outils de collaboration en ligne

La collaboration est un composant clé du travail moderne et de l'environnement d'apprentissage, facilité par des outils numériques qui permettent aux personnes de travailler ensemble peu importe leur emplacement physique. Les outils collaboratifs en ligne, tels que **Slack**, **Trello** et **Asana**, offrent des plateformes pour permettre aux groupes de communiquer, partager des documents et gérer des projets en temps réel. Connaître le fonctionnement de ces outils est considéré comme une compétence numérique, car ils sont grandement utilisés tant dans le cadre éducatif que professionnel pour améliorer la productivité et promouvoir le travail.

Ces outils peuvent être intégrés dans les activités de classe pour apprendre aux élèves le management de projet, la communication et la collaboration dans les espaces numériques. Par exemple, les projets de groupe qui ont besoin que les élèves utilisent des outils de collaboration numérique peuvent aider à développer des compétences pratiques dans les tâches de management, communiquer effectivement et travailler ensemble vers un but commun.

Les bases de la création de contenu

Le contenu numérique implique de produire de nombreuses formes de média numériques, telles que des textes, des images, vidéos et contenu interactif. Cette compétence n'est pas limitée aux compétences techniques et cela implique de la créativité, la compréhension des besoins du public, et appliquer des considérations éthiques, telles que respecter les droits d'auteurs et éviter le plagiat. Des

compétences de base sur la création de contenu incluent d'utiliser des outils numériques pour éditer, élaborer et publier du contenu, ainsi que comprendre les principes du storytelling numérique.

Vous devriez essayer avec différentes plateformes de création de contenu, du blog à la production vidéo, construire vos compétences et exprimer vos idées. Comprendre les bases de la création de contenu implique aussi de reconnaître le rôle des design visuels et l'expérience des utilisateurs, qui sont essentiels pour créer du contenu numérique engageant et accessible. De plus, vous devriez apprendre sur l'importance de l'accessibilité des contenus numériques, vous assurant que vos créations sont inclusives et que de nombreux publics peuvent les utiliser.

IV. L'ÉDUCATION AUX MÉDIAS

Définition et portée

L'éducation aux médias vous habilite à accéder, analyser, évaluer, créer et vous engager avec du contenu médiatique sur diverses plateformes. Cela implique une compréhension de la nature des messages des médias, le procédé de production des médias, et le rôle que les médias jouent à modeler la société. L'éducation aux médias comprend également la reconnaissance de la dynamique du pouvoir dans la propriété des médias et les influences économiques, politiques et culturelles qui animent le contenu médiatique.

La portée des médias s'est étendue de manière significative dans l'ère numérique, incluant les médias traditionnels comme les journaux et la télévision, ainsi que les médias numériques tels que les réseaux sociaux, podcasts, blogs et services de streaming. Alors que de nouvelles technologies apparaissent, comme l'intelligence artificielle et la réalité augmentée, la portée de l'éducation aux médias continue à évoluer, requièrent une éducation et une adaptation continue. Ce plus grand cadre montre le besoin d'une approche compréhensive qui intègre l'éducation aux médias pour de nombreux sujets et aspects de la vie de tous les jours.

Comprendre les messages des médias

Comprendre les messages des médias nécessite la capacité d'analyser de manière critique comment les médias construisent la réalité. Les messages des médias ne sont pas neutres; ils reflètent les intentions et les préjugés de leurs créateurs, ce qui peut influencer la façon dont vous percevez et interprétez l'information. Les producteurs de médias utilisent diverses techniques, comme le cadrage, la sélection des sources, l'imagerie visuelle et les appels émotionnels, pour façonner leurs messages et affecter vos perceptions.

Par exemple, l'utilisation de visuels dramatiques dans de nouvelles couvertures peut amplifier l'impact émotionnel de l'histoire, amenant potentiellement à accroître l'intérêt ou la panique du public. De la même façon, l'oubli de certaines perspectives ou voix peuvent altérer la compréhension d'un problème, présentant une vue à sens unique. En apprenant à déconstruire ces messages, vous pouvez identifier les suppositions et biais qui sont sous-entendus, amenant à une compréhension plus nuancée des médias.

Le développement des compétences analytiques peut être supporté à travers des activités qui impliquent de comparer différentes images médiatiques d'un même événement, discuter de l'influence de la propriété des médias sur la couverture médiatique.

Reconnaître et gérer la désinformation

La désinformation est un défi omniprésent dans le paysage médiatique actuel, où la vitesse et la portée de la communication numérique peuvent amplifier les informations fausses ou trompeuses. Afin de reconnaître et gérer l'impact de la désinformation, il est important de comprendre ces différents aspects :

- **Le contenu fabriqué :** Inclut des informations fausses créées pour tromper. Par exemple, un article de fake news qui clame qu'une célébrité est morte peut se diffuser rapidement sur les réseaux sociaux, causant de la confusion et de la détresse.
- **Le clickbait :** Fait référence à des titres sensationnels ou trompeurs conçus pour attirer les clics et le trafic vers les sites Web, souvent au détriment de l'exactitude. Par exemple, un titre comme 'Vous ne croirez pas à ce que ce politicien a fait!' peut conduire à un article qui exagère ou déforme les faits pour attirer les lecteurs.
- **Les deepfakes :** Des vidéos manipulées ou des images qui montrent que des

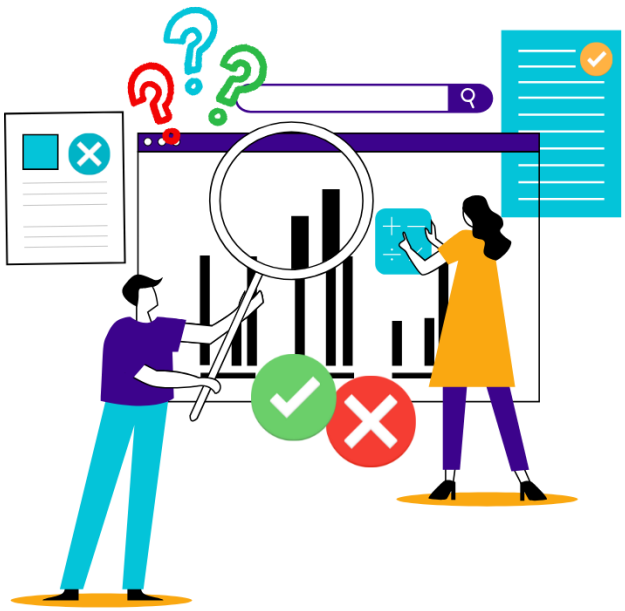
gens disent ou font des choses qu'ils n'ont jamais faites en utilisant l'intelligence artificielle. Un exemple pourrait être une vidéo deepfake d'une figure publique, tel qu'un politicien, faisant une annonce qu'il n'a jamais faite, qui peut-être utiliser pour diffuser de faux récits ou les discréditer.

- **Le contenu trompeur :** Des informations qui déforment la réalité ou présentent des faits d'une manière déformée. Par exemple, utiliser une photo d'un événement sans lien pour représenter les actualités peut tromper les spectateurs à penser que c'est connecté à l'histoire qui est racontée.
- **Le faux contexte :** Une information véritable présenté dans un contexte trompeur, peut altérer son sens profond. Un exemple est une vieille photo d'une manifestation qui est utilisée pour représenter un événement actuel, donnant aux spectateurs l'impression que la situation en cours est plus grande qu'il n'y paraît.
- **Le contenu imposteur :** Implique du contenu qui imite de vraies sources. Par exemple, de faux sites web imitant l'apparence des médias réputés pour répandre de fausses histoires, ce qui rend difficile pour les lecteurs de faire la distinction entre les vraies et les fausses nouvelles.
- **La satire ou parodie :** Le contenu satirique, tels que les articles de site web comme **The Onion**, prévu pour divertir, mais qui peuvent être confondus avec un reportage factuel si le public n'est pas conscient de sa nature satirique.
- **La fausse attribution :** Créditer un contenu ou une citation à une source fausse ou inexistante. Par exemple, attribuer une citation fabriquée à un scientifique ou à une figure publique bien connue pour donner une crédibilité injustifiée à une allégation.
- **Les rumeurs et canulars :** Informations non vérifiées qui se répandent sur les réseaux sociaux, créant souvent de fausses impressions ou la panique. Un exemple classique est la propagation virale de canulars concernant des rappels de produits ou de faux conseils de santé, comme le mythe selon lequel boire de l'eau chaude peut prévenir la COVID-19.

