INCLUSION NUMÉRIQUE ET SOLIDARITÉ

DÉCEMBRE 2019

CYBERHARCÈLEMENT : LECTURE ACADÉMIQUE DE CE PHÉNOMÈNE

RENAISSANCE numerique

PRÉAMBULE

L'objectif de cette note est d'offrir un aperçu de la recherche académique existante sur le sujet du cyberharcèlement — plus précisément, le cyberharcèlement chez des jeunes — qui peut nourrir l'approche française. Cette note est organisée selon les grands axes qui se retrouvent dans la littérature, avec une attention particulière portée à l'intervention (prévention, détection, réponse). Un index des programmes internationaux dans la prévention et des centres de ressources est fourni à la fin de la note, ainsi que des recommandations concrètes pour les parties prenantes identifiées.

La recherche dans ce champs présente une faiblesse, en partie en raison des défis liés à la collecte de données et également au rythme de la recherche académique par rapport à la vitesse des changements sur le Web. Cette faiblesse est même plus marquée dans la littérature française. Pour cette raison, cette note s'appuie davantage sur la recherche anglophone.

TABLE DES MATIÈRES

CE QU'IL FAUT RETENIR ____ 6

PARTIE 1
MIEUX COMPRENDRE LE CONCEPT ____ 8

Cyberharcèlement vs. harcèlement « classique » ____ 9

Typologies du cyberharcèlement ____ 10

Des degrés divers de vulnérabilité en ligne ____ 15

PARTIE 2
RÉPONSES ET MÉCANISMES DES DIFFÉRENTS ACTEURS ____ 16

Stratégies chez les plateformes : pistes d'amélioration ____ 17

Prévenir par la pédagogie ____ 19

Mécanismes de réaction (« coping mechanisms ») chez les enfants ____ 20

Mobiliser les enfants pour construire une réponse efficace ____ 23

RECOMMANDATIONS PAR PARTIE PRENANTE ____ 25

ANNEXES ____ 31

Pratiques inspirantes ____ 32

Pour aller plus loin ____ 33

CE QU'IL FAUT RETENIR

- La cyberviolence consiste en des violences ponctuelles alors que le cyberharcèlement consiste en des violences répétées.
- Le déséquilibre de pouvoir entre le harceleur et la victime peut être lié aux compétences du premier relatives aux outils numériques.
- Le réflexe de représailles peut être plus fort dans le cyberharcèlement ; ce qui fait que la victime devient l'agresseur.
- La plupart des cas de cyberharcèlement se produisent en dehors de l'école.
- Le cyberharcèlement touche de façon disproportionnée les filles, les membres des minorités sexuelles, raciales ou ethniques et les enfants ayant des problèmes de santé mentale et des problèmes de comportement.
- Les victimes soutenues ou défendues par des témoins sont moins déprimées et anxieuses, ont une meilleure estime de soi et sont finalement moins rejetées par leurs pairs que les autres.
- Quand les enfants comprennent que le cyberharcèlement n'est pas la norme, les taux de harcèlement diminuent.
- Les programmes scolaires de lutte contre le cyberharcèlement sont moins efficaces s'ils sont conçus pour une période limitée, plutôt que pour une longue durée.
- Les élèves ont souvent l'impression que les enseignants et les adultes ne sont pas conscients du problème ou sont incapables de les aider efficacement ; ce qui les décourage de les informer.
- Il existe un aspect de migration entre plateformes dans le cyberharcèlement qui mérite davantage de recherche.
- Les enfants lisent et comprennent rarement les politiques de confidentialité des services qu'ils utilisent et ils ne comprennent pas les limites public-privé de ces espaces, ni les diverses options de sécurité et de recours qui leur sont offertes.
- Les programmes de prévention et d'intervention les plus réussis concernent l'implication des enfants eux-mêmes.
- Malgré une prolifération de ressources disponibles en ligne s'adressant aux internautes sur le sujet du cyberharcèlement, la recherche de conseils en ligne comme mécanisme de réaction s'avère moins efficace que d'autres stratégies chez les harcelés.

PARTIE 1
MIEUX COMPRENDRE LE CONCEPT

CYBERHARCÈLEMENT VS. HARCÈLEMENT « CLASSIQUE »

Le cyberharcèlement est souvent défini en élargissant la définition de harcèlement « classique », qui repose sur trois critères principaux : 1) un comportement agressif intentionnel ; 2) des actes répétitifs ; et 3) une relation interpersonnelle caractérisée par un déséquilibre systématique de pouvoir (Olweus, 1993). Le cyberharcèlement décrit un comportement qui correspond à ces trois catégories et qui utilise des formes électroniques de contact (Kowalski et al., 2012, 2014 ; Patchin et Hinduja, 2012). Blaya réaffirme l'importance de l'aspect de répétition dans le cyberharcèlement, le distinguant ainsi de la cyberviolence. Pour Blaya, **la cyberviolence consiste en des violences ponctuelles, alors que le cyberharcèlement consiste en des violences répétées au moins une fois par semaine sur une durée d'un mois** (Blaya, 2018).

Il existe pourtant des limites théoriques et pratiques à l'applicabilité de ces trois caractéristiques au cyberharcèlement. Par exemple, l'intention est difficile à déterminer dans un environnement en ligne (Hee et al., 2018). Le concept de répétition dans le cyberharcèlement n'est pas simple non plus, car les technologies numériques fournissent aux agresseurs un moyen de propager largement le cyberharcèlement, de sorte qu'un seul acte peut devenir répétitif avec le temps (Slonje et al., 2012). **En ce qui concerne le déséquilibre de pouvoir, la force relative du cyberharcèlement peut être liée aux compétences en matière d'outils numériques** (Cross et al., 2009). La question de savoir si le cyberharcèlement devrait se limiter aux relations entre pairs, alors que toutes les formes de harcèlement en ligne ne se déroulent pas entres pairs, fait également l'objet d'un débat (Cross et al., 2009).

