



e-réputation et harcèlement numérique

ou

Comprendre ses droits et responsabilités face au cyber-harcèlement

Résumé : fiche d'activité pour mettre en place un mémo élève autour des notions de e-réputation et de cyber-harcèlement (définitions, droits, responsabilités et protection).

Thématique : Réseaux sociaux

Point du programme traité :

Contenus : Les réseaux sociaux peuvent être le support d'un harcèlement numérique, par le biais de photographies partagées sans consentement ou impossibles à retirer, par la diffusion de fausses nouvelles, de dénonciations ou de calomnies.

Des pratiques, des outils et des services permettent de se protéger, lutter et dénoncer de tels agissements.

Capacité mobilisée:

Connaître les dispositions de l'article 222-33-2-2 du code pénal.

Compétence transversale mobilisée :

Faire un usage responsable et critique des sciences et technologies numériques.

Lieu de l'activité : En salle informatique ou CDI

Matériels / logiciels utilisés : Ordinateur avec navigateur web

Durée de l'activité : 2h00

1) Deux accroches possibles

un slogan : Une photo c'est perso, la partager c'est harceler

<https://www.nonaharcelement.education.gouv.fr/>

une vidéo de la CNIL: réfléchissez avant de cliquer :

<https://www.youtube.com/watch?v=5V2xOPLoS8&feature=youtu.be>

Constats et interrogations à amener avec les élèves:

Tout le monde utilise les photos et vidéos.

Qui connaît le cadre législatif autour de ces données ?

Qui connaît les signes d'un cyberharcèlement ?

Qui connaît la démarche à suivre si l'on est témoin, victime ?

Qui connaît les moyens et outils pour préserver sa e-réputation ?

2) Introduction : définition et impacts de l'e-reputation

Définir l'identité numérique :

L'identité numérique est constituée de toutes les données associées à votre nom sur la Toile. Il peut s'agir d'éléments identitaires : patronyme, statut professionnel, diplômes obtenus, expériences précédentes. Ce sont des données normalement maîtrisées, puisque c'est vous qui les avez mise en ligne.

Définir l'e-réputation :

L'e-réputation correspond à votre image en ligne. La réputation en ligne est entretenue par tout ce qui vous concerne et qui est mis en ligne sur les réseaux sociaux, les blogs ou les plate formes de partage de vidéos, directement par vous mais aussi par d'autres.

Éviter et dépister le harcèlement au lycée :

Il se traduit souvent par des violences verbales, physiques et/ou morales de façon répétée (bousculades, vols, surnoms méchants, insultes, moqueries, rejets...).

Lorsque ces mêmes faits se déroulent sur les réseaux sociaux, par SMS ou par mail, on parle alors de cyberharcèlement.

Exemples de situations de cyber-harcèlement :

Happy slapping : lynchage en groupe puis publication de la vidéo sur un site

Propagation de rumeurs par téléphone, sur internet.

Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.

Publication de photographies sexuellement explicites ou humiliante

Messages menaçants, insulte via messagerie privée

Commande de biens/services pour la victime en utilisant ses données personnelles

Conséquences du cyber-harcèlement

Il peut générer des conséquences graves pour :

- la scolarité (baisse des résultats scolaires, décrochage scolaire)
- la santé (maux de ventre ou de tête, perte de l'estime de soi, profond mal être).

La cyberviolence et le cyber-harcèlement ont des conséquences graves sur les victimes mais aussi les agresseurs et les témoins. Il existe un consensus général selon lequel ces conséquences seraient plus importantes que celles du harcèlement traditionnel en raison des caractéristiques

particulières de ce type de violence (anonymat, pouvoir de dissémination et public élargi etc.). Il existe des différences selon le type de cyberviolence et les jeunes sont plus affectés par des abus au moyen du téléphone portable ou par la diffusion indésirée de photographies/vidéo clips de la victime que par des courriels désagréables ou des agressions dans des réseaux sociaux. Contrairement à la violence ordinaire, face à l'écran, les victimes sont très souvent seules et ne peuvent pas être aidées par leurs camarades.

Surveiller sa e-réputation pour sa vie d'adulte :

Moteurs de recherche et réseaux sociaux permettent à un employeur, un recruteur, un client, ou à un proche d'accéder à des informations sur vous, qu'elles soient de nature professionnelle ou personnelle. Cette pratique est d'ailleurs si courante qu'on emploie l'expression « googliser » quelqu'un quand on cherche des informations sur cette personne sur un moteur de recherche et « stalker » pour qualifier une personne qui espionne une autre sur les réseaux sociaux. Il est donc très important aujourd'hui de contrôler et de maîtriser son image en ligne, qui est accessible par tous.