Le contrôle et la vérification des faits

La vérification des faits ou fact-checking implique systématiquement d'évaluer l'exactitude et la fiabilité des informations en consultant de nombreuses sources, examinant les preuves, et utiliser des outils de vérification. Les actions clés d'une vérification des faits efficace sont :

- **L'évaluation de la source :** Commencez par vérifier la crédibilité de la source. Les sources réputées ont généralement des normes éditoriales transparentes, fournissent des détails sur les auteurs et divulguent tout conflit d'intérêt potentiel.
- **Le recoupement ou croisement des sources :** Comparez les informations avec d'autres sources réputées. La cohérence entre plusieurs sources crédibles augmente la probabilité que l'information soit exacte.



- **L'utilisation d'outils de vérification :** Des outils comme **Google Reverse Image Search** peuvent aider à vérifier l'authenticité des images, tandis que des extensions de navigateur comme **NewsGuard** fournissent des évaluations sur la crédibilité des sites d'actualités.
- **La vérification de l'expertise de l'auteur :** Évaluez si l'auteur est qualifié pour parler du sujet. Les experts ou les autorités reconnues dans le domaine sont plus susceptibles de fournir des informations fiables.
- **L'analyse des preuves :** Recherchez des preuves à l'appui, telles que des données, des résultats de recherche ou des citations directes d'experts. Les informations fiables sont généralement bien étayées par des preuves pouvant être vérifiées de manière indépendante.

La consommation éthique des médias

La consommation médiatique éthique implique d'être précautionneux dans le choix des médias que nous faisons et l'impact que ces choix peuvent avoir sur les individus et la société. Cela requiert une approche critique pour partager et sélectionner du contenu multimédia, en considérant des facteurs comme la précision, les biais, la représentation et les effets potentiels sur le discours public. Des consommateurs de médias éthiques sont proactifs à chercher diverses perspectives, questionnant l'intention derrière les messages des médias et évitant le partage d'informations dangereuses ou fausses.

Afin de consommer des médias éthiquement, il est important de comprendre l'influence des algorithmes sur les médias qu'on rencontre. Les algorithmes des plateformes de réseaux sociaux et de moteur de recherche personnalisent leur contenu en se basant sur votre comportement, créant des chambres d'écho qui renforcent vos croyances existantes et limitent l'exposition aux points de vue différents. En étant conscient de ces influences, vous pouvez prendre des mesures pour diversifier votre utilisation des médias, telles que suivre des sources avec différentes perspectives en utilisant des outils qui traquent les préjugés des médias ou à chercher de manière délibérée du contenu qui remet en question vos hypothèses.

La création de contenu responsable

En tant que créateur, vous devriez faire attention au potentiel impact de votre contenu, considérant comment cela peut affecter de nombreuses audiences, particulièrement vulnérables ou des groupes marginalisés. Cela inclut d'éviter du langage ou des images qui perpétuent des stéréotypes, d'être sûr que vous êtes juste et de respecter la vie privée des individus et leur consentement dans les représentations médiatiques. Par exemple, lorsque vous créez du contenu qui implique de vraies personnes, il est important d'obtenir leur consentement et de promouvoir un contexte pour éviter la mauvaise représentation.

En favorisant la capacité à s'engager de manière critique avec les messages médiatiques, à reconnaître et gérer la désinformation, et à créer du contenu de manière éthique, vous pouvez vous donner et donner aux autres les moyens de naviguer dans le paysage médiatique avec confiance et intégrité. À mesure que les médias continuent d'évoluer, les principes de la littératie médiatique resteront essentiels pour promouvoir une société plus inclusive, équitable et engagée de manière critique.

V. L'UTILISATION RESPONSABLE DES RÉSEAUX SOCIAUX

Selon une étude, 97% des 16-29 ans dans l'Union européenne utilisent internet tous les jours, et 83% ont utilisé une plateforme de réseaux sociaux en 2023 (Eurostat,2023). étant donné que l'utilisation des plateformes numériques est répandue parmi les jeunes, vous devriez comprendre les avantages et les inconvénients de l'utilisation des réseaux sociaux.

Les avantages des réseaux sociaux

La culture en ligne permet la communication et la connexion avec d'autres citoyens numériques, et en construisant un capital social, la plateforme des réseaux sociaux peut améliorer le bien-être. Cela fournit aussi un environnement pour étendre vos intérêts, connaissances et compétences ainsi que pour le divertissement et le soutien.

De plus, cela vous aide à rester informé sur ce qui se passe dans le monde. De nombreuses chaînes d'informations ont des profils sur les réseaux sociaux, ou elles partagent les informations les plus importantes et concises de façon compréhensible, ce qui permet de rester à jour.

Les réseaux sociaux peuvent être particulièrement utiles pour les jeunes dans le besoin, l'environnement en ligne simplifie l'accès à de l'aide professionnelle tout en préservant l'anonymat. De plus, grâce à des amis et des personnes partageant les mêmes idées dans des groupes en ligne, vous pouvez recevoir un soutien émotionnel immédiat. Les réseaux sociaux diminuent les sentiments de solitude et d'isolation. Les communautés en ligne qui sont modérées par des professionnels de centres de santé mentale sont exceptionnellement précieux - ils créent un environnement sûr pour partager des émotions et recevoir le soutien de leur pair.

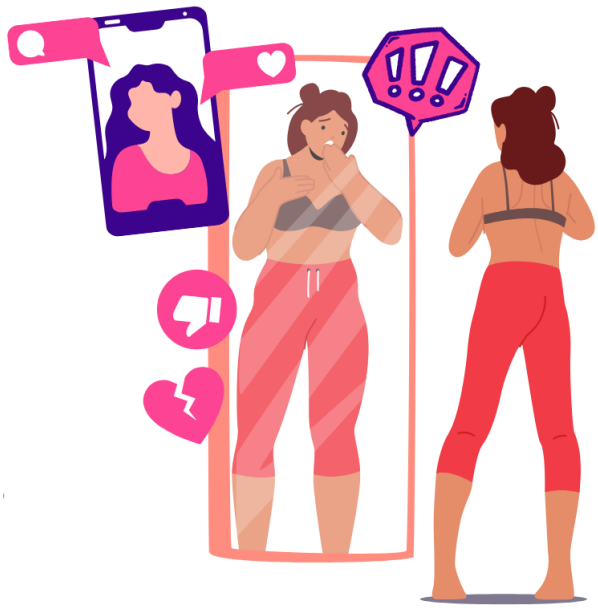
Certains bloggeurs et influenceurs parlent des problèmes en lien avec la santé mentale et offrent de l'espace ou les individus peuvent partager leurs témoignages. Suivre l'histoire de la réhabilitation de quelqu'un peut vous encourager à surmonter vos problèmes/difficultés.

Les risques des réseaux sociaux

Tout en reconnaissant les avantages des réseaux sociaux, vous devez être conscient des divers pièges sur Internet qui peuvent représenter un risque et une menace. Statistiquement parlant, l'exposition au risque augmente avec la fréquence de la présence en ligne et l'intensité de l'engagement. Une multitude de facteurs, y compris l'âge, le sexe, le niveau d'éducation et le milieu culturel, influencent le niveau de vulnérabilité aux risques et leurs répercussions.

Avec l'augmentation de l'utilisation des outils de communication, réseaux sociaux, et plateformes de jeux vidéo, vous êtes à risque de harcèlement en ligne, stalking en ligne, messages incendiaires, messages de haine, prédation sexuelle ainsi que l'usurpation d'identité. Le monde virtuel contient aussi divers contenus dangereux de nature sexuelle ou violente, désinformation, racisme, antisémitisme et bien plus encore, qui ont d'importantes répercussions sur la santé mentale sur les jeunes et la société en général.

De plus, les adolescentes sont très vulnérables aux attaques en ligne du à la comparaison sociale sur l'attractivité physique et les faux standards de beauté. Les réseaux sociaux grouillent de photos avec des individus utilisant des filtres de beauté et de retouches pour créer des images non réalistes de visages et corps parfaits. Due à la forte exposition à de tels contenus, les



femmes sont vulnérables à l'insatisfaction corporelle et à la perception négative de soi, ce qui est également lié à une faible estime de soi et peut entraîner des problèmes de santé mentale ou des troubles alimentaires.

Par conséquent, les publications cools d'événements, de vacances et de festivals peuvent déclencher la peur de manquer quelque chose (FOMO) et des sentiments de jalousie et d'insuffisance personnelle. Nous oublions souvent de prendre en compte que beaucoup de ces publications sont mises en scène et ne reflètent pas la vie réelle des utilisateurs.

Le divertissement des plateformes en ligne vous permet de 'vous échapper' du monde réel. En recherchant la dopamine, vous, en tant que citoyen numérique, consommez souvent trop de contenu en ligne, ce qui peut entraîner une dépendance en ligne. Un tel comportement est épuisant en termes de temps et a un impact négatif sur votre santé physique, vos relations sociales, votre concentration et votre productivité, ce qui peut à son tour entraîner une mauvaise performance académique ou professionnelle. Par conséquent, cela entraîne un inconfort psychologique et des répercussions sur la santé. Les réseaux sociaux sont également associés à des perturbations du sommeil et à l'anxiété.