Vu que le cyberharcèlement se passe (au moins en partie) dans un environnement virtuel, les agresseurs ne sont pas toujours conscients des conséquences de leurs actions et des effets sur leurs victimes (Blaya, 2013). L'anonymat possible dans le cyberharcèlement est souvent mentionné comme une différence significative par rapport au harcèlement traditionnel. Mais de nombreuses autres différences ont été notées. Le cyberharcèlement a été associé à des conséquences plus négatives, y compris de graves souffrances psychologiques chez les victimes (Kim et Song, 2013 ; Song, 2017). La victime dans le cyberespace ressentant souvent l'intimidation « seule » ou isolée,

le choc psychologique peut être plus grave (Cho, 2013 ; Seo et Cho, 2013). **Le réflexe de représailles peut également être plus fort dans le cyberharcèlement ; ce qui fait que la victime devient l'agresseur** (Kowalski et Limber, 2007).

Selon Slonje, malgré un chevauchement important entre le harcèlement classique et le cyberharcèlement (Salmivalli et Pöyhönen, 2012), **la plupart des cas de cyberharcèlement se produisent en dehors de l'école** (Slonje et al., 2012). En France, une étude réalisée en 2014 par Kubiszewski et al. sur le chevauchement entre le cyberharcèlement et le harcèlement à l'école chez les adolescents français a montré que « *le cyberharcèlement ne s'inscrit pas dans le harcèlement scolaire mais offre plutôt aux autres élèves de nouvelles possibilités de harceler* » (Kubiszewski et al., 2014). Il a été fréquemment noté que **les lieux du cyberharcèlement reflètent les technologies les plus utilisées de l'époque** (Whittaker et Kowalski, 2014) **et sont donc propres au contexte et se transforment sans cesse.** Selon l'ONG britannique *Ditch The Label*, qui mène une enquête annuelle sur le harcèlement chez les lycéens et les étudiants de fac au Royaume-Uni, le cyberharcèlement est le plus répandu sur Instagram (42%), suivi par Facebook (37%) et Snapchat (31%) (*Ditch The Label*, 2017). **Il y a également un aspect trans-plateforme notable : le harcèlement peut commencer sur une plateforme et se déplacer sur une autre, ou bien un cyber-harceleur peut atteindre une victime par d'autres plateformes que celle où l'échange a commencé**. D'autres recherches sont nécessaires pour appréhender ce phénomène de migration.

TYPOLOGIES DU CYBERHARCÈLEMENT

LES DIFFÉRENTS RÔLES

De nombreuses réponses au cyberharcèlement, en particulier en ce qui concerne l'usage des technologies d'intelligence artificielle et la détection du cyberharcèlement, se concentrent sur la relation binaire de harceleur/victime. Cependant, **une grande partie de la recherche sur le cyberharcèlement porte sur l'identification des différents rôles des participants et des témoins, ainsi que sur l'exploration de la gamme de la participation entre harceleur et victime.**

Hee et al. s'appuient sur quatre rôles : victime, harceleur, défenseur de la victime, et assistant au harceleur. Vandebosch et al. identifient trois types de témoins : ceux qui participent au harcèlement, ceux qui aident la victime et ceux qui ne font rien (Salmivalli et al., 1996 ; Vandebosch et al., 2018 ; Hee et al., 2018). Les recherches sur le harcèlement classique ont identifié jusqu'à huit modes différents de réaction chez les témoins (Olweus, 2001). **Il est à noter que victimes soutenues ou défendues par des témoins sont moins déprimées et anxieuses, ont une meilleure estime de soi et sont finalement moins rejetées par leurs pairs que les autres** (Sainio, Veenstra, Huitsing, et Salmivalli, 2011). **La sensibilisation et la formation des témoins font ainsi l'objet de nombreuses initiatives** (Leduc et coll., 2018).

LES TACTIQUES DE CYBERHARCÈLEMENT

La liste suivante comprend les actions qui sont généralement considérées comme des « tactiques » de cyberharcèlement. Les comportements peuvent être plus spécifiques selon les supports numériques utilisés. Cette liste, regroupée par thème, est une synthèse des ressources de *StopBullying.gov*, un site internet du gouvernement fédéral américain géré par le département de la Santé et des Services sociaux, l'Anti-Defamation League aux États-Unis, et CyberMentors, un programme lancé au Royaume-Uni par le premier ministre et la professeure Tanya Byron en 2009.

Il existe un spectre de harcèlement en ligne allant du « non technique » aux pratiques qui se rapprochent du piratage informatique. Cela renforce la notion préalablement évoquée d'un déséquilibre de pouvoir entre ceux qui ont des compétences techniques de niveau supérieur et les autres.

Thème	« Tactiques » de cyberharcèlement
Exclusion	• Exclure délibérément des personnes de jeux ou de groupes en ligne
Menaces, intimidation, provocation, incitation à l'automutilation	• Envoyer des messages menaçants ou gênants, menacer de blesser quelqu'un, dire à quelqu'un de se suicider • La création de sites Web ou de groupes de haine contre un individu • Voler le mot de passe et bloquer l'accès de quelqu'un à son compte • « *Trolling* » : provoquer quelqu'un avec des comportements réactionnaires • « *Flaming* » : dénigrer quelqu'un dans un environnement public en ligne en utilisant un langage profane ou vulgaire pour affirmer son pouvoir ou établir une position dominante • « *Happy Slapping* » : agresser physiquement ou embarrasser une victime tout en enregistrant l'incident avec des photos/vidéos, puis afficher le matériel en ligne publiquement • « *Cyberstalking* » : Appeler quelqu'un ou envoyer des messages à quelqu'un avec une formulation grave, persistante ou envahissante et qui suscite une inquiétude injustifiée chez le répondant • Causer indirectement des dommages à l'appareil digital de la victime (par exemple, en infectant l'ordinateur de la victime avec un logiciel malveillant)
Exposition, abus de la vie privée	• Affichage ou transmission de communications ou images personnelles • Diffusion des images de webcams d'une manière menaçante ou manipulatrice • « *Doxing* » (forme abrégée du mot « documents ») : rendre publics les renseignements personnels d'une personne (adresse, numéro de téléphone, informations sur les comptes de médias sociaux, et d'autres données privées)
Atteinte à la réputation, dénigrement	• Poster des commentaires ou des rumeurs sur quelqu'un en ligne • Afficher une photo ou une vidéo dénigrante • Faire et partager des images ou des vidéos dénigrantes (dans certains cas, ce partage d'images peut constituer un acte criminel s'il s'agit d'images pornographiques et d'enfants mineurs) • Créer ou voter pour quelqu'un dans un sondage en ligne insultant (une fonction offerte par de nombreux sites internet)
Diffamation sévère, impliquant des autorités	• Faire de fausses allégations au fournisseur de service internet au sujet de la victime qui affiche de l'information sensible ou inappropriée • Encourager la victime à s'engager dans le piratage numérique et puis le signaler aux autorités, à ses parents ou aux éducateurs • Partager de fausses informations concernant la victime sur le fait qu'il/elle planifie une attaque violente

