4e

# Réseau informatique
# Synthèse 3

## La cyberviolence : usurpation d'identité, usage détourné

Lorsque l'on utilise Internet et les réseaux sociaux, on peut être confronté à la cyberviolence. Il est important de savoir ce qu'est la cyberviolence et comment s'en protéger.

La cyberviolence peut prendre plusieurs formes :

- **Cyberviolence** : *Actes malveillants* commis par le biais des technologies numériques, tels que *les insultes, les menaces, le harcèlement ou la diffusion de photos ou vidéos privées.*
- **Usurpation d'identité** : *Utilisation de l'identité d'une autre personne sans son consentement* pour commettre des actes malveillants.
- **Usage détourné** : *Utilisation d'une image ou d'une information à des fins malveillantes*, sans l'autorisation de la personne concernée.

Afin de mieux se protéger des cyberviolences, on peut :

- **Ne pas répondre** aux cyberviolences : ignorer les messages et les commentaires haineux.
- **Conserver les preuves** : sauvegarder les messages, les commentaires et les captures d'écran des cyberviolences.
- **En parler à un adulte de confiance** : parents, professeurs, éducateurs ou responsables associatifs.
- **Signaler les cyberviolences** : aux plateformes sur Internet et aux autorités.

La cyberviolence se manifeste par des **actes malveillants** tels que le **harcèlement**, la **diffusion de contenus privés** ou l'**usurpation d'identité**. Pour s'en protéger, il est important de **ne pas répondre aux agressions**, de **conserver les preuves** et d'en **parler à un adulte de confiance**. Il est également possible de **signaler les cyberviolences aux plateformes concernées** et aux autorités.

## La cybersécurité

Lorsque l'on navigue sur Internet, on laisse des **traces numériques** : une **adresse IP**, un **historique de navigation** des sites visités ou les recherches effectuées. Ces informations peuvent être utilisées pour **tracer l'utilisateur, l'identifier, lui voler ses données personnelles**…

La cybersécurité vise à se protéger contre ces dangers et à garantir la sécurité de nos données.

Il faut connaître les informations qui peuvent être ciblées par malveillance :

- **Données personnelles** : toutes les informations concernant l'utilisateur, comme le nom, l'adresse, le numéro de téléphone ou des photos privées.
- **Traces numériques** : informations laissées sur Internet, comme l'historique de navigation, les cookies ou les messages sur les réseaux sociaux.
- **Géolocalisation** : position géographique déterminée grâce aux GPS des smartphones ou aux adresses IP des ordinateurs.
- **Identification** : processus qui permet de déterminer l'identité d'une personne.
- **Authentification** : processus qui permet d'autoriser des accès à des ressources informatiques.
- **Propriété intellectuelle** : ensemble des droits qui protègent les créations intellectuelles, comme les inventions, les œuvres littéraires et artistiques ou les logiciels.

Pour se protéger des dangers et garantir la sécurité des informations, il convient de :
1. **Protéger les données personnelles** : Ne jamais donner d'informations personnelles à des inconnus, utiliser des mots de passe forts et uniques pour chaque compte, et activer l'authentification à deux facteurs.
2. **Gérer les traces numériques** : Supprimer régulièrement les cookies, utiliser un navigateur web privé pour les recherches et configurer les paramètres de confidentialité sur les réseaux sociaux.
3. **Respecter la propriété intellectuelle** : Ne pas copier ou télécharger illégalement du contenu protégé par des droits d'auteur, et toujours citer les sources que l'on utilise.

La cybersécurité est la pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. Ces cyberattaques visent généralement à accéder à des informations sensibles, à les modifier ou à les détruire, à extorquer de l'argent aux utilisateurs. Il existe des moyens simples de se protéger, comme utiliser des mots de passe forts, gérer ses traces numériques et respecter la propriété intellectuelle.