De plus, vous devez être conscient que tout ce qui est en ligne n'est pas vrai et que de nombreux profils partagent de la désinformation, ce qui peut être très dangereux si pris au sérieux.

Les aspects controversés des réseaux sociaux : le rôle des algorithmes

Les algorithmes, en tant qu'ensemble de règles, de calculs et de processus de prise de décision que les plateformes utilisent pour trier, recommander et présenter du contenu aux utilisateurs, sont conçus pour prioriser le contenu avec lequel les utilisateurs sont les plus susceptibles d'interagir, en se basant sur des données comportementales antérieures telles que les likes, les partages et le temps passé sur un contenu spécifique.

Un aspect positif de l'algorithme des réseaux sociaux est l'amélioration de l'expérience des utilisateurs, car le contenu est personnalisé, réduisant la surcharge d'information et promettant les informations intéressantes pour l'utilisateur. Par exemple, les algorithmes vous aident à trouver des communautés et des informations en lien avec vos intérêts, rendant les plateformes plus facile d'utilisation.

Cependant, une préoccupation majeure est le renforcement des chambres d'écho, ou vous êtes principalement à du contenu qui s'aligne avec vos opinions existantes. Les algorithmes priorisent le contenu sensationnel, amplifiant la désinformation, à mesure que l'engagement augmente. Si vous n'avez pas connaissance de ces manipulations, vous pouvez facilement tomber dans les chambres d'écho qui renforce les biais et promeut la désinformation, ce qui peut amener à la polarisation et la radicalisation.

Les effets psychologiques de ces algorithmes sont aussi importants. Une exposition constante à du contenu chargée émotionnellement peut amener à de l'anxiété, de la dépression et des sentiments d'isolation. De plus, la nature addictive des plateformes guidées par des algorithmes contribue à l'utilisation excessive des réseaux sociaux, où vous vous retrouvez dans des cycles interminables de défilement sans réaliser le prix émotionnel qu'il prend.

Les effets de la législation européenne sur les services numériques obligeant les plateformes à divulguer leurs algorithmes de recommandation sont encore à venir.

Le clic conscient : conseils pour une utilisation responsable des réseaux sociaux

L'environnement en ligne devrait être sûr et sécurisé et rendre tous les utilisateurs à l'aise. Les gens utilisent souvent des plateformes pour socialiser, du networking professionnel, ou de l'activisme, mais la manière dont ils s'engagent en ligne peut avoir des effets à long terme sur leurs vies personnels et sur la société. Les compétences telles que l'esprit critique,

l'empathie et le numérique, l'éducation aux médias et à l'information sont vitales pour bien utiliser les réseaux sociaux qui sont utilisés dans le cadre du citoyen numérique. Pour devenir un citoyen numérique responsable, vous devriez suivre toutes ces recommandations :

- **Réfléchissez avant de poster :** Les réseaux sociaux encouragent les posts impulsifs. Les publications faites par colère ou frustration peuvent mal refléter votre caractère et peuvent être mal interprétés par les autres. Une approche consciente lors du partage peut éviter les malentendus ou de mettre en péril votre réputation en ligne.
- **Comprenez les conséquences de partager des informations personnelles** : Partager des informations personnelles, telles que les données personnelles, la localisation, les intentions de voyages, ou des opinions sensibles, peuvent vous mettre en danger. Ces posts peuvent être utilisés pour traquer vos activités, compromettre votre confidentialité, ou même amener à une usurpation d'identité.
- **Faites attention aux activités criminelles :** Il est essentiel de rester vigilant contre les risques humains et technologiques dans les espaces numériques. Reconnaître et éviter l'hameçonnage et identifier les tentatives de vols ainsi que les cyberattaques. Évitez de cliquer sur des liens inconnus ou suspects et télécharger des fichiers de sources non vérifiées.
- **Vérifier les informations avant de les partager :** Avant de partager des articles ou des posts, assurez-vous qu'ils viennent de sources fiables. Vous devriez développer des compétences d'esprit critique pour discerner le contenu factuel des rumeurs ou pièges à cliques. Les messages inexacts ou trompeurs nuisent non seulement à votre crédibilité, mais contribuent également au préjudice social.

- **Maintenez le respect et l'empathie dans les interactions en ligne :** Les réseaux sociaux peuvent être un espace pour des dialogues constructifs et sains. Éviter l'engagement dans des disputes en ligne ou les attaques personnelles, car elles prennent rapidement de l'ampleur et laissent des impressions négatives. Pratiquer l'empathie numérique et écouter les points de vue différents de manière respectueuse, parce que cela promeut un environnement en ligne positif.
- **Employez un engagement actif et positif :** Votre réputation numérique peut être mise en avant à travers des contributions considérées. Que ce soit sur des forums professionnels ou sur les réseaux sociaux, contribuant avec de précieuses idées et s'entraîner à l'empathie numérique peut aider à former une identité numérique forte et positive. Cela inclut de s'engager dans des discussions importantes, partager du contenu réfléchi, et supporter des initiatives qui promeuvent l'inclusion et la responsabilité sociale en ligne.
- **Considérez votre public** : Les réseaux sociaux sont souvent publics ou semi-publics, et l'audience peut être plus grande que prévu. Des posts prévus pour vos amis peuvent facilement atteindre de futurs employeurs, des institutions académiques ou des spectateurs imprévus. Maintenir un ton typique, décent et respectueux et utiliser la netiquette peut protéger votre réputation en ligne.
- **Évitez la surconsommation de réseaux sociaux :** Limitez la consommation de réseaux sociaux en faisant attention à votre temps d'écran. De nombreux smartphones permettent aux utilisateurs de mettre des limites de temps pour les applications, incluant les réseaux sociaux, et

d'envoyer des notifications quand la limite est atteinte. Ces fonctionnalités aident à gérer le temps d'écran et encouragent la prise de conscience sur un usage excessif.

E-réputation : Comment communiquer et vous présenter en ligne

La manière dont vous êtes perçu en ligne, entendue comme votre e-réputation, est un reflet direct de votre présence en ligne. La présence en ligne ou e-présence est liée à la sécurité en ligne et au comportement éthique dans les environnements en ligne. La présence en ligne va au-delà de la participation passive ; elle consiste à cultiver activement une empreinte numérique par le biais d'interactions, de création de contenu et de comportement éthique, soulignant l'importance de la littératie numérique et de la conscience de soi pour façonner votre personnalité publique.

Votre identité en ligne peut être formée à la fois intentionnellement et involontairement. La création intentionnelle de l'identité implique le profil, les photos, les messages et les informations personnelles que vous décidez de mettre en ligne. Les caractéristiques involontaires de votre identité sont établies par quelqu'un d'autre qui télécharge quelque chose à votre sujet, par exemple une balise dans une photo ou un message. De nos jours, les plateformes vous notifient que vous avez été marqué et offrent la possibilité de refuser ou de confirmer le marquage. Cette option vous donne un certain niveau de contrôle sur votre identité en ligne indirecte.

Tout ce qui est partagé en ligne laisse une trace, alors il est essentiel d'être conscient sur ce qui va être partagé et son impact potentiel. La réputation numérique que vous créez peut être facilement vue à travers des recherches en ligne de votre prénom ou d'autres données personnelles identifiables. Les résultats de recherche peuvent inclure des posts sur les réseaux sociaux, des commentaires, des profils professionnels ou du contenu public associé à votre identité.

Une présence en ligne positive, telle que les réussites professionnelles ou un engagement constructif sur des forums, améliore votre réputation. D'autre part, du contenu négatif, comme un comportement inapproprié sur les réseaux sociaux, des commentaires controversés ou du partage de fausses informations, peuvent endommager votre image et avoir un impact négatif sur de futures opportunités de carrières. Par exemple, des candidatures pour un travail ou à l'université peuvent être rejetées en raison de la présélection initiale des candidats sur les réseaux sociaux.