Usurpation d'identité	• Voler une identité en ligne • Faire semblant d'être quelqu'un d'autre en ligne afin de solliciter ou d'afficher des renseignements personnels ou faux • Usurper l'identité d'une personne pour faire des commentaires en ligne qui lui causent du tort • « *Mirroring* » : utiliser un nom utilisateur presque identique à celui de la victime • Inscription de quelqu'un à de nombreuses listes marketing de pornographie et/ou de publicité par email et par messagerie instantanée • « *Phishing* » : tromper, persuader ou manipuler quelqu'un pour qu'il révèle des renseignements personnels ou financiers à son sujet ou au sujet de ses proches1
Harcèlement sexuel avec des supports numériques	• L'enregistrement d'images ou de vidéos de la victime qui peuvent être interprétées comme étant de nature sexuelle, souvent prises sans son consentement, et qui sont publiées ou partagées à grande échelle afin de faire honte à la victime (ciblant principalement les filles) • « *Sextortion* » : le fait d'exploiter d'autres enfants à des fins sexuelles et/ou des activités liées à la sexualité en échange de ne pas divulguer des informations à leur sujet

1 Bien naturellement, un message de phishing envoyé par un enfant ne contiendra probablement pas un logiciel malveillant utilisé par un cybercriminel. Ce qui est le plus souvent en danger, ce sont les renseignements personnels.

DES DEGRÉS DIVERS DE VULNÉRABILITÉ EN LIGNE

Le cyberharcèlement comporte de graves risques et certains enfants sont plus exposés ou plus vulnérables que d'autres. Des facteurs comme le sexe, l'ethnicité et l'identité sexuelle peuvent correspondre à une exposition accrue au risque de cyberharcèlement. **Il a été constaté que le cyberharcèlement touche de façon disproportionnée les filles, les membres des minorités sexuelles, raciales ou ethniques et les enfants ayant des problèmes de santé mentale et de comportement** (Rice et al., 2015). **Le cyberharcèlement comporte souvent une composante de harcèlement sexuel et de honte liée au sexe ou à l'orientation sexuelle** (Shariff, 2008). Au Royaume-Uni, par exemple, les filles sont deux fois plus susceptibles que les garçons d'être victimes de cyberharcèlement, ainsi que les enfants non britanniques et des minorités ethniques (Cross et al.). Blaya note également dans sa recherche actuelle **une augmentation de la grossophobie** et cyberviolence envers les enfants en surpoids.

Au-delà de ces caractéristiques identitaires, **le rapport de force observé dans les interactions de cyberharcèlement peut être rattaché aux écarts en matière de compétences numériques.** Le programme britannique *Cybermentors* rejette ainsi l'idée que les jeunes sont intrinsèquement vulnérables en ligne et que s'ils restent hors ligne, ils seront plus en sécurité. Ils maintiennent que **les jeunes ayant un accès et une expérience internet limités sont particulièrement plus vulnérables en raison de leur manque de connaissance et de confiance dans les outils numériques** (Cross et al., 2009).

PARTIE 2
RÉPONSES ET MÉCANISMES DES DIFFÉRENTS ACTEURS

STRATÉGIES CHEZ LES PLATEFORMES : PISTES D'AMÉLIORATION

Les plateformes en ligne sont critiquées pour leur manque de régulation et leurs politiques de modération inadéquates. Mais au-delà de cela, il a été noté que les politiques de protection de la vie privée et les mécanismes de recours sont insuffisants ou présentés de manière insuffisante. Livingstone et Haddon remarquent que **les enfants lisent et comprennent rarement les politiques de confidentialité des services qu'ils utilisent et qu'ils ne comprennent pas les limites public-privé de ces espaces, ni les diverses options de sécurité et de recours qui leur sont offertes.** Selon Livingstone et Haddon, « *une partie de ce problème peut être corrigée par l'éducation aux médias, [mais] dans l'ensemble, une meilleure réglementation et une meilleure conception des interfaces sont nécessaires* » (Livingstone et Haddon, 2009).

Dans son enquête sur les réponses des plateformes au phénomène du cyberharcèlement, Milosevic note que certaines entreprises ont aussi créé des « centres de sécurité » (*Safety Corners*), qui peuvent rediriger les utilisateurs vers des associations afin d'obtenir de l'aide ou trouver des informations. Ces centres de sécurité partagent des vidéos et des textes pédagogiques développés par les entreprises en collaboration avec les associations (Milosevic, 2016). Mais l'efficacité de ces centres de sécurité n'a pas été rigoureusement évaluée.

Même avec des fonctionnalités restreintes, les plateformes peuvent encore être mal utilisées (Hinduja, 2016). Par exemple, Snapchat a des règles qui disent prévenir le cyberharcèlement, mais il est possible de prendre une capture d'écran d'une image et de la partager avec d'autres applications mobiles, y compris une application appelée *SnapSave*, qui permet à l'utilisateur de prendre des captures d'écran et des enregistrements anonymes. Davantage de recherches sont également nécessaires dans ce domaine.

LA MODÉRATION « PROACTIVE » DU CONTENU (*PROACTIVE CONTENT MODERATION*)

De nombreuses plateformes ont recours à la modération proactive du contenu avec l'appui des technologies. L'exploration (surveillance) automatique du réseau qui permet de détecter les cas de cyberharcèlement dès qu'ils surviennent, est l'une de ces pratiques (Dinakar, Jones, Havasi, Lieberman, et Picard, 2012 ; Xu, Jun, Zhu, et Bellmore, 2012). Certaines plateformes ont également recours au « filtrage préalable » ou à l'« analyse des sentiments » : lorsqu'une personne publie un mot « déviant » , le système compare le message à une base de données de « mauvais mots ». La plateforme peut alors envoyer à l'utilisateur un message du type « Êtes-vous sûr de vouloir poster ceci ? » , afin de le dissuader de poster des messages qui transgressent les règles communautaires. Ou encore, le système peut vérifier le niveau de gravité du message et soumettre le contenu signalé à un modérateur humain pour un examen plus approfondi (Milosevic, 2016).

