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 ?

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

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

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

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.

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

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

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

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 conservés que pendant la durée nécessaire à la finalité prévue.

TikTok condamé 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 patterns[1] » 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 :

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.