VI. COMPRENDRE ET GÉRER VOTRE EMPREINTE NUMÉRIQUE

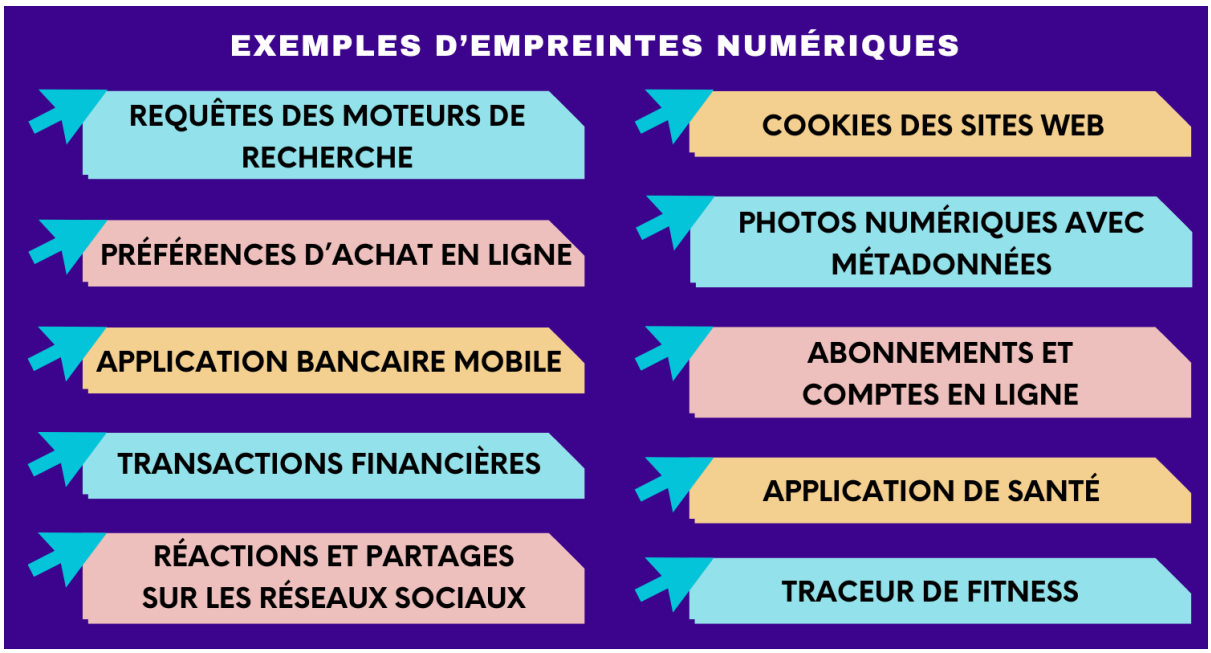
Dans le monde interconnecté d'aujourd'hui, vos activités en ligne laissent des données derrière vous connues comme l'empreinte numérique.

Une empreinte numérique fait référence à la trace de données que vous créez en utilisant l'Internet. Elle comprend toutes les informations sur vos activités en ligne, les interactions et la présence à travers diverses plateformes numériques. Vous pouvez rencontrer deux types d'empreintes numériques – active et passive.

Une empreinte numérique active se réfère aux données que vous partagez intentionnellement en ligne, dont vous êtes conscient et que vous contrôlez. Cela inclut n'importe quelle information que vous postez ou soumettez, tel que les posts sur les réseaux sociaux (sur des plateformes comme Facebook, X ou Instagram), les revues en ligne que vous écrivez pour vos produits ou vos services, la création de comptes, incluant les informations soumises quand vous créez des comptes sur divers sites web.

Une empreinte numérique passive est des informations collectées sur vous sans votre implication directe. Cela inclut l'historique de navigation enregistré par les sites Web, les enregistrements d'adresses IP, les données de localisation des appareils mobiles et les données collectées par les applications exécutées en arrière-plan.

Chaque action que vous faites en ligne laisse des traces et parfois votre empreinte numérique peut se retrouver là où vous ne le souhaitez pas. Voici quelques exemples d'empreintes numériques afin que vous puissiez en être plus conscient :



Le lien entre l'empreinte numérique et l' e-réputation est important, car l'empreinte numérique forme les fondations de l' e-réputation de quelqu'un. Comme nous l'avons mentionnée plus haut, une empreinte numérique englobe toutes les données et traces faites par un individu sur les activités en ligne, de manière intentionnelle et non intentionnelle. Cela inclut des posts sur les réseaux sociaux, commentaires, achats en ligne et historique de recherche parmi tant d'autres.

L'empreinte numérique d'une personne a un impact direct sur son e-réputation car elle reflète ses valeurs, ses intérêts et ses comportements. Les employeurs potentiels, les partenaires commerciaux et même les connaissances personnelles évaluent souvent l'e-réputation d'une personne en examinant son empreinte numérique. Une empreinte numérique positive peut améliorer votre image professionnelle et personnelle, en mettant en avant votre expertise et votre fiabilité. À l'inverse, une empreinte numérique négative, comme un contenu inapproprié ou des opinions controversées, peut nuire à la crédibilité et à la confiance, et faire perdre des opportunités.

La gestion de votre empreinte numérique est essentielle pour maintenir une e-réputation favorable. Cela implique de faire attention au contenu partagé en ligne, d'utiliser les paramètres de confidentialité et de contrôler régulièrement sa présence en ligne pour s'assurer qu'elle correspond à l'image personnelle et professionnelle que l'on souhaite donner.

Les pièges potentiels

Les empreintes numériques non gérées peuvent amener à de nombreux risques en plus d'une e-réputation négative :

- **Les risques liés à la vie privée :** Les empreintes numériques peuvent vous exposer à des risques de confidentialité, incluant le cyber stalking, le harcèlement et même les menaces physiques. Les informations partagées en ligne peuvent être utilisées avec malveillance.
- **Les menaces de sécurité :** Les cybercriminels peuvent exploiter des empreintes numériques pour le vol d'identité, des arnaques d'hameçonnage, et de la falsification de compte. Exposer des informations telles que les noms d'utilisateurs et les mots de passe peut être utilisé pour gagner un accès non autorisé à vos comptes, résultant à des pertes financières et d'autres dommages.
- **Les publicités ciblées et l'exploitation des données :** Les entreprises utilisent les empreintes numériques pour suivre le comportement et les préférences des utilisateurs, permettant une publicité ciblée. Bien que cela puisse améliorer l'expérience utilisateur, cela soulève également des préoccupations au sujet de la confidentialité des données et de la mesure dans laquelle les renseignements personnels sont utilisés sans consentement explicite.
- **L'impact environnemental :** Le stockage et l'analyse des données numériques contribuent à la consommation d'énergie et aux émissions de carbone. Faire attention à votre empreinte numérique peut aider à gérer votre impact environnemental.

L’aspect environnemental

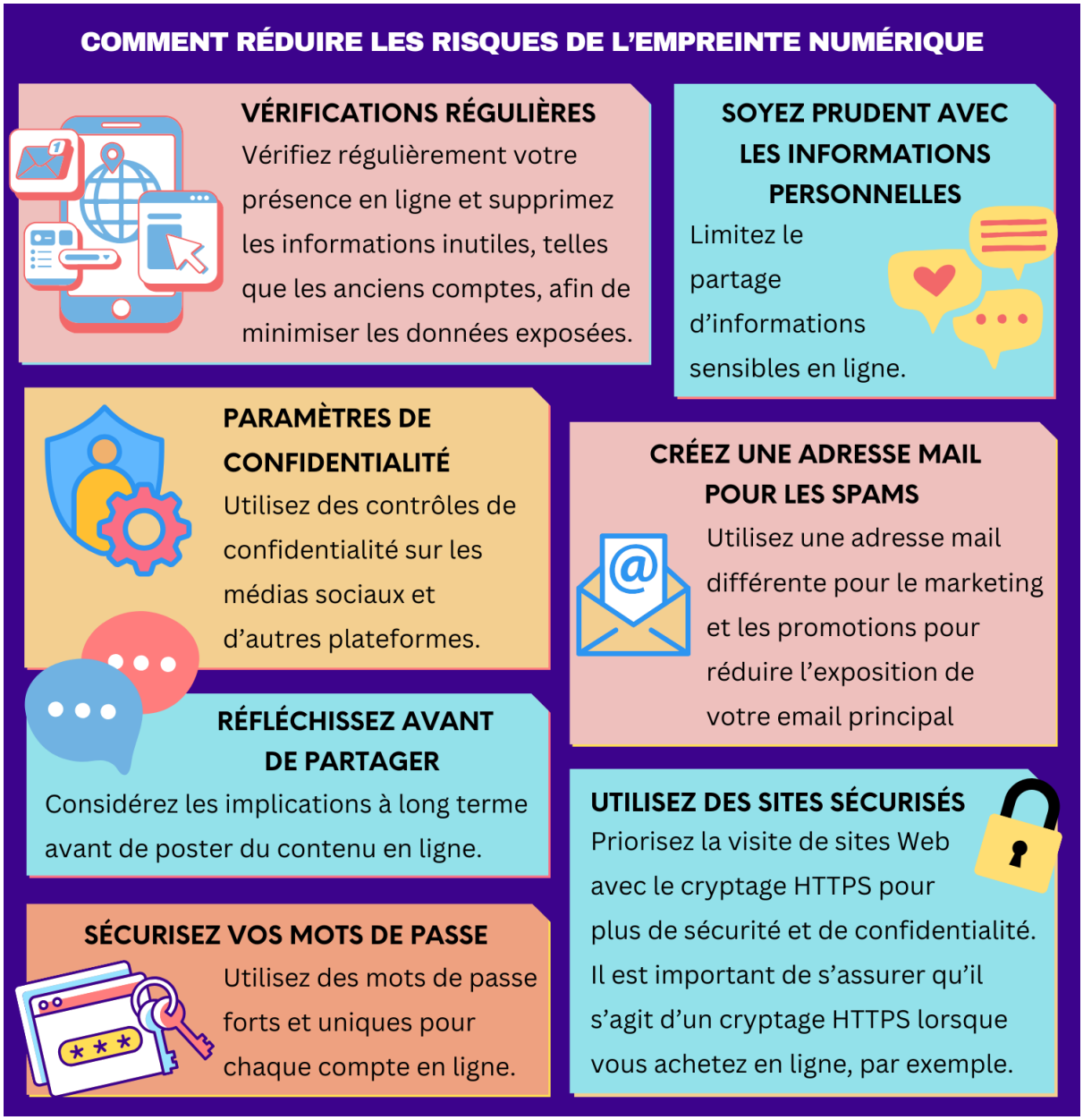
L’aspect environnemental de l’empreinte numérique est une considération de plus en plus importante à mesure que nos activités en ligne continuent de croître. Les activités numériques nécessitent une consommation d’énergie importante, car les centres de données et les réseaux qui alimentent les services en ligne représentent environ 1 % des émissions mondiales de gaz à effet de serre liées à l’énergie.