La détection et la prévention automatisées du cyberharcèlement constituent une tendance majeure au sein des plateformes et dans la recherche scientifique. Les technologies d'intelligence artificielle — dont l'apprentissage automatique (*machine learning*) et l'apprentissage profond (*deep learning*) — permettent d'identifier les messages potentiellement dangereux avec une précision croissante (Hee et al., 2018 ; Agrawal et Aweka, 2018 ; Al-Garadi et al., 2018). **Cependant, ces technologies peuvent donner lieu à de nombreux faux positifs et une grande partie du contenu qui est valide pourrait être supprimée**, ce qui porterait atteinte à la liberté de parole de l'utilisateur (Milosevic, 2016). D'une manière générale, les solutions d'intelligence artificielle sont obligées de faire des classifications binaires (harcèlement vs. non-harcèlement), ne saisissant pas les nuances des échanges et les modalités plus subtiles qui sont elles-mêmes en constante évolution. De plus, **les solutions d'intelligence artificielle ne peuvent pas fournir le soutien émotionnel ou les conseils d'un engagement humain, ni impliquer les pairs et les témoins d'une manière constructive.**

PRÉVENIR PAR LA PÉDAGOGIE

Une attention croissante est accordée aux pratiques de l'éducation aux médias et à l'information (EMI). L'EMI vise à lutter contre le cyberharcèlement en apprenant aux enfants à réfléchir avant de communiquer en ligne, à utiliser la technologie de manière éthique et responsable, à discerner la nature et la qualité du contenu en ligne, etc. **Quand les enfants comprennent que le cyberharcèlement n'est pas la norme, les taux d'intimidation diminuent** (Barbara, 2010). Plutôt que de supposer que c'est un phénomène commun et inévitable, les enfants devraient comprendre la véritable prévalence du cyberharcèlement. L'ONG canadienne MediaSmarts estime que les enfants doivent comprendre les effets émotionnels du cyberharcèlement pour contrebalancer une culture numérique qui est favorisée par des sentiments d'apathie et des mécanismes de séparation : « *ce qui peut sembler juste une blague peut avoir un effet puissant sur une autre personne* » (*MediaSmarts.ca*).

Les programmes scolaires de lutte contre le cyberharcèlement deviennent de plus en plus répandus, mais ils ont tendance à être inefficaces s'ils tombent dans les clichés et les stéréotypes ou présentent des scénarios irréalistes. Ils sont aussi moins efficaces s'ils sont conçus pour une période limitée, plutôt que pour une longue durée. Selon l'étude « *Young Canadians in a Wired World* » de MediaSmarts, les jeunes considèrent que les programmes de lutte contre le cyberharcèlement qui sont administrés qu'une seule fois (lors des assemblées scolaires par exemple) ont pour effet de banaliser la question. Selon la même étude, les politiques de « *tolérance zéro* » dans les écoles ont rendu les enfants réticents à signaler les cas de cyberharcèlement par crainte des effets sur leurs pairs (Valerie, 2012).

La formation des enseignants est un axe majeur de la stratégie de prévention à l'école, particulièrement importante lorsque les enseignants n'ont pas la même compréhension des outils numériques et des tendances de cyberharcèlement que les élèves. **Les élèves ont souvent l'impression que les enseignants et les adultes ne sont pas conscients du problème ou sont incapables de les aider efficacement, ce qui les décourage de les informer** (Slonje et Smith, 2008 ; Slonje 2012). Byrne montre que les infirmières scolaires sont particulièrement bien placées pour aider les victimes de cyberharcèlement et qu'elles devraient être formées pour réagir (Byrne, 2018).

Slonje et al. se font l'écho des conclusions de l'étude de MediaSmarts, et demandent que les programmes de cyberharcèlement soient intégrés à des politiques scolaires continues et globales.

MÉCANISMES DE RÉACTION (« *COPING MECHANISMS* ») CHEZ LES ENFANTS

Les enfants qui sont victimes de cyberharcèlement développent plusieurs stratégies pour se protéger sur le plan numérique : bloquer les contacts en ligne, changer les noms d'utilisateur ou les adresses électroniques, supprimer des messages sans les lire (Aricak et al., 2008 ; Smith et al., 2008). En fait, **le blocage des messages et des utilisateurs s'avère être l'option préférée des enfants**, bien que certains enfants optent pour des mesures de réaction plus conflictuelles, en répondant directement aux harceleurs (Aricak et al., 2008 ; Smith et al., 2008). **Le désir de réagir peut être plus fort dans le cyberharcèlement que dans le harcèlement traditionnel, incitant la victime à devenir l'agresseur** (Kowalski et Limber, 2007). Il peut être particulièrement important pour le cyber-harceleur de comprendre le résultat de ses actions pour prévenir le comportement cyclique vu que le réflexe de représailles peut être plus fort dans le cyberharcèlement (Kowalski et Limber, 2007 ; Slonje et al., 2012).

Connaître comment les victimes font face au cyberharcèlement et évaluer l'efficacité de leurs stratégies soulève de nombreux défis méthodologiques. Dans une étude réalisée en 2013 sur les enfants tchèques, Machackova et al. examinent les expériences et les réactions des enfants face au cyberharcèlement. Pour avoir une évaluation plus précise de « l'efficacité », ils font la distinction entre les mécanismes de réactions par les victimes du cyberharcèlement sévère et les mécanismes de réactions par les enfants victimes de formes moins graves de harcèlement en ligne. Ils constatent finalement que les stratégies les plus utiles sont :

- les solutions technologiques qui bloquent le contact : supprimer les profils de réseautage social, changer les profils ou les numéros de téléphone, etc. ;
- éviter le site ;
- chercher du soutien.