Sources: <https://www.nonaharcelement.education.gouv.fr/que-faire/je-suis-victime/#collegelycee>
<https://www.cnil.fr/fr/nos-conseils-pour-mieux-maitriser-votre-reputation-en-ligne>
<https://www.cnil.fr/fr/reagir-en-cas-de-harcelement-en-ligne>

3) Une activité possible en classe : Construire un mémo utilisateur

a) Les objectifs élèves

Lister avec les élèves les points à maîtriser pour être un utilisateur averti des réseaux sociaux. Proposer d'élaborer un mémo synthèse (sous forme de tableau, carte mentale, affiche....).

Objectif possible : outil de sensibilisation à construire pour des élèves de 3ème par exemple.

b) Des ressources possibles organisées sous forme de tableau

sites génériques

<https://www.nonaharcelement.education.gouv.fr/>

<https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/>

Tableau possible avec ressources disponibles associées

Utilisateur	Victime ?
<p>Code de bonne conduite</p> <p>Identifier le cyberharcèlement : https://www.nonaharcelement.education.gouv.fr/que-faire/quest-ce-que-le-cyberharcèlement/</p>	<p>Comment vérifier sa e-réputation ? https://www.cnil.fr/fr/nos-conseils-pour-mieux-maitriser-votre-reputation-en-ligne</p> <p>tester son e-reputation https://webmii.com/</p>
<p>Connaître la loi https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000029334247</p> <p>https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006419738&cidTexte=LEGITEXT000006070722</p> <p>https://www.cnil.fr/fr/les-sanctions-penales</p> <p>https://www.cnil.fr/fr/demander-le-retrait-de-votre-image-en-ligne</p> <p>si quelqu'un d'autre est harcelé? https://www.cnil.fr/fr/reagir-en-cas-de-harcèlement-en-ligne</p> <p>https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201</p>	<p>Comment réagir face à une atteinte à sa e-réputation ? https://www.cnil.fr/fr/reagir</p> <p>https://www.cnil.fr/fr/nos-conseils-pour-mieux-maitriser-votre-reputation-en-ligne</p> <p>Comment réagir lorsque je suis témoin ? https://www.nonaharcelement.education.gouv.fr/wp-content/uploads/2018/11/2018_NAH_infog_en-cas-de-harcèlement.pdf</p>
<p>Connaître les sanctions encourues en cas d'écart à la loi</p> <p>mêmes liens que connaître la loi</p>	<p>Comment protéger sa e-reputation ? Gérer ses données personnelles : https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles</p> <p>les bonnes pratiques : https://www.cnil.fr/fr/maitriser-mes-donnees</p>

c) Des attendus possibles

Utilisateur	Victime ?
<p>Code de bonne conduite</p> <ul style="list-style-type: none"> - Toujours demander l'accord d'autrui avant de prendre une photo, une vidéo..... - Vérifier sa e-reputation et se protéger <p>Identifier le cyberharcèlement :</p> <p>Il peut prendre plusieurs formes telles que :</p> <ul style="list-style-type: none"> • les intimidations, insultes, moqueries ou menaces en ligne • la propagation de rumeurs • le piratage de comptes et l'usurpation d'identité digitale • la création d'un sujet de discussion, d'un groupe ou d'une page sur un réseau social à l'encontre d'un camarade de classe • la publication d'une photo ou d'une vidéo de la victime en mauvaise posture • le sexting (c'est la contraction de « sex » et « texting ». On peut le définir comme « Des images produites par les jeunes (17 ans et moins) qui représentent d'autres jeunes et qui pourraient être utilisées dans le cadre de la pornographie infantile 	<p>Comment vérifier sa e-réputation ?</p> <ol style="list-style-type: none"> 1- Tapez régulièrement votre nom dans un moteur de recherche pour voir quelles informations vous concernant circulent sur les moteurs de recherche ou bien dans un réseau social ; 2- Paramétrez des notifications qui vous préviennent lorsque votre nom, votre adresse électronique ou d'autres données sont en ligne. Des services privés proposent cette fonctionnalité pour les particuliers. Néanmoins, soyez conscient que ce type de service gratuit entraîne une contrepartie, souvent liée à l'exploitation de vos données, par exemple à des fins de ciblage publicitaire
<p>Connaître la loi</p> <ul style="list-style-type: none"> - <u>Le harcèlement</u> est un délit (pénal) : article 222-33-2-2 - <u>Injure et diffamation</u> sont punies : loi du 29 juillet 1881 - <u>La collecte et la conservation de données personnelles</u> peuvent être un délit : articles 226-18 et 226-19 - <u>la collecte, transmission et publication de données personnelles</u> peuvent être des délits : Les articles 226-1 et 226-8 du code pénal - <u>Le fait de « partager »</u> implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement - <u>L'usurpation d'identité</u> est un délit pénal 226-4-1 du code pénal 	<p>Comment réagir face à une atteinte à sa e-réputation ?</p> <p>Problème d'image :</p> <ol style="list-style-type: none"> 1- Retrouver les coordonnées d'un organisme pour exercer vos droits (souvent en bas de la page d'accueil du site concerné, par la CNIL,) 2- Demander le retrait de votre image en ligne (auteur, site) <p>Problème de piratage de compte :</p> <p>réagir si compte piraté (informer et réinitialiser le mot de passe)</p> <p>Cyber harcèlement</p> <ol style="list-style-type: none"> 1- ne pas répondre ni se venger 2- verrouiller l'ensemble de ses comptes sociaux <p>Dans tous les cas alerter un adulte</p> <p>Un adulte référent (proche, dans établissement scolaire,.....)</p> <p>appeler 30 20</p> <p>netecoute.fr ou 0 800 200 000</p>