De plus, l’empreinte carbone de la consommation de contenu numérique est importante. À mesure que les services et technologies numériques tels que le jeu en nuage, la blockchain et la réalité virtuelle se développent, l’impact environnemental des empreintes digitales devrait fortement augmenter. Pour répondre à ces préoccupations environnementales, les experts recommandent de promouvoir des pratiques de sobriété numérique afin de réduire la consommation numérique inutile, entre autres stratégies.

En conclusion, la compréhension et la gestion de l’aspect environnemental des empreintes digitales sont cruciales pour assurer un avenir numérique plus durable.

Comment pouvons-nous réduire les risques de l’empreinte numérique ?

Gérer votre empreinte numérique commence par la gestion de vos données personnelles. Les conseils suivants peuvent vous aider à réduire les risques de partage de vos données personnelles :



Un autre conseil pratique est d'être familier avec les outils suivants et ce que ça peut faire pour vous :

- **Les VPNs (Virtual Private Networks) ou réseaux privés virtuels :** Masquez votre adresse IP et encryptez vos activités en ligne.
- **Les bloqueurs de publicité :** Réduisez la traçabilité en bloquant les publicités et les trackers.
- **Les navigateurs sécurisés :** Utilisez des navigateurs dotés de fonctions de confidentialité intégrées.
- **Les moteurs de recherche axés sur la protection de la vie privée :** Choisissez les moteurs de recherche qui ne tracent pas vos requêtes.

- **Les outils de suppression de données :** Utilisez les services permettant de supprimer vos renseignements personnels des sites de courtier en données.
- **Les réseaux sécurisés :** Assurez-vous que votre réseau Wi-Fi est protégé pour réduire le risque d'exposition.
- **Les mises à jour logicielles :** Mettez régulièrement à jour les logiciels et les programmes antivirus de vos appareils.

En comprenant votre empreinte numérique et en implémentant ces stratégies, vous pouvez améliorer votre présence en ligne et atténuer les potentiels risques associés avec vos activités numériques.

En toute sécurité : Pourquoi la protection des informations personnelles est essentielle

Les renseignements de nature délicate comme les noms, les adresses, les numéros d'identification, les données financières et même les préférences et les habitudes sont devenus un bien précieux, non seulement pour les particuliers, mais aussi pour les sociétés, les entités tierces et inévitablement les criminels. La protection des renseignements personnels est essentielle pour éviter les atteintes à la vie privée, comme le vol d'identité et d'autres activités malveillantes découlant de violations de données. Les violations de données sont devenues plus fréquentes, ce qui signifie que vous devez comprendre comment vos données personnelles sont collectées et stockées, ainsi que les risques liés à une protection inadéquate (Conseil de l'Europe 2019).

Le droit à la vie privée est un droit fondamental de la personne, et son importance s'est accentuée dans l'environnement numérique moderne. En 2018, le règlement général sur la protection des données (RGPD) de l'Union européenne a été introduit pour réglementer la collecte, le stockage et l'utilisation des données personnelles (Sharma 2022). Cette loi donne aux gens plus d'autorité sur leurs renseignements personnels, ce qui leur permet de gérer leur présence numérique plus efficacement.

Les risques d'exposition des données

Dans de nombreux cas, les utilisateurs ne sont pas au courant des risques posés par le partage de données. Des actions en apparence innocente, tel que poster une photo ou partager votre localisation sur les réseaux sociaux, peut inévitablement révéler plus que convenu et vous mettre à risque.

Les conséquences d'une violation de données à caractère personnel peuvent être lourdes et graves. Une menace importante est le vol d'identité, où des personnes malveillantes volent et utilisent des données personnelles sensibles comme des numéros d'identification, des identifiants de connexion ou des informations financières pour des achats non autorisés ou l'ouverture de comptes au nom de la victime. Un risque supplémentaire est que quelqu'un puisse créer un faux profil de médias sociaux en se faisant passer pour vous, ce qui a plusieurs conséquences négatives. L'imposteur peut faire quelque chose d'illégal, nuire à votre réputation en trompant vos amis, votre famille ou vos collègues. De plus, ces comptes peuvent mener à l'invasion de la vie privée, exposant des informations personnelles et des contacts. Cela pourrait également permettre des attaques d'hameçonnage ou de vol d'identité, lorsque l'imposteur utilise le faux profil pour obtenir un accès non autorisé à des données sensibles, des comptes financiers ou d'autres plateformes en ligne, vous causant de graves dommages.

De plus, la fuite de données personnelles peut amener à une atteinte à la réputation, tout particulièrement quand les informations personnelles sont exposées dans des contextes inappropriés ou mal utilisé par des parties tiers. Si les informations personnelles sensibles, telles que les messages privées, photos, vidéos sont exposés en ligne, cela peut être utilisé pour endommager la réputation d'un individu, ce qui met en péril les relations personnels et professionnels, ce qui peut résulter, de ce fait, en harcèlement ou cyber harcèlement. Dans des cas extrêmes, la fuite de données personnelles peut escalader jusqu'à des menaces bien réelles, telles que le stalking ou l'extorsion.

En outre, les atteintes à la vie privée peuvent causer une détresse émotionnelle, laissant les victimes se sentir vulnérables, violées et craignant les répercussions possibles. Ce fardeau psychologique peut gravement affecter le bien-être, la santé mentale et le sentiment de sécurité des personnes. La violation de la vie privée entraîne souvent des sentiments d'impuissance, car les victimes se rendent compte qu'elles n'ont plus le contrôle sur leurs renseignements personnels. Cette perte de contrôle peut entraîner une anxiété accrue, du stress et un état constant de peur quant à ce qui pourrait se passer ensuite. Les victimes peuvent éprouver de l'insomnie, de la paranoïa ou de la dépression, car la violation peut éroder leur confiance dans les systèmes numériques et les autres autour d'eux. Cette détresse s'intensifie lorsque les conséquences de l'atteinte, comme la fraude financière ou le vol d'identité, sont manifestes. Le sentiment de vulnérabilité est exacerbé lorsque des informations sensibles, telles que des photos privées ou de la correspondance, sont exposées en ligne. Cette exposition peut nuire à la réputation, entraîner de la cyberintimidation, du harcèlement et même des menaces à la sécurité physique. Les problèmes de santé mentale, comme le trouble de stress post-traumatique (TSPT), peuvent également se manifester, surtout si des données sensibles telles que des dossiers médicaux ou des photos intimes sont exposées.

L'impact sur le sentiment de sécurité est également critique. Les personnes touchées par des atteintes à la vie privée se sentent souvent en danger dans leurs environnements numériques et physiques, craignant une exploitation ou un préjudice supplémentaire. Ce manque de sécurité peut entraîner un retrait social, car les victimes évitent les espaces numériques et réduisent leurs interactions pour minimiser une exposition supplémentaire. Le fardeau

psychologique ne se limite donc pas au moment de la violation, mais peut s'étendre bien au-delà, affectant divers aspects de la vie quotidienne.

Pour éviter de tels résultats, il est essentiel de reconnaître l'importance de protéger les renseignements personnels et de prendre des mesures appropriées pour atténuer ces risques. Les citoyens numériques doivent prendre des mesures efficaces pour s'assurer que leurs informations personnelles ne seront pas non autorisées, accessibles ou utilisées à mauvais escient.

