Le cyber-harcèlement

Le reconnaitre, le prévenir, le traiter

Stephen LÉDÉ, Charge de mission TICE
CRDP de l'Academie de Montpellier -CDDP du Gard

Comprendre le cyber-harcèlement

Définition, formes, modalités et conséquences

Définition

Le cyber-harcèlement est le fait d'utiliser les TIC pour :

- Nuire à autrui de manière délibérée
- Nuire pendant une période répétée dans le temps

Formes du cyber-harcèlement

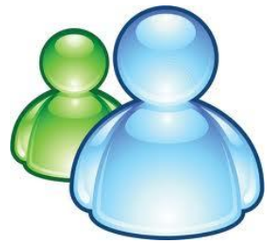
Le cyber-harcèlement se manifeste par :

- Les moqueries
- Les injures
- La diffamation
- Le discrédit
- L'intimidation
- L'usurpation d'identité
- Les menaces physiques
- Les prises de contact insistantes

Moyens du cyber-harcèlement

- Les téléphones portables

- Les messageries instantanées



- Forums, chat, jeux, blogs

- Les courriels

- Les réseaux sociaux

Formes du cyber-harcèlement

Avec un téléphone portable

- Envoyer des SMS-MMS désagréables (menaces, moqueries, insultes...)

- Prendre et partager des photos embarrantes (sexting : images sexuellement explicites)

- Filmer ou diffuser de la violence (happyslapping)

Formes du cyber-harcèlement

Avec la messagerie instantanée

- Piratage de compte et envoi de messages insultants
- Utilisation de login/mot de passe d'un camarade
- Envoi de messages ou contenus inappropriés
- Chantage au déshabillage

Formes du cyber-harcèlement

Avec les forums, chats, jeux

- Insultes et menaces anonymes
- Escroquerie (vol de compte joueur)
- Manipulation et chantage (création de fausse identité)

Formes du cyber-harcèlement

Avec les courriels

- Harceler une personne en lui envoyant des messages indésirables de manière répétée
- Envoyer des contenus inappropriés
- Transférer des emails privés
- Envoyer des virus, des spams

Formes du cyber-harcèlement

Avec les réseaux sociaux

Ils rassemblent tous les usages vus auparavant

- Publier des photos ou vidéos humiliantes
- Publication de commentaires désagréables
- Usurpation de comptes
- Création de faux profil pour intimider
- Création d'un groupe humiliant (nom d'une personne, injures)
- Mise à l'ecart d'une personne

Modalités de cyber-harcèlement

- Il se produit partout et tout le temps (24h/24 et 7j/7)
- Diffusion massive et instantanée, sans aucun contrôle
- Caractère permanent des contenus diffusés
- Anonymat possible du harceleur
- Empathie difficile : distance avec la victime encourage agressivité et banalisation de la violence

Modalités de cyber-harcèlement

Toute publication sur Internet laisse des traces :

Le cyber-harcèlement est donc plus facile à prouver

Conséquences du cyber-harcèlement

Le cyber-harcèlement a les mêmes conséquences que le harcèlement :

- Blessures durables de l'enfant
- Culpabilité, dévalorisation pour le harceleur, la victime et le spectateur
- Conséquences scolaires, sociales et psychiques de longue durée pour tous les acteurs de la vie scolaire

Prévenir le cyber-harcèlement

Protection des informations personnelles, outils pédagogiques, encadrement des usages

Protection des informations personnelles

Elle passe par :

- La gestion des mots de passe
- La gestion des paramètres de confidentialité des réseaux sociaux
- Le respect de la vie privée
- Le respect du droit à l'image

Gestion des mots de passe

Par simplicité la majorité des utilisateurs définit un **mot de passe unique** pour tous les services

50% des internautes utilisent un mot de passe unique

Source : Étude Imperva, janvier 2010

Gestion des mots de passe

Parmi les mots de passe courants, citons :

- qwerty ou azerty
- les prénoms

20% des internautes font leur choix parmi un panel de 5000 mots seulement !

Gestion des mots de passe

Un bon mot de passe doit donc comporter :

- Des lettres (a, b, c, d ...)
- Des chiffres (1, 2, 3 ...)
- Des majuscules ou minuscules
- Des caractères spéciaux (€, @, &, $, £...)

Il est unique pour chaque service utilisé

Comment le retenir ?

Gestion des mots de passe

On code un mot et on va retenir :

- Le mot de départ
- La technique de codage

Gestion des mots de passe

Exemples de compositions:

Supprimez les doublons dans un mot assez long et ajoutez la longueur originale.

Exemple : « **suppression** » donne ***supresion-11***

Gestion des mots de passe

Autre exemple :

Ecrivez un mot phonétiquement en combinant majuscules, minuscules et chiffres.

Exemple : « **suppression** » donne ***SuPRe6on***

Gestion des mots de passe

Autre exemple :

Choisir une phrase et prendre les premières lettres de chaque mot.

Exemple : « **les sanglots longs des violons de l’automne** » donne « ***lsldvdla*** »

Etc, etc. etc...

