Nom :	Prénom :	Classe :

SNT — Réseaux sociaux & accès aux données personnelles (TP)

Éléments du programme : Les réseaux sociaux → Distinguer plusieurs réseaux sociaux selon leurs caractéristiques. Les données structurées et leur traitement → Données, définir une donnée personnelle, identifier les différents descripteurs d'un objet, distinguer la valeur d'une donnée de son descripteur, traitement de données structurées.

Introduction

L'accès aux **données personnelles**[1] par les réseaux sociaux est un phénomène contemporain qui a bouleversé la gestion et la protection de la vie privée à l'ère numérique. Les plateformes demandent aux utilisateurs de fournir leurs informations personnelles dès la création du compte et lors de l'utilisation quotidienne, parfois *explicitement*, parfois à travers le *suivi invisible* des comportements et préférences.

➤ Exercice 1 (à vous de jouer)

Donnez au moins 4 noms de réseaux sociaux :

Qu'est-ce que ça va changer ?

L'accès généralisé des réseaux sociaux aux données personnelles a transformé plusieurs aspects de la vie privée. Les plateformes exploitent ces données pour *personnaliser les expériences*, *cibler la publicité*, *influencer les comportements d'achat*, mais aussi pour créer de vastes bases de profils numériques qu'elles pourront revendre à d'autres plateformes. Les modifications des *conditions d'utilisation* entraînent parfois le partage des données entre différentes applications du même groupe.

➤ Exercice 2

Donnez le nom de **deux applications** d'un même groupe susceptible de partager vos données personnelles d'une application à l'autre, et vice versa.

1 Voir, à ce propos, le cours « Métadonnée, données personnelles ».

Y-a-t-il des risques, et pour qui ?

L'accès aux données personnelles par les réseaux sociaux présente de nombreux risques :

- Pour **l'utilisatrice / utilisateur** : piratage, usurpation d'identité, phishing[2], cyberharcèlement, doxing[3], fuite ou vente de données sensibles.
- Pour les **entreprises** : vol ou fuite de données confidentielles.
- Pour un **pays** : propagation de fausses informations (infox), manipulations politiques, atteinte à la vie privée collective[4].

➤ Exercice 3

À partir des exemples fictifs suivants, identifiez la **cible** (utilisatrice/utilisateur, entreprise ou pays) ainsi que le **type de risque** (piratage, doxing, vol de données, etc.).

Exemple	Cible (à compléter)	Type de risque (à compléter)
Un groupe WhatsApp créé par des élèves diffuse des données confidentielles concernant une autre élève. Certains messages appellent à lui « mettre la pression, devant chez elle ».		
Plusieurs actions coordonnées visant à créer un climat de haine envers une communauté religieuse ont été relevées dans toute la société.		
Un élève qui n'a rien commandé en ligne a reçu un SMS avec un lien, lui indiquant que son colis était bloqué par la douane. Le lien ouvre un formulaire qui lui demande son nom, son prénom, son adresse, ainsi que le règlement des frais de douane.		
Une grande entreprise de téléphonie mobile a envoyé une alerte à ses 3 millions de clients, pour leur demander de se connecter à leur compte, et de changer rapidement leur mot de passe. Aucun lien n'était présent dans l'alerte.		

2 L'hameçonnage (phishing, en anglais) est une activité cybercriminelle très répandue. C'est une forme « d'ingénierie sociale », c'est à dire une pratique de manipulation psychologique à des fins d'escroquerie, où l'attaquant incite les utilisateurs à divulguer des données personnelles sensibles ou à installer des logiciels malveillants (virus, cheval de Troie, logiciel publicitaire, rançongiciel, etc.)

3 La divulgation de données personnelles, appelée *doxing* ou *doxxing* en anglais, est une infraction consistant à rechercher et à divulguer sur Internet des informations sur l'identité et la vie privée d'un individu dans le but de lui nuire. (source : article « Divulgation de données personnelles » sur Wikipédia France).