Et les stratégies les moins utiles sont :

- les actes de représailles ;
- la confrontation ;
- la recherche de conseils en ligne.

Dans l'étude, plus de la moitié des victimes ont choisi de supprimer le cyber-harceleur de leur liste de contacts et ont changé leurs paramètres pour le bloquer. Mais ils ont évité des stratégies plus « radicales » comme changer leur propre nom d'utilisateur ou numéro de téléphone ou supprimer leur profil (Machackova et al., 2013). Il est également intéressant de noter que bien que les solutions technologiques se soient avérées parmi les plus efficaces, **la recherche de conseils en ligne s'est avérée moins efficace.** Les chercheurs pensent que cela peut être lié à la qualité et à l'accessibilité des conseils disponibles en ligne. Malgré la grande variété de ressources en ligne, la méthode de recherche de conseils en ligne peut elle-même poser un problème.

LES RÉPONSES AU CYBERHARCÈLEMENT

La liste ci-après est tirée de *HelpGuide.org*, une organisation à but non lucratif basée aux États-Unis, et de *Ditch the Label*, une organisation caritative britannique. Il s'agit de conseils génériques et non spécifiques au contexte français.

- En général, ne répondez pas. Évitez de réagir par des représailles et d'aggraver la situation.
- Si vous le pouvez, prenez une capture d'écran et gardez un enregistrement sur votre ordinateur.
- Bloquez l'utilisateur-harceleur.
- Signalez l'utilisateur-harceleur. Vous pouvez signaler leurs activités à leur fournisseur de service internet ou à tout réseau social ou autre site Web qu'ils utilisent pour vous cibler. Le cyberharcèlement peut constituer une violation des conditions d'utilisation du site Web ou, selon les lois en vigueur dans votre région, peut même justifier des accusations criminelles.
- Selon le service, vous pouvez augmenter vos paramètres de confidentialité et même restreindre certains utilisateurs. En général, gardez vos paramètres de confidentialité à un niveau élevé et ne vous connectez pas avec des personnes que vous ne connaissez pas.
- Si l'intimidation persiste, vous pouvez changer votre numéro de téléphone ou supprimer votre compte.
- S'il s'agit d'un camarade de classe, signalez le harceleur à un enseignant ou à un personnel de votre école.
- Parlez à quelqu'un pour trouver du soutien, mais aussi pour documenter l'événement.
- Si quelqu'un vous menace, vous donne des renseignements personnels ou vous fait craindre pour votre sécurité, communiquez avec un adulte dès que possible.

MOBILISER LES ENFANTS POUR CONSTRUIRE UNE RÉPONSE EFFICACE

Les programmes de prévention et d'intervention les plus réussis concernent l'implication des enfants eux-mêmes ; ce qui témoigne de l'importance des programmes entre pairs (*peer-programs*), de l'intervention des témoins et de la responsabilisation des enfants de manière générale. Le programme *Cybermentors* a reçu une évaluation très positive par des chercheurs dans ce cadre (Banerjee, Robinson, et Smalley, 2010 ; Thompson et Smith, 2011). Dans ce programme, les jeunes de 11 à 25 ans ont été formés comme « cybermentors » : ils demeurent disponibles à l'école et en ligne grâce à un site Web de soutien par des pairs. Il a été démontré que **le système de pair à pair permettait aux enfants de se sentir à l'aise, tandis que la ressource en ligne permettait d'avoir une distance rassurante et familière**. Entre-temps, des mesures de sécurité ont été intégrées au processus pour permettre de signaler les comportements dangereux, et des conseillers qualifiés ont été rendus disponibles en ligne au besoin (Cross et al., 2009).

Le rôle du pair en tant que témoin est également crucial (Hawkins, Pepler, et Craig, 2001 ; Oh et Hazler, 2009 ; Song, 2017). **Les témoins qui interviennent de façon positive dans le cyberharcèlement ou le harcèlement traditionnel sont souvent appelés des « *upstanders* »** : témoins actifs, qui réagissent en défense ou en soutien de la victime ou signalent l'intimidation (*StopBullying.gov*, *OnlineSense.org*). Il existe de nombreuses initiatives et campagnes qui encouragent les pairs d'être des « *upstanders* » et de fournir diverses formes de soutien. Bien qu'il y ait un consensus général dans la recherche sur le fait que l'intervention positive des témoins atténue le problème du cyberharcèlement, les témoins n'agissent souvent pas lorsqu'ils constatent ce type de situation (Whittaker et Kowalski, 2015). Des recherches supplémentaires sont nécessaires sur la façon d'encourager ces témoins à intervenir de façon positive et sur les méthodes les plus efficaces d'intervention.

Hinduja et Patchin (2017) soulignent l'importance de la résilience des jeunes, bien que souvent négligée dans le débat sur le cyberharcèlement.

À partir d'un échantillon de jeunes américains, les chercheurs ont constaté que les jeunes en capacité de réagir étaient moins susceptibles d'être blessés. La résilience est comprise comme « *la capacité de rebondir, de s'adapter avec succès face à l'adversité et de développer des compétences sociales et académiques malgré l'exposition au stress sévère... ou simplement au stress du monde actuel* » (Henderson et Milstein, 2003), et est un produit de facteurs internes et externes divers (Hinduja et Patchin, 2017). La priorité à accorder à la culture de la résilience dans le développement des jeunes est liée à l'autonomisation numérique ainsi qu'à une approche globale qui les sensibilise aux dimensions techniques et sociales du problème.

RECOMMANDATIONS PAR PARTIE PRENANTE

ÉCOLES

- Les écoles devraient établir et communiquer des politiques et des procédures claires, transparentes et faciles à comprendre, qui précisent la réponse que les écoles apportent aux incidents et qui indiquent les délais de réponse, les contacts désignés et les mécanismes de soutien disponibles pour les victimes ainsi que les harceleurs. Les écoles devraient disposer d'un protocole et d'une cartographie clairs du système pour répondre aux cas de cyberharcèlement.

- Les écoles devraient donner la priorité à la mise en œuvre de programmes globaux et permanents de sensibilisation et de prévention, plutôt qu'à des interventions improvisées (*ad hoc*, ou actions phares).

- Les écoles devraient fournir un soutien et une formation suffisants aux enseignants et aux autres membres du personnel.