Restez en sécurité en ligne : Des conseils pratiques pour maintenir votre confidentialité

Avec des données personnelles constamment à risque d'exposition ou d'emploi abusif, il est important de comprendre et d'implémenter des stratégies de protection effectives pour les protéger. Vous pouvez retrouver des pratiques clés pour aider des individus à protéger leur confidentialité dans les espaces numériques :

Limitez le partage d'informations et ajustez les paramètres de sécurité

Partager des informations personnelles en ligne devrait être fait prudemment. Vous pouvez partager plus d'information que nécessaire sans le savoir, tel que la position en temps réel ou des habitudes personnelles. Réduire la quantité de données personnelles partagées, que ce soit sur les réseaux sociaux ou d'autres plateformes, peut aider à vous protéger contre les risques de cyberstalking ou de vol d'identité. Par exemple, éviter de poster les itinéraires de voyage ou des mises à jour de routine qui pourraient vous rendre vulnérable au harcèlement ou à d'autres activités malveillantes.

Ajuster les paramètres de confidentialité permet de contrôler qui a accès aux données personnelles, atténuer le risque d'exposition non désirée. Il peut être recommandé de mettre le profil en privé, et ne pas laisser des inconnus vous suivre. De plus, créer une liste « d'amis proches » sur des plateformes comme Instagram ou d'utiliser les paramètres de confidentialité Facebook pour limiter la visibilité des posts peut aider à prévenir d'une exposition non désirée.

Mettez à jour les paramètres de confidentialité régulièrement

À mesure que la technologie et les pratiques de confidentialité évoluent, il est important d'examiner et de mettre à jour régulièrement les paramètres de confidentialité de vos applications et comptes en ligne. Cela garantit que les données personnelles sont partagées en fonction de vos préférences. Vous devez également désactiver les fonctionnalités de partage de localisation ou révoquer les autorisations inutiles des applications et services qui n'ont plus besoin d'accéder à vos données.

Restez informé des lois sur la confidentialité des données

Le RGPD a été mis en place pour protéger la confidentialité des données des individus en veillant à ce que les sites web obtiennent un consentement explicite avant de collecter des informations personnelles. Rester informé de ces lois vous permet de mieux comprendre vos droits et de prendre le contrôle de votre empreinte numérique. Par exemple, le RGPD donne aux utilisateurs le droit de demander que leurs données soient supprimées ou ne soient pas partagées avec des tiers.

Gérez les cookies et les paramètres du navigateur

Les cookies, de petites données stockées sur les appareils des utilisateurs, sont utilisés par la plupart des sites Web et sont généralement activés par défaut dans les navigateurs Web. Vous pouvez modifier leurs paramètres pour accepter ou refuser les cookies.

Alors que certains cookies sont essentiels pour la fonctionnalité du site, d'autres peuvent suivre votre activité sur différents sites. La gestion des préférences en matière de cookies dans les paramètres de votre navigateur

peut vous aider à contrôler quels types de cookies sont autorisés, limitant ainsi le suivi inutile. En outre, l'effacement périodique des cookies et des données de navigation peut contribuer à améliorer la confidentialité.

Développez des connaissances technologiques de base

Avoir une compréhension de base des concepts technologiques tels que le cryptage, les cookies et les adresses IP peut grandement contribuer à la protection de votre vie privée en ligne. Par exemple, le fait de savoir comment fonctionne le chiffrement peut vous aider à choisir des méthodes de communication sécurisées et la compréhension des adresses IP peut vous aider à mieux comprendre comment votre emplacement pourrait être suivi en ligne. Les technologies qui améliorent la confidentialité, comme les VPN et les navigateurs sécurisés, peuvent également vous permettre de protéger vos données plus efficacement et d'accroître votre anonymat en ligne.

Soyez prudent avec le Wi-Fi public et les appareils partagés

Le Wi-Fi public, bien que pratique, pose un risque de sécurité important en raison de son manque de cryptage. Il est ainsi plus facile pour les cybercriminels d'intercepter des données personnelles. Pour rester en sécurité lorsque vous utilisez le Wi-Fi public, évitez d'effectuer des transactions sensibles telles que les services bancaires en ligne ou les achats. Une alternative plus sûre consiste à utiliser un VPN, qui crypte votre connexion Internet et protège vos données contre les interceptions par d'autres personnes. De même, l'utilisation d'appareils publics ou partagés, comme les ordinateurs dans la bibliothèque universitaire, présente des risques pour la sécurité. Les données personnelles, telles que les identifiants de connexion ou l'historique de navigation, peuvent être stockées par inadvertance et consultées par des utilisateurs subséquents.

Utilisez des mots de passe forts et une authentification à deux facteurs (2FA)

L'un des moyens les plus simples de protéger les comptes en ligne est d'utiliser des mots de passe forts et uniques. Un mot de passe fort combine généralement des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Il est également essentiel d'éviter de réutiliser les mots de passe sur différentes plateformes. L'authentification à deux facteurs (2FA) ajoute une couche de sécurité supplémentaire, nécessitant une deuxième forme d'identification, telle qu'un code de message texte ou une application d'authentification, ce qui réduit considérablement les risques d'accès non autorisé.

Utilisez des sites sécurisés (HTTPS)

Lorsque vous partagez des renseignements personnels ou faites des achats en ligne, assurez-vous toujours que le site Web est sécurisé en vérifiant le préfixe HTTPS dans l'URL. Le S en HTTPS signifie « sécurisé », ce qui indique que le site web utilise un chiffrement pour protéger les données interceptées par des tiers. Recherchez l'icône de verrouillage ou de bascule à côté de l'URL pour vérifier que la connexion est sécurisée.

En mettant en œuvre ces conseils pratiques, vous pouvez améliorer considérablement votre vie privée et votre sécurité en ligne, ce qui n'est pas seulement une nécessité mais une responsabilité. Grâce à une gestion proactive de la protection des renseignements personnels et à la sensibilisation technologique, vous pouvez minimiser les risques associés au partage de données personnelles en ligne.

VII. CONCLUSION

Alors que le monde numérique devient de plus en plus central à notre vie quotidienne, il n'a jamais été aussi essentiel d'équiper les jeunes des compétences et des valeurs de la citoyenneté numérique. Selon Eurostat (2023), 97 % des personnes âgées de 16 à 29 ans dans l'UE utilisent Internet quotidiennement et 83 % sont actifs sur les réseaux sociaux. Ces statistiques mettent en évidence le rôle omniprésent des technologies numériques dans la façon dont les jeunes apprennent, se connectent et s'engagent avec le monde.

L'espace numérique sert comme une « fenêtre sur le monde » offrant des opportunités pour acquérir de nouvelles connaissances et compétences. Cependant, afin de tirer pleinement parti de ces opportunités tout en parcourant les risques, les jeunes ont besoin d'une base solide dans la citoyenneté numérique. Ce guide, aligné sur le cadre des compétences numériques pour les citoyens de la Commission européenne, fournit cette base en mettant l'accent sur la pensée critique, le comportement éthique et les compétences essentielles pour l'avenir.

La citoyenneté numérique ne se limite pas au savoir-faire technique, elle consiste à favoriser une participation informée, respectueuse et responsable dans les environnements numériques. En intégrant les principes de la protection des renseignements personnels en ligne, de la littératie médiatique, de l'utilisation responsable des médias sociaux et de la gestion des empreintes digitales, ce guide permet aux apprenants de prendre des décisions réfléchies et de contribuer positivement à la communauté numérique.

Les compétences décrites dans ce guide sont non seulement essentielles pour naviguer dans le paysage numérique d'aujourd'hui, mais elles sont également essentielles pour réussir à l'avenir dans un monde de plus en plus numérisé. En tant qu'éducateurs, formateurs et organisations qui mettent en œuvre ces pratiques, ils aideront à façonner une génération capable de relever les défis et d'optimiser les opportunités de l'ère numérique.

Ensemble, continuons de promouvoir la citoyenneté numérique comme pierre angulaire de l'éducation, en veillant à ce que les jeunes puissent explorer en toute sécurité, de manière éthique et efficace les possibilités illimitées du monde numérique.

GLOSSAIRE

Activisme en ligne	L'utilisation d'outils et de plateformes numériques pour défendre des causes sociales, politiques, environnementales ou économiques.
Addiction numérique	L'utilisation excessive et compulsive des technologies numériques, comme les téléphones intelligents, les ordinateurs, les médias sociaux, les jeux vidéo ou Internet, au point où elle a une incidence négative sur divers aspects de la vie d'une personne, tels que les relations, le travail, la santé ou le bien-être général.
Biais	Une tendance ou préférence qui affecte le jugement d'un individu, sa perception ou son comportement d'une manière injuste, faussé ou inégal.
Capital social	La valeur dérivée des interactions sociales et les liens que les gens ont au sein de leurs communautés, organisations ou sociétés.
Chambres d'écho	Des environnements, dans les médias ou les réseaux sociaux, où les individus sont exposés principalement à des informations, opinions ou idées qui renforcent leurs croyances ou points de vue existants plutôt que de les remettre en question avec diverses perspectives.
Citoyen numérique	Une personne qui utilise les technologies numériques et Internet de façon responsable, éthique et efficace pour s'engager dans la société, la politique, l'éducation et la culture.