	<p>porter plainte est possible 0800 235 236</p> <p>Demander d'appliquer le droit à l'oubli pour les mineurs (suppression intégrale d'un site) L'article 40 modifié de la loi informatique et Libertés – au même titre que le Règlement européen sur la protection des données - consacre un droit à l'oubli spécifique pour les mineurs. Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement demander au site l'effacement des données le concernant et ce, dans les meilleurs délais. En pratique, si le responsable de traitement n'a pas effacé les données ou répondu à la personne dans un délai d'un mois, la personne concernée peut saisir la CNIL</p> <p>Comment réagir lorsque je suis témoin ? => cf alerter adulte référent ou N° d'appel déjà mentionnés</p>
<p>Connaître les sanctions encourues en cas d'écart à la loi</p> <p>- Harcèlement: peine d'an d'emprisonnement et de 15 000 €</p> <p>- Injure et diffamation amende de 12.000€</p> <p>- Collecte et mémorisation des informations Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.</p> <p>- Enregistrement/ transmission de données privées un an d'emprisonnement et 45 000 € d'amende</p>	<p>Comment protéger sa e-reputation ? Gérer ses données personnelles :</p> <ul style="list-style-type: none"> • droit d'information (connaître les données utilisées) • droit d'opposition utilisation de données (pour des fichiers non obligatoires) • droit d'accès aux données (Obtenir et vérifier les données qu'un organisme détient sur vous.) • droit de rectification de données (Rectifier les informations inexactes vous concernant) • droit de déréférencement (Ne plus associer votre nom-prénom à un contenu visible dans un moteur de recherche.) • droit d'effacement • droit à la portabilité (Emporter une copie de vos données pour les réutiliser ailleurs) • droit lié au profilage • (Remonter le fil de votre profilage, vous y opposer et demander l'intervention d'un humain dans une décision automatisée vous concernant.) • droit à la limitation des données (demander à un organisme de geler

le fait de porter atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

un an d'emprisonnement et de 15 000€ d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

- Usurpation d'identité:

peine d'un an d'emprisonnement et de 15.000€ d'amende

temporairement l'utilisation de certaines de vos données)

Certains particuliers, artisans/commerçants et personnalités publiques font appel à des entreprises d'e-réputation

les bonnes pratiques :

- Connaître les 10 principes clés

- 1- Réfléchissez avant de publier
2. Respectez les autres
3. Ne dites pas tout
4. Sécurisez vos comptes
5. Créez plusieurs adresses e-mail
6. Attention aux photos et aux vidéos
7. Utilisez un pseudonyme
8. Attention aux mots de passe
9. Faites le ménage dans vos historiques
10. Vérifiez vos traces

- 4 réflexes

<https://www.cnil.fr/fr/4-reflexes-pour-mieux-protger-votre-identite-en-ligne>

- Comprendre ses traces

cours sur le web et les données

<https://www.cnil.fr/fr/comment-ca-marche>

- Configurer ses outils

<https://www.cnil.fr/fr/configurer>

- Réagir en cas de problème