- Les écoles devraient mettre en œuvre des politiques et des mécanismes qui encouragent les enfants à signaler plutôt que des politiques telles que la « tolérance zéro » .

- Une attention particulière devrait être accordée aux programmes de pair à pair.

- Les programmes devraient combiner des éléments et supports en ligne et hors ligne. La formation sur le cyberharcèlement peut être dispensée dans le cadre de la formation à l'empathie et à la diversité.

- L'éducation au numérique ne doit pas se restreindre à l'EMI et doit inclure la compréhension d'Internet et du Web dans sa globalité, le fonctionnement des mécanismes des réseaux sociaux (comme les algorithmes, la viralité, les paramètres de confidentialité) et encourager la citoyenneté en ligne.

PLATEFORMES

- De nombreuses plateformes expérimentent de nouvelles fonctionnalités qui prétendent limiter le harcèlement ou assurer la sécurité des victimes, par exemple, l'outil « Restreindre » (*Restrict*) d'Instagram : les commentaires des comptes que vous limitez ne seront pas affichés publiquement sur vos messages (sauf si vous les acceptez), et les utilisateurs limités ne pourront voir quand vous êtes actif ou avez lu leurs messages directs. Ce genre de fonctionnalités supplémentaires est utile pour ceux qui hésitent à signaler ou à bloquer les agresseurs. Les plateformes expérimentent également la suppression des caractéristiques qui favorisent la viralité (le bouton « *Like* » , le nombre de « *followers* » , etc.). La suppression de ces mécanismes peut changer les ergonomies des plateformes qui facilitent l'intimidation en ligne. Il y un travail à faire en matière de « *civic by design* » (inspiré par la logique de « *privacy by design* ») afin d'apporter davantage de fonctionnalités et protections nuancées aux utilisateurs.

- Les entreprises devraient renforcer leurs procédures de signalement et améliorer l'expérience de l'utilisateur afin de le rendre plus réactif et réceptif.

- Les plateformes devraient s'assurer que leurs services sont conformes aux lois sur le harcèlement, la vie privée et la sécurité, et assurer aussi leur fonctionnement efficace.

- La protection de la confidentialité des données est particulièrement préoccupante étant donné la sensibilité des données relatives aux enfants. Les plateformes devraient s'engager sérieusement à protéger les données des enfants. En plus de se conformer au Règlement général sur la protection des données en Europe, cela exige d'expliquer les données et les politiques de confidentialité d'une manière que les enfants comprennent. Cela implique aussi de ne pas partager les données des enfants avec des tiers.

- Les interactions en ligne — bien naturellement rendues anonymes pour préserver la vie privée — peuvent être utiles aux chercheurs qui travaillent sur le sujet. La plupart des recherches se font sur Twitter,

en partie parce qu'il est plus facile pour les chercheurs de « *scrapper* » les données sur Twitter, mais cela signifie que la recherche a moins de visibilité sur les autres plateformes et mécanismes.

- Bien que les politiques officielles des plateformes aient tendance à être écrites sur leurs sites Web, ces politiques n'expliquent pas toujours comment fonctionnent les mécanismes contre le cyberharcèlement. Les plateformes devraient rendre leurs algorithmes transparents pour permettre à la communauté des chercheurs de les examiner et de suggérer des améliorations, mais aussi pour permettre au grand public de comprendre les mécanismes de médiation de leurs échanges en ligne. Bien entendu, la transparence n'est pas une fin en soi, mais plutôt une étape nécessaire pour comprendre quelles solutions sont efficaces du point de vue des jeunes utilisateurs.

FAMILLES

- Les familles ont un rôle essentiel à jouer dans toute stratégie efficace de lutte contre le cyberharcèlement. Il a été constaté dans la recherche que leur participation engendre une réduction de l'intimidation et de la victimisation.

- Les familles devraient comprendre les modalités des paramètres de confidentialité et les profils des comptes. Ils devraient connaître les meilleurs moyens de limiter le nombre de personnes qui peuvent rechercher et contacter leur enfant, ainsi que les informations que d'autres peuvent obtenir sur lui.

- Les familles devraient connaître les mécanismes de signalement à leur disposition et prendre des mesures au besoin. Elles peuvent signaler les incidents de cyberharcèlement à l'école, aux autorités locales, aux sites de réseaux sociaux et à leur fournisseur d'accès à Internet (FAI).

- Les familles devraient discuter avec leur enfant de ce qui constitue un contenu approprié et inapproprié à partager en ligne et de ce qui constitue un comportement en ligne approprié et inapproprié sur les réseaux sociaux. Les enfants pensent souvent qu'ils devraient avoir le droit à la vie privée sur des réseaux sociaux, mais il y a une responsabilité d'accompagnement des familles, sans être intrusives. Les familles et les enfants devraient s'entendre sur ce que les parents peuvent savoir sur les interactions en ligne de leur enfant.

- Les familles doivent être attentives aux symptômes de cyberharcèlement — décrits ici par le Centre de recherche sur le cyberharcèlement *Cyberbullying.org.*

- Les familles doivent porter un regard critique sur les ressources et conseils qu'elles trouvent en ligne, étant donné que ces derniers ne sont pas toujours rigoureusement évalués et qu'ils peuvent être liés à la vente d'un produit commercial.

AUTORITÉS PUBLIQUES

- Le soutien aux familles devrait être une priorité. Il s'agit notamment de s'assurer que la formation à destination des familles soit disponible et accessible, et d'élaborer des ressources pour les familles avec des enfants vulnérables ou ayant des besoins particuliers.

- Faire participer les enfants à l'élaboration des politiques et des pratiques. Cela peut se faire en partie en allouant des subventions aux organisations de jeunesse pour permettre aux jeunes de développer et entreprendre des initiatives de lutte contre le cyberharcèlement.

- Financer la recherche pour mesurer la prévalence et l'impact du cyberharcèlement à l'échelle nationale sur une base annuelle. Cela devrait se faire en collaboration avec les plateformes et la société civile.

- Sensibiliser le public au cadre juridique existant en matière de cyberharcèlement.

