

Nom :	Prénom :	Classe :
-------	----------	----------

SNT — Réseaux sociaux - chapitre 2

Objectifs :

- Savoir définir les termes d'identité numérique et e-réputation.
- Comprendre à partir de quand avoir une fausse identité devient illégal.
- Découvrir l'aspect quasi ineffaçable d'une trace numérique.
- Découvrir comment l'UE protège nos données personnelles.

Identité numérique et réputation en ligne

L'**identité numérique** et la **réputation en ligne** (e-reputation) forment une sorte de **carte de visite virtuelle** qui influence directement la confiance, les relations sociales et professionnelles, et les opportunités de carrière.

Doit-on faire preuve de prudence lorsqu'on publie des messages sur un réseau social ?

Identité numérique

L'**identité numérique** correspond aux informations et aux **traces** laissées **en ligne**, telles que les profils sur les réseaux sociaux, les publications, et les données personnelles partagées sur différents sites.

Information	Description
Réputation	Ce que l'on dit sur moi
Expression	Ce que je dis
Réseau	Qui je connais
Certification	Qui peut certifier de mon identité
Achat	Ce que j'achète
Opinion	Ce que je pense
Savoir	Ce que je sais
Hobbies	Ce que j'aime
Avatar	Comment je me montre
Profession	Quel est mon métier et où je travaille

► Exercice 1 — À vous de jouer !

a) À votre avis, quelles informations vous concernant sont accessibles par le biais des réseaux sociaux que vous utilisez ?

Les réseaux sociaux peuvent révéler bien plus que ce qu'on pense : son **identité**, ses **coordonnées**, ses **centres d'intérêt**, ses **habitudes de vie** et parfois même sa **localisation** ou ses **relations**. Même sous pseudonyme, des contenus publiés sur plusieurs plateformes peuvent être recoupés pour reconstituer une partie de sa vie privée.

b) Est-il possible de disposer d'une fausse identité numérique ? Si oui, comment ?

Oui, il est techniquement possible de disposer d'une fausse identité numérique.

Exemple : faux profil sur un réseau social avec nom, photo et informations inventées...

c) À partir de quand avoir une fausse identité devient illégal ?

Dans la plupart des pays, ce n'est pas le fait d'avoir un pseudonyme qui pose problème, mais les faits **d'usurper une identité** réelle, et **d'utiliser** cette fausse identité pour commettre une infraction (escroquerie, fraude, achat à crédit, etc).

d) Pourquoi rester vigilant lorsqu'on entre en contact avec une personne inconnue sur Internet ?

Les discussions avec des inconnus sur Internet exposent à des dangers liés aux **violences numériques**, telles que :

- Cyberharcèlement.
- Cyberhumiliation.
- "Revenge porn" diffusé sur des "comptes fisha" (« affiche » en verlan).
- Diffusion d'images violentes, sexuelles ou haineuses (pour traumatiser).
- Dénigrement (ou "trollage").

→ Pour en savoir plus, voir l'article "[violence numérique](#)" sur Wikipédia.

E-réputation

L'**e-réputation**, parfois appelée *web-réputation*, *réputation numérique* ou *réputation en ligne*, est l'**image perçue** d'une personne, d'une entreprise ou d'une marque sur Internet, façonnée par les avis, les commentaires et les informations accessibles publiquement. L'e-réputation peut être influencée par les actions directes de l'individu ou de l'entité concernée, mais aussi par les contributions d'autres internautes.

► Exercice 2

a) Comment les commentaires laissés sur le Web peuvent-ils nuire à l'e-réputation d'une personne ou d'une entreprise ? Donner un exemple.

Les **commentaires négatifs** sur le Web peuvent gravement **endommager l'e-réputation** d'une personne ou d'une entreprise en **influençant la perception publique** et les décisions des consommateurs.

Exemple : « *cet artisan est incompetent et mal élevé, fuyez ce professionnel !* ».

Ce type de critique cible l'individu plutôt que le service, démoralise et repousse les clients potentiels sans offrir de retour constructif. Elle se propage vite, ternissant l'image professionnelle durablement.

b) Quelles types de réactions (positives ou négatives) pourrait engendrer la publication d'une photo de vacances sur un réseau social accessible à tous ?