Outils pédagogiques

2025 ex machina

- 2025 ex machina est un serious game dédié aux 12-17 ans

- Le but : on est en 2025 et des faits compromettants refont surface. Il faut retourner dans le passé pour changer le cours des événements !

- 2025 comporte des jeux à mener collectivement ou individuellement sur ordinateur ou smartphone.

2025 ex machina

- Les serious game proposés permettent d'aborder 4 situations :
    - Les réseaux sociaux
    - Les jeux vidéos en ligne
    - L'Internet mobile
    - Blog, chat et forum

CNIL Jeunes

- CNIL Jeunes comporte de nombreuses ressources pour un usage responsable d'Internet
    - Espace dédié aux enseignants avec fiches pédagogiques et méthodologiques
    - Espace dédié aux parents avec fiches informatives et tutoriels
    - Espace pour les jeunes avec jeux et sensibilisation

Encadrement des usages

- L'utilisation du téléphone portable en établissement doit être inscrite dans le règlement intérieur (L 511-5 du code de l'Education)
- Une filtrage efficace est indispensable (liste fournie par l'Université de Toulouse ou les fournisseurs d'accès pour les petites structures)
- NetEcoute (0820 200 000) peut vous aider à configurer ces services en cas de besoin

Cas pratiques

Quelles réactions possibles ?

Cas n°1

- Un élève est battu par d'autres élèves et filmé à son insu.

- Ce film est transmis par Bluetooth à d'autres élèves de l'établissement.

- Le film est également diffusé sur internet au moyen d'un blog

Une législation récente

- Il s'agit d'un happy-slapping ou "*gifle joyeuse*"

- Il porte atteinte à la dignité humaine et aux valeur scolaires (article L121-1 du Code de l'éducation)

- Avant le 22 février 2007 il ne pouvait être rattaché qu'à une forme de non-assistance à personne en danger (article 223-6 CP)

- Depuis cette date il est possible d'utiliser l'article 222-33-3 CP pour réprimer le happy-slapping

Cas n°2

- Des élèves vont chercher la photo d'un professeur sur Facebook.

- Un article plutôt sympathique est diffusé sur le blog d'un élève

- Certains commentaires sont désobligeants voire insultants

Plusieurs notions juridiques en jeu

- Un cadre de communication numérique
- Une atteinte à la vie privée d'autrui
- Une atteinte à la représentation de la personne
- Un outrage
- Diffamation et injure
- Une victime de la communication numérique

Un cadre de communication numérique

- La réalité du droit pénal s'applique au monde virtuel de l'Internet en vertu de deux lois :
  - Loi du 30 septembre 1986 sur la communication audiovisuelle
  - Loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Une atteinte à la vie privée d'autrui

- L'accès a un établissement scolaire n'est pas possible pour tous : ce n'est pas un lieu public mais une propriété publique représentant un lieu privé

- L'atteinte à la vie privée est résumée dans les articles 226-1 et 226-2 CP

- La photo est enregistrée sans la consentement de la personne

- Il s'agit d'une photo d'une personne se trouvant dans un lieu privé

Une atteinte à la représentation de la personne

- Ce cas se pose lorsqu'il y a photomontage non consenti
- Ce photomontage ne doit pas être explicite et ne doit comporter aucune mention
- L'article 226-8 CP comporte mention de ceci.

Un outrage

- Pour qu'il y ait outrage,il faut qu'il y ait :
  - Des paroles, gestes, menaces, écrits ou images
  - À l'encontre d'une personne chargée d'une mission de service public
  - Dans l'exercice ou à l'occasion de l'exercice de sa mission
  - Portant atteinte à sa dignité ou au respect dû a sa fonction
  - La communication doit être directe (face à face ou par écrit)

Diffamation et injure

- Ces notions sont précisées dans l'article 29 de la loi sur la liberté de la presse du 29 juillet 1881.

- La diffamation est une affirmation publique d'un fait mensonger dont il faut démontrer le caractère fallacieux

- L'injure est blessante sans aucune démonstration nécessaire

- Il est prévu jusqu'à 12000€ d'amende auxquels on peut ajouter des dommages et intérêts pour préjudice moral à la victime

Une victime de la communication numérique

- L'article 6-IV de la LCEN prévoit un droit de réponse mais il faut qu'il y ait débat légitime : ceci ne s'applique pas s'il y a diffamation ou injure

- L'article 6-I-5 de la LCEN prévoit les conditions de retrait des informations litigieuses mais il nécessite de la part de la victime de fournir des informations très détaillées à son offenseur

Une victime de la communication numérique

- Dans ce cas on préfèrera une attaque au motif de diffamation et/ou injure au pénal
- Une action civile reste possible (art 1382 CC "***Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.***")

Une victime de la communication numérique

- Pour qu'il y ait action pénale il ne doit pas y avoir de consentement.

- Si le consentement est acquis, la seule action possible sera civile (art9 CC "***Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes les mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé***")

Une victime de la communication numérique

- Le Code Civil pose deux conditions :
    - Il faut qu'un dommage soit subi
    - Il faut que soit porté atteinte à la vie privée et à son intimité
- Les limites entre vie privée / publique ainsi que l'intention de nuire relèvent de la subjectivité du magistrat