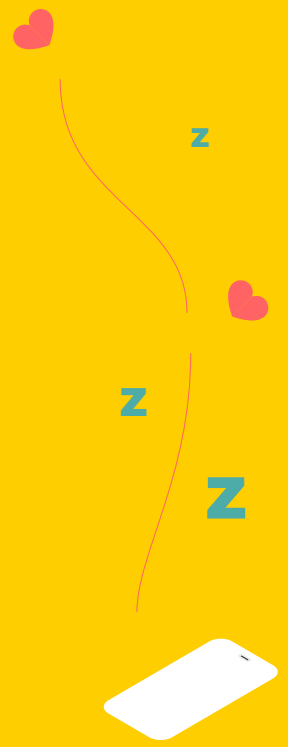
SOCIÉTÉ CIVILE, RECHERCHE

- Il est nécessaire de mener des recherches impartiales et robustes sur les modalités et les effets du cyberharcèlement, ainsi que sur l'efficacité des stratégies de prévention et d'intervention.
- **Les chercheurs ne devraient pas limiter leur analyse du cyberharcèlement à quelques plateformes, mais étudier l'écosystème en ligne de manière globale et être attentifs à des phénomènes de migration entre supports et au harcèlement multi-support.**
- **Davantage de recherches devraient être menées sur le phénomène de témoins « actifs » afin de mieux comprendre leurs motivations, l'efficacité de leurs actions et les moyens d'encourager cette démarche.**
- La majorité des études reste dans le cadre scolaire mais vu que le cyberharcèlement ne se limite pas à la journée scolaire, d'autres recherches sont nécessaires hors du milieu scolaire.
- La société civile devrait décortiquer le concept de l'EMI en tant que réponse « fourre-tout » aux problèmes en ligne.

ENFANTS

- En tant que pairs et camarades de classe, les enfants sont particulièrement bien placés pour être des témoins « actifs » en classe et même en ligne. Les enfants devraient signaler de manière appropriée les cas de cyberharcèlement lorsqu'ils sont victimes ou témoins. Des programmes et des mécanismes de formation sont essentiels à cet égard.
- Les enfants devraient développer des comportements en ligne sûrs et bien réfléchis, ce que certains appellent « l'hygiène numérique » (*digital hygiène*) : utiliser des paramètres de confidentialité, ne pas partager des informations sensibles, etc.
- **Il faut éviter de banaliser l'idée que lorsqu'ils vont en ligne ils doivent automatiquement compromettre leur vie privée et leur sécurité et plutôt questionner la normalité de ces mécanismes.**

ANNEXES



PRATIQUES INSPIRANTES

Stop Bullying (États-Unis) : https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

- *StopBullying.gov* fournit de l'information provenant de divers organismes gouvernementaux sur ce qu'est le harcèlement, le cyberharcèlement, qui est à risque et comment vous pouvez prévenir et réagir au harcèlement. Le contenu est fourni par les partenaires du comité de rédaction, qui travaille en collaboration avec le ministère de l'Éducation et le ministère de la Santé et des Services sociaux.

ADL CyberAlly Workshops (États-Unis) : https://www.adl.org/education/resources/tools-and-strategies/bullying-and-cyberbullying-workshops

- L'Anti-Defamation League (ADL) est une ONG traditionnellement axée sur l'antisémitisme. Elle offre des formations et des ressources pour lutter contre les préjugés et propose des programmes sur le harcèlement et le cyberharcèlement dans les écoles. ADL offre une gamme d'ateliers interactifs pour les écoles primaires, intermédiaires et secondaires.

Cyberbullying Research Center (États-Unis) : https://cyberbullying.org/

- Le Cyberbullying Resource Center est dirigé par les Dr Sameer Hinduja (Florida Atlantic University) et Dr Justin W. Patchin (University of Wisconsin-Eau Claire). Il sert de centre d'échange d'information sur la façon dont les adolescents utilisent et abusent de la technologie. Il comprend des études, des témoignages et de nombreuses ressources destinées aux parents, aux enseignants, aux psychologues, aux agents de police, et aux jeunes eux-mêmes.

Queensland Anti-Cyberbullying Taskforce (Australie) : https://campaigns.premiers.qld.gov.au/antibullying/taskforce/assets/anti-cyberbullying-taskforce-final-report.pdf

- La Queensland Anti-Cyberbullying Taskforce a été créée en février 2018 afin d'élaborer un cadre pour lutter contre le cyberharcèlement des enfants et des jeunes du Queensland et recommander des mesures communautaires et gouvernementales. Leur rapport final contient l'approche communautaire (« *Community Approach* ») de la *taskforce*, y compris les mesures recommandées aux gouvernements, aux parents, aux éducateurs, aux enfants et jeunes, aux écoles, aux entreprises de réseaux sociaux, aux organisations sportives et communautaires et aux universités.

KiVa (Finlande) : http://www.kivaprogram.net/

- Le programme KiVa, développé en Finlande, est un programme scolaire universel qui s'attaque au cyberharcèlement à l'école en travaillant avec les enseignants, les parents, les familles, les dirigeants communautaires et les élèves. Il comprend la formation des enseignants, des cours et des environnements d'apprentissage virtuels. Les enseignants utilisent un manuel pour l'enseignement en classe, qui est complété par un jeu informatique anti-harcèlement pour les élèves du primaire et un forum internet pour les élèves du secondaire. Bien qu'il ne soit pas spécifiquement axé sur le cyberharcèlement, ce programme s'est révélé aussi efficace pour réduire le cyberharcèlement que le harcèlement traditionnelle (Salmivalli, Kärna, et Poskiparta, 2011).

POUR ALLER PLUS LOIN

- Blaya, Catherine, (2019). Cyberhaine. Les jeunes et la violence sur Internet. Nouveau Monde éditions. ISBN 978-2-36942-770-4

- The Anti-Defamation League Center for Technology & Society, (2019). The Trolls are Organized and Everyone's a Target: The Effects of Online Hate and Harassment.

- M. A. Al-Garadi et al., (2019). Predicting Cyberbullying on Social Media in

the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. IEEE Access, vol. 7, pp. 70701-70718, 2019 doi: 10.1109/ACCESS.2019.2918354

- Patchin, J.W. & Hinduja, S.,(2019). The Nature and Extent of Sexting Among a National Sample of Middle and High School Students in the U.S. Archives of Sexual Behavior 48: 2333. https://doi.org/10.1007/s10508-019-1449-y

- Blaya, Catherine, (2018). Le cyberharcèlement chez les jeunes. Enfance, 3(3), 421-439. doi:10.3917/enf2.183.0421.