4 L'atteinte à la vie privée collective fait référence à des actions ou des comportements qui compromettent la confidentialité et les droits d'un groupe de personnes plutôt que ceux d'un individu.

Les permissions données à une application sur un smartphone

Les **permissions** données à une application de réseau social sur un smartphone sont des **autorisations techniques** qui déterminent les **accès** accordés par l'utilisatrice ou l'utilisateur à certaines **fonctionnalités** ou **données** présentes *dans* le téléphone.

Ce système provient des exigences en matière de confidentialité imposées par les systèmes d'exploitation mobiles (Android, iOS) pour que chaque application demande explicitement des accès aux **données sensibles** du terminal (photos, contacts, localisation, micro, etc.). L'objectif est de redonner à l'utilisateur le contrôle sur ses données au moment de l'installation ou lors de l'utilisation de fonctions spécifiques. L'utilisateur peut **accepter ou refuser**, voire **révoquer** ces accès ultérieurement depuis les paramètres du téléphone.

Si elle accorde des permissions excessives (localisation, contacts, stockage, etc.) l'utilisatrice ou l'utilisateur s'expose à des **risques de fuite de données personnelles**. Cette fuite peut être volontaire (par l'application elle-même) ou involontaire (piratage).

Il est donc crucial de limiter les permissions aux seules fonctionnalités nécessaires, de les contrôler régulièrement et d'être vigilant(e) quant aux applications installées sur son appareil.

🖥️ Activité

Penchons-nous sur les différentes permissions d'accès demandées par des applications populaires.

Pour commencer, choisissez **une application** à étudier, parmi celles qui vous sont proposées :

Discord	Facebook	Instagram
Snapchat	TikTok	Whatsapp

1. Téléchargement d'un fichier CSV

En utilisant un navigateur Web, **téléchargez le fichier CSV** correspondant à l'application retenue :

Nom	Adresses (URL) des fichiers CSV
Discord	`https://fmr.tf/s/permissions_discord.csv`
Facebook	`https://fmr.tf/s/permissions_facebook.csv`
Instagram	`https://fmr.tf/s/permissions_instagram.csv`
Snapchat	`https://fmr.tf/s/permissions_snapchat.csv`
TikTok	`https://fmr.tf/s/permissions_tiktok.csv`
Whatsapp	`https://fmr.tf/s/permissions_whatsapp.csv`

2. Import du fichier CSV

En utilisant le tableur[5] de votre choix, **importez le fichier CSV** dans un nouveau document.
Puis, répondez aux questions suivantes :

Quels sont les descripteurs du tableau importé ?

Combien comptez-vous d'enregistrements ?

3. Nouvelle colonne

- Ajoutez une **nouvelle colonne**, à gauche de votre tableau.
- Donnez-lui le descripteur suivant : `Donnée personnelle ?`

4. Sauvegarde intermédiaire

Sauvegardez votre travail dans un fichier qui portera votre **nom**, **prénom**, **classe** et nom de l'application choisie.

Exemple de nom de fichier : `Durand Ambre 2nde10 TikTok`

Note : Vous pouvez choisir *l'extension de fichier* de votre choix.
Par exemple : `.ods` pour LibreOffice Calc, ou `.xlsx` pour Excel.

5. Analyse des permissions, édition du tableau

Lisez la **description** de chacune des **permissions** de votre tableau.

Selon-vous, est-ce que certaines de ces permissions représentent un risque pour vos données personnelles ?

→ Si c'est le cas, **ajoutez le mot** `oui` dans la colonne "Donnée personnelle ?" de la permission.
→ Sinon, laissez la case vide.

6. Sauvegarde finale

Sauvegardez vos dernières modifications (dans le même fichier qu'à l'étape 4).

7. Envoi de votre travail

Envoyez votre fichier à l'adresse suivante :

`https://fmr.tf/drop`

5 Voir, à ce propos, le cours « Données structurées : recherche, filtre, tri, calcul ».