Les réactions peuvent être variées, allant de l'**admiration** à la **jalousie** ou aux **risques sécuritaires** : une habitation vide peut attirer des cambrioleurs.

c) Que deviennent dans la durée nos traces numériques laissées sur Internet (Web, emails, messageries instantanées, etc.) ?

Les **traces numériques** persistent souvent **indéfiniment** ou sur de **très longues périodes**, selon les plateformes et les régulations. **Elles ne disparaissent pas** "naturellement" et **peuvent resurgir** des années plus tard, impactant la **vie privée** ou **professionnelle**.

Exemple : un message Gmail ou WhatsApp peut être archivé éternellement, s'il n'a pas été supprimé manuellement...

d) Pourquoi il apparaît essentiel de maîtriser et de surveiller son identité numérique et sa e-réputation ?

Maîtriser et **surveiller** son **identité numérique** et sa **e-réputation** est essentiel pour se protéger des **cybermenaces** comme le **vol d'identité** ou les **attaques à la réputation**, qui persistent durablement en ligne.

Comment l'UE protège-t-elle nos données personnelles ?

L'Union européenne protège les données personnelles principalement via le **Règlement Général sur la Protection des Données (RGPD)**, entré en vigueur en 2018, qui impose des **règles strictes** aux entreprises et administrations traitant ces données, notamment :

- **Principe de limitation des finalités** : les données sont seulement utilisées pour un but précis. Exemple : lorsqu'on s'inscrit à un club, on ne s'inscrit pas pour autre chose, après.
- **Principe de minimisation** : seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement sont collectées.
- **Principe d'intégrité et de confidentialité** : les données doivent être protégées contre l'accès non autorisé, la perte ou la divulgation.
- **Principe de limitation de la conservation** : les données ne sont conservées que pendant la durée nécessaire à la finalité prévue.

TikTok condamné en 2023

Le 15 septembre 2023, TikTok a reçu une amende de 345 millions d'euros pour violation du RGPD :

1. Les paramètres de profil des comptes d'utilisateurs mineurs étaient définis par défaut sur « public », ce qui signifie que n'importe qui (sur TikTok ou en dehors) pouvait consulter le contenu publié par l'utilisateur mineur. Articles RGPD enfreints : 25(1), 25(2), 5(1)(c), et 24(1).
2. Le paramètre « Association familiale » permettait à un utilisateur non mineur (dont le statut de parent ou de tuteur ne pouvait être vérifié) d'associer son compte à celui d'un utilisateur mineur. Cela permettait à cet utilisateur non mineur d'activer les messages privés pour les utilisateurs mineurs âgés de plus de 16 ans, ce qui présentait des risques potentiels graves pour ces derniers. Articles RGPD enfreints : 5(1)(f) et 25(1).
3. Le fait que les paramètres de profil des utilisateurs mineurs aient été définis par défaut sur « public » présentait également plusieurs risques pour les enfants de moins de 13 ans qui avaient accès à la plateforme. Article RGPD enfreint : 24(1).
4. TikTok n'a pas fourni suffisamment d'informations transparentes aux utilisateurs mineurs. Articles RGPD enfreints : 12(1) et 13(1)(e).
5. TikTok a mis en place des « dark patterns¹ » en incitant les utilisateurs à choisir des options plus intrusives en matière de confidentialité lors de leur inscription et lorsqu'ils publient des vidéos. Article RGPD enfreint : 5(1)(a).

► Exercice 3

Donner un autre exemple de dark pattern :

L'option pour se désabonner d'un service est cachée derrière plusieurs sous-menus ou libellés ambigus, rendant la démarche fastidieuse.

1 Un **dark pattern** (ou "interface trompeuse") est une interface utilisateur délibérément conçue pour tromper ou manipuler l'utilisateur, le poussant à prendre des décisions potentiellement préjudiciables et contraires à ses intérêts. Par exemple, pour obtenir le consentement à la collecte de données personnelles, l'utilisateur peut être interrompu par un menu surgissant subitement (pop-up) qui l'empêche de poursuivre l'utilisation du service. Ce menu propose un bouton de refus peu visible et un bouton d'acceptation aux couleurs vives et attractives.