Citoyenneté numérique	L'utilisation responsable, éthique et éclairée de la technologie, en particulier d'Internet, pour participer efficacement à la société.
Commerce numérique / e-commerce	L'achat et la vente de biens et services sur Internet.
Communauté numérique / en ligne	Un groupe de personnes qui interagissent, partagent et collaborent au moyen de plateformes numériques et d'espaces en ligne.
Compétence numérique	L'ensemble des compétences, connaissances et attitudes requises pour utiliser efficacement et de façon responsable les technologies numériques dans divers aspects de la vie, y compris le contexte personnel, éducatif et professionnel.
Compétences numériques	Les capacités à utiliser efficacement les outils et les plateformes technologiques.
Contenu numérique	Désigne toute information ou tout matériel créé, stocké, distribué ou consommé sous forme numérique.
Cyberharcèlement	L'utilisation de la technologie pour harceler, menacer, humilier ou blesser quelqu'un.
Cyberstalking	L'utilisation d'Internet, des médias sociaux ou d'autres plateformes en ligne pour traquer ou harceler une personne ou un groupe.
Désinformation	Les informations délibérément fausses ou trompeuses diffusées dans l'intention de tromper ou de manipuler autrui.

Droits d'auteurs	Un cadre juridique qui donne aux créateurs de contenu originaux des droits exclusifs à leur utilisation, reproduction, distribution et adaptation de leur création.
Droits de propriété intellectuelle (DPI)	Les protections juridiques accordées aux créateurs et aux propriétaires de la propriété intellectuelle (PI), qui comprend les créations immatérielles de l'esprit.
Droits numériques	Les droits et libertés dont jouissent les individus dans le monde numérique, y compris leur capacité à accéder, utiliser, créer et partager du contenu et de l'information numériques tout en protégeant leurs données personnelles et leur vie privée.
Éducation au numérique	La capacité d'utiliser efficacement, en toute sécurité et de manière responsable les technologies, outils et plateformes numériques pour accéder à l'information, l'évaluer, la créer et la communiquer.
Éducation aux médias	L'habilité d'accéder, analyser, évaluer et créer des médias dans diverses formes.
Email / courier électronique	Une méthode d'échange de messages numériques entre les personnes utilisant des appareils électroniques, essentiellement sur Internet.
Empathie	La capacité à comprendre, partager et s'identifier aux sentiments, pensées ou expériences d'autres personnes.
Empreinte numérique	La traînée de données ou d'informations qu'une personne laisse derrière elle lorsqu'elle utilise des appareils numériques, interagit en ligne ou s'engage avec la technologie.

Environnement numérique	Tout espace virtuel ou écosystème où se produisent des interactions, activités ou processus numériques.
Équité	Les principes de justesse et de justice dans la distribution des ressources, des opportunités et de traitement, en s'assurant que les individus ou des groupes reçoivent ce dont ils ont besoin pour atteindre l'égalité des résultats.
Espace numérique	Tout environnement ou toute plateforme existant en ligne ou alimenté par des technologies numériques, ou les utilisateurs interagissent, communiquent et s'engagent dans le contenu, les services ou les uns avec les autres.
Esprit critique	Le processus consistant à analyser, évaluer et synthétiser activement et objectivement de l'information pour prendre des décisions ou des jugements raisonnés et bien éclairés.
Évaluation critique	Le procédé d'évaluer attentivement et d'analyser quelque chose, que ce soit une idée, un argument, du travail, une théorie, ou une source d'information – en examinant leurs forces, faiblesses, pertinence, exactitude, et validité en général.
Exploitation en ligne	Le fait d'utiliser Internet ou les plateformes numériques pour profiter injustement de personnes, souvent par la manipulation, la coercition ou la tromperie, à des fins personnelles, financières ou sexuelles.
Fact-checking / verification des faits	Le procédé de vérifier l'exactitude et la véracité de l'information, revendications ou déclarations en général en les comparant à des sources fiables et crédibles.

Grooming / Pédopiégage	Le procédé par lequel un individu construit une relation avec un enfant ou une personne vulnérable pour manipuler, exploiter ou les abuser.
Hameçonnage / Phishing	Un type de cyberattaque dans lequel les attaquants se font passer pour des institutions ou des individus légitimes afin d'inciter les gens à révéler des informations sensibles, telles que des mots de passe, des numéros de carte de crédit, des numéros de Sécurité sociale ou d'autres données personnelles.
Harcèlement en ligne	L'utilisation de plateformes et de technologies numériques pour nuire, intimider, menacer ou dénigrer intentionnellement un individu ou un groupe.
Incendier / Flaming	L'acte de poster ou d'envoyer des commentaires incendiaires, offensifs ou insultant en ligne avec l'intention de provoquer les autres, en incitant à la colère et commençant des conflits.
Inclusion	La pratique consistant à créer des environnements, des systèmes et des communautés qui embrassent la diversité et garantissent que tous les individus, indépendamment de leurs antécédents, identités ou capacités, ont un accès égal aux possibilités, à la participation et au respect.
Intelligence Artificielle (IA)	La simulation de l'intelligence humaine dans les machines qui sont programmées pour penser, apprendre et réaliser des tâches qui nécessitent généralement une cognition humaine, telles que la compréhension du langage, la reconnaissance des modèles.

Maîtrise de l'information	La capacité de localiser, d'évaluer et d'utiliser l'information de façon efficace, efficiente et éthique.
Mésinformation	Les renseignements faux ou inexacts qui sont diffusés, peu importe l'intention de tromper.
Monde numérique	L'écosystème mondial crée par les technologies numériques, ou l'information, la communication et les activités ont lieu par des moyens électroniques en ligne.
Narration numérique	La pratique consistant à utiliser des outils et des plateformes numériques pour créer et partager des histoires.
Numérique / Digital	Tout ce qui concerne la représentation, le stockage ou le traitement de l'information dans des formats binaires discrets (par exemple, 0 et 1) par opposition aux signaux analogiques continus. La technologie numérique est fondamentale pour l'informatique et les télécommunications modernes.
Outils numériques	Les logiciels, plateformes, applications ou appareils qui utilisent la technologie numérique pour effectuer des tâches, résoudre des problèmes, communiquer ou faciliter des activités.
Participation	La participation active ou à l'engagement de personnes dans des activités, des processus décisionnels ou des événements.
Podcast	Un programme audio ou vidéo numérique qui peut être diffusé en continu ou téléchargé à partir d'Internet, généralement dans une série d'épisodes.

Réalité Augmentée (RA / AR)	Une technologie qui recouvre l'information numérique, tel que les images, les sons ou autres données, dans l'environnement en temps réel.
Réalité Virtuelle (RV / VR)	Une simulation générée par ordinateur d'un environnement qui plonge les utilisateurs dans un monde complètement virtuel, généralement grâce à l'utilisation d'un casque, de capteurs et parfois d'équipements supplémentaires comme des gants ou des manettes.
Références de l'Auteur	Font référence aux qualifications, à l'expérience, à la formation et à l'expertise qu'une personne possède relativement au sujet sur lequel elle écrit.
Règlement général sur la protection des données (RGPD)	Une loi complète sur la protection des données édictée par l'Union européenne (UE). Il est entré en vigueur le 25 mai 2018 et vise à réglementer le traitement des données personnelles des personnes au sein de l'UE et de l'Espace économique européen (EEE).
Renseignements personnels ou renseignements personnels identifiables (PII)	Toute donnée ou information pouvant servir à identifier, contacter ou localiser une personne, directement ou indirectement.
Réseaux sociaux	Les plateformes et applications numériques qui permettent aux utilisateurs de créer, partager et échanger du contenu, des idées et de l'information avec d'autres personnes au moyen de communautés virtuelles et de réseaux.

Résolution de problèmes numérique	La capacité d'utiliser des outils, des technologies et des ressources numériques pour identifier, analyser et trouver des solutions aux problèmes ou aux défis dans divers contextes, comme le travail, la vie personnelle ou l'éducation.
Services de streaming	Les plateformes ou des technologies qui permettent aux utilisateurs d'accéder et de consommer du contenu multimédia (comme de la musique, des vidéos, des émissions de télévision, des films et des émissions en direct) sur Internet en temps réel, sans avoir à télécharger le contenu au préalable.
Usurpation de compte	L'acte de se faire passer pour un compte ou une identité légitime afin de tromper les autres.
Vol ou usurpation d'identité	L'acquisition non autorisée et l'utilisation des informations personnelles de quelqu'un d'autre, à des fins typiquement frauduleuses.