- Van Hee C, Jacobs G, Emmery C, Desmet B, Lefever E, Verhoeven B, et al., (2018). Automatic detection of cyberbullying in social media text. PLoS ONE 13(10): e0203794. https://doi.org/10.1371/journal.pone.0203794

- Byrne E, Vessey JA, Pfeifer L., (2018). Cyberbullying and Social Media: Information and Interventions for School Nurses Working With Victims, Students, and Families. J Sch Nurs. 2018 Feb;34(1):38-50. doi: 10.1177/1059840517740191.

- Agrawal S., Awekar A., (2018). Deep Learning for Detecting Cyberbullying Across Multiple Social Media Platforms. In: Pasi G., Piwowarski B., Azzopardi L., Hanbury A. (eds) Advances in Information Retrieval. ECIR 2018. Lecture Notes in Computer Science, vol 10772. Springer

- Karissa Leduc et al., (2018). The influence of participant role, gender, and age in elementary and high-school children's moral justifications of cyberbullying behaviors, Computers in Human Behavior (2018). DOI: 10.1016/j.chb.2018.01.044

- Hinduja, Sameer & Patchin, Justin, (2017). Cultivating youth resilience to prevent bullying and cyberbullying victimization. Child abuse & neglect. 73. 51-62. 10.1016/j.chiabu.2017.09.010.

- Song, Jiyeon & Oh, Insoo, (2017). Factors Influencing Bystanders' Behavioral Reactions in Cyberbullying Situations. Computers in Human Behavior. 78. 10.1016/j.chb.2017.10.008.

- Ditch the Label, (2017). The Annual Bullying Survey 2017. https://www.ditchthelabel.org/

- Blaya, Catherine et al., (2016). Stop aux appels à la haine sur Internet ! (SAHI) Recherche-Action sur les incitations à la haine dans le cyberespace chez les jeunes âgés entre 11 et 18 ans CNRS

- Betts, Lucy & Spenser, Karin, (2016). People think it's a harmless joke: young people's understanding of the impact of technology, digital vulnerability and cyberbullying in the United Kingdom. Journal of Children and Media. 11. 1-16. 10.1080/17482798.2016.1233893.

- Milosevic, T., (2016). Social Media Companies' Cyberbullying Policies. International Journal Of Communication, 10, 22. Retrieved from https://ijoc.org/index.php/ijoc/article/view/5320/1818

- European Parliament Committee on Civil Liberties, Justice, and Home Affairs, (2016). Directorate-General for Internal Policies Policy Department, Citizens Rights and Constitutional Affairs, Cyberbullying Among Young People. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

- The Anti-Defamation League, (2016). Responding to Cyberhate, Progress and Trends https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/2016-ADL-Responding-to-Cyberhate-Progress-and-Trends-Report.pdf

- Whittaker, Elizabeth & Robin M. Kowalski, (2015). Cyberbullying Via Social Media, Journal of School Violence, 14:1, 11-29, DOI: 10.1080/15388220.2014.949377

- Näsi, Matti & Räsänen, Pekka & Hawdon, James & Holkeri, Emma & Oksanen, Atte, (2015). Exposure to online hate material and social trust among Finnish youth. Information Technology &amp People. 28. 607-622. 10.1108/ITP-09-2014-0198.

- Kubiszewski, Violaine & Fontaine, Roger & Potard, Catherine & Auzoult, Laurent, (2015). Does cyberbullying overlap with school bullying when taking modality of involvement into account?. Computers in Human Behavior. 2015. 49-57. 10.1016/j.chb.2014.10.049.

- Rice, E., Petering, R., Rhoades, H., Winetrobe, H., Goldbach, J., Plant, A., ... Kordic, T., (2015). Cyberbullying perpetration and victimization among middle-school students. American journal of public health, 105(3), e66–e72. doi:10.2105/AJPH.2014.302393

- Machackova, H., Cerna, A., Sevcikova, A., Dedkova, L., & Daneback, K., (2013). Effectiveness of coping strategies for victims of cyberbullying. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7(3), article 5. http://dx.doi.org/10.5817/CP2013-3-5

- Tomsa, Raluca & Jenaro, Cristina & Campbell, Marilyn & Neacsu, Denisa, (2013). Student's Experiences with Traditional Bullying and Cyberbullying: Findings from a Romanian Sample. Psiworld 2012. 78. 586-590. 10.1016/j.sbspro.2013.04.356.

- Blaya, Catherine, (2013). Les ados dans le cyberespace : Prises de risque et cyberviolence. Pédagogies en développement. 9782804175948

- Blaya, Catherine & Seraphin Alava, (2012). Risques et sécurité des enfants sur Internet : rapport pour la France. ffhal-00978590f

- Kowalski, Robin & Limber, Susan & Agatston, Patricia, (2012). Cyber Bullying: Bullying in the Digital Age. American Journal of Psychiatry - AMER J PSYCHIAT. 165. 10.1002/9780470694176.

- Slonje, R., et al.,(2012). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior dx.doi.org/10.1016/j.chb.2012.05.024

- Salmivalli, Christina & Kärnä, Antti & Poskiparta, Elisa, (2011). Counteracting bullying in Finland: The KiVa program and its effect on different forms of being bullied. International Journal of Behavioral Development - INT J BEHAV DEV. 35. 405-411. 10.1177/0165025411407457.

- Jäger, T., Amado, J., Matos, A., & Pessoa, T., (2010). Analysis of Experts' and Trainers' Views on Cyberbullying. Australian Journal of Guidance and Counselling, 20(2), 169-181. doi:10.1375/ajgc.20.2.169

- Livingstone, Sonia and Haddon, Leslie, (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp.1-6.

DIRECTION DE LA PUBLICATION

Jennyfer Chrétien, Déléguée générale de Renaissance Numérique

RÉDACTRICE

Claire Pershan, Chargée de mission de Renaissance Numérique

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Décembre 2019