BIBLIOGRAPHIE

Toutes les images sont extraites de **Canva**.

Aboujaoude, E. (2022). "Protecting Privacy to Protect Mental Health: The New Ethical Imperative". *Journal of Medical Ethics*. **https://doi.org/10.1136/medethics-2018-105313**

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild". *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674-689. **https://dl.acm.org/doi/10.1145/2660267.2660347**

Baltacı, Ö., Bektas, M., & Kutlu, F. (2021). "Internet addiction, social anxiety, and coping strategies among university students: A cross-sectional study". *Journal of Research in Adolescence*, 31(3), 565-575.

Better Internet for Kids. (2020). *Insafe insights on...online reputation*. **https://www.betterinternetforkids.eu/practice/awareness/article?id=6668871**

Bucher, T. (2018). "If...Then: Algorithmic Power and Politics". *Oxford Studies in Digital Politics, New York, 2018; online edn, Oxford Academic*. **https://doi.org/10.1093/oso/9780190493028.001.0001**

Carrascal, J.P., et al. (2013). "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." *Computers in Human Behavior*, vol. 29, no. 2, 2013, pp. 340–349. **https://arxiv.org/abs/1112.6098**

Cataldo, I., Lepri, B., Neoh, M. J.-Y., & Esposito, G. (2021). "Social media usage and development of psychiatric disorders in childhood and adolescence: A review". *Frontiers in Psychiatry, 11*. **https://doi.org/10.3389/fpsyt.2020.508595**

Cyber Citizenship. (2023). *Digital Citizenship 101: Responsible Online Behavior*. **https://www.cybercitizenship.org/digital-citizenship-guide/**

ENISA. (2017). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. **https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines**

eSafety Commissioner. (2024). *Digital reputation*. **https://www.esafety.gov.au/key-topics/staying-safe/digital-reputation**

European Data Protection Supervisor. (2020). Guidelines on the Protection of Personal Data. **https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en**

Eurostat. (2024). *Young people - digital world.* **https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/39761.pdf**

Fardouly, J., Magson, N. R., Rapee, R. M., Johnco, C. J., & Oar, E. L. (2020). "The use of social media by Australian preadolescents and its links with mental health". *Journal of Clinical Psychology*, *76*(7), 1304–1326. **https://doi.org/10.1002/jclp.22936**

Gillespie, T. (2018). "Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media". *Yale University Press*. **http://dx.doi.org/10.12987/9780300235029**

Helberger, N. (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism*, *8*(6), 842–854. **https://doi.org/10.1080/21670811.2020.1773888**

Isin, E., & Ruppert, E. (2015). *Being Digital Citizens.* Rowman & Littlefield International, Ltd. ISBN/9781786614490. **https://rowman.com/WebDocs/Being_Digital_Citizens_Second_Ed_Open_Access.pdf**

Kaspersky. (2024). *What is a Digital Footprint?*. **https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint**

Kotobee Blog. (2024). *Game-Based Learning: What It Is and How to Apply It*. **https://blog.kotobee.com/game-based-learning/**

Kozyreva, A., Wineburg, S., Lewandowsky, S., Hertwig, R. (2022). "Critical Ignoring as a Core Competence for Digital Citizens." *Current Directions in Psychological Science* 32 (1): 81–88. Crossref. **https://journals.sagepub.com/doi/full/10.1177/09637214221121570**

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report 2009.* EU Kids Online Network. **http://eprints.lse.ac.uk/24372/**

McCrae, N., Gettings, S., & Purssell, E. (2017). "Social media and depressive symptoms in childhood and adolescence: A systematic review". *Adolescent Research Review*, 2, 315–330. **https://doi.org/10.1007/s40894-017-0053-4**

Netsafe. (2018). *From literacy to fluency to citizenship: Digital citizenship in education (2nd ed.)*. Wellington, NZ. **https://www.researchgate.net/publication/332886585**

Nolan, S., Hendricks, J., Ferguson, S., & Towell, A. (2017). "Social networking site (SNS) use by adolescent mothers: Can social support and social capital be enhanced by online social networks? – A structured review of the literature". *Midwifery*, 48, 24–31. **https://doi.org/10.1016/j.midw.2017.03.002**

OECD. (2022). *Is digital media literacy the answer to our disinformation woes?* The OECD Education Podcast. **https://www.oecd-ilibrary.org/education/is-digital-media-literacy-the-answer-to-our-disinformation-woes_326b63bf-en**

Oxford Dictionary. (n.d.). *Definition of 'digital citizenship.* **https://dictionary.cambridge.org/dictionary/english/digital-citizenship**

Popat, A., & Tarrant, C. (2023). "Exploring adolescents' perspectives on social media and mental health and well-being – a qualitative literature review". *Clinical Child Psychology and Psychiatry*, 28, 323–337. **https://doi.org/10.1177/13591045221092884**

Pretorius, C., Chambers, D., & Coyle, D. (2019). "Young People's Online Help-Seeking and Mental Health Difficulties: Systematic Narrative Review". *Journal of medical Internet research*, *21*(11), e13873, **https://doi.org/10.2196/13873**

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook*. Council of Europe. **https://rm.coe.int/16809382f9**

Ringrose, J., Gill, R., Livingstone, S. & Harvey, L. (2012). "A qualitative study of children, young people and 'sexting': A report prepared for the NSPCC". London: NSPCC. **https://www.researchgate.net/publication/265741962**

Sala, A., Porcaro, L., & Gómez, E. (2024). "Social Media Use and adolescents' mental health and well-being: An umbrella review". *Computers in Human Behavior Reports*, *14*, 100404. **https://doi.org/10.1016/j.chbr.2024.100404**

Scheinin, M. (2009). "Law and Security: Facing the Dilemmas". *SSRN Electronic Journal*. **http://dx.doi.org/10.2139/ssrn.1555686**

Secure Privacy. (2022). *The Ultimate Guide to Cookie Consent*. **https://secureprivacy.ai/blog/the-ultimate-guide-to-cookie-consent**

Senekal, J. S., Groenewald, G. R., Wolfaardt, L., Jansen, C., & Williams, K. (2023). "Social media and adolescent psychosocial development: A systematic review". *South African Journal of Psychology*, 53, 157–171. **https://doi.org/10.1177/00812463221119302**

Sharma, A. (2022). "Teaching Digital Privacy: Navigating the Intersection of Technology, Education, and Privacy." *Kanpur Historians*. Vol. IX, Issue II. **https://www.researchgate.net/publication/381952547_Teaching_Digital_Privacy_Navigating_the_Intersection_of_Technology_Education_and_Privacy**

Sheldon, R. (2023). *Navigating the Digital World: Online Reputation and Online Etiquette*. Igniyte. **https://www.igniyte.com/blog/navigating-the-digital-world-online-reputation-and-online-etiquette/**

Techopedia. (2023). *How to Protect Your Privacy Online*. **https://www.techopedia.com/how-to/how-to-protect-your-privacy-online**

Twenge, J. M., Haidt, J., Lozano, J., & Cummins, K. M. (2022). "Specification curve analysis shows that social media use is linked to poor mental health, especially among girls". *Acta Psychologica*, *224*, 103512. **https://doi.org/10.1016/j.actpsy.2022.103512**

UNICEF. (2023). *Digital civic engagement by young people*. **https://www.unicef.org/innocenti/reports/digital-civic-engagement-young-people**

G, V. (2024, July 31). *How can your digital footprint affect you in business opportunities?* Reputation Sciences. **https://www.reputationsciences.com/how-can-your-digital-footprint-affect-you/**

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills, and attitudes*. Publications Office of the European Union. **https://data.europa.eu/doi/10.2760/115376**

Webster, D., Dunne, L., & Hunter, R. (2021). „Association between social networks and subjective well-being in adolescents: A systematic review". *Youth & Society*, 53, 175–210. **https://doi.org/10.1177/0044118X20919589**

Wolford B, (n.d.), *What is GDPR, the EU's new data protection law?*, GDPR.eu, **https://gdpr.eu/what-is-gdpr/**

DIGICITY

GAME-BASED
DIGITAL CITIZENSHIP

www.projectdigicity.eu

Cofinancé par
l'Union européenne

Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence Nationale Fondation Tempus. Ni l'Union européenne ni l'Agence Nationale Fondation Tempus ne sauraient en être tenues pour responsables.

Code du projet: 2023-2-RS01-KA220-YOU-000170562

LogoPsyCom PENS digiQ YuzuPulse