Cyberviolence chez les jeunes
Les défis de la Cyberintimidation

PRINTEMPS NUMÉRIQUE

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :
Québec

Montréal, février 2025
ISBN : 978-2-9816413-7-3
Dépôt légal – Bibliothèque et archives nationales du Québec

Rapport réalisé dans le cadre du Programme de soutien financier ***Ensemble contre l'intimidation*** du ministère de la Famille du Québec (MFA)

- Responsable de la recherche et de la rédaction : Dre Amina Yagoubi, Sociologue Ph.D, AKY-Conseils.
- Production et édition : Printemps numérique.

Le présent rapport complète le projet du « Référentiel de compétences de prévention de la cyberintimidation chez les jeunes » (2022-2025).

Citer le document : Yagoubi, A. (2025) *Cyberviolence chez les jeunes : Les défis de la Cyberintimidation* - Printemps numérique, p. 1-128

TABLE DES MATIÈRES

REMERCIEMENTS

C’est avec un profond engagement envers le bien-être de la jeunesse que le **Printemps numérique** répond à l’appel du **ministère de la Famille du Québec** (MFA) afin de réaliser le projet intitulé: **« *Référentiel de compétences de prévention de la cyberintimidation chez les jeunes* »** (2022-2025). Ce projet, initié dans le cadre de l’appel à projets 2022-2023 du Programme de soutien financier ***Ensemble contre l’intimidation*** du ministère de la Famille du Québec, a bénéficié de l’engagement remarquable de nombreuses personnes et organisations.

En premier lieu, nos remerciements s’adressent au ministère de la Famille du Québec, dont l’initiative *Ensemble contre l’intimidation* met en avant une vision responsable afin de prévenir et contrer la cyberintimidation chez les jeunes au Québec. Le soutien du MFQ est essentiel pour mener à bien notre mission de prévention de la cyberintimidation chez les jeunes. Dans un contexte où les frontières entre le réel et le virtuel deviennent floues et où les jeunes sont de plus en plus exposés aux menaces en ligne, notre projet a pour objectif de sensibiliser, mais aussi d’outiller des intervenants travaillant auprès de jeunes au Québec.

Nous tenons également à remercier l’engagement de la **Table de concertation intersectorielle et interrégionale sur la littératie numérique** à ce projet, une initiative déployée par le Printemps numérique et qui regroupe plus de 300 membres issus de 145 organisations. Il sera un partenaire clé dans la diffusion du « Référentiel de compétences de prévention de la cyberintimidation chez les jeunes », renforçant ainsi la portée du projet.

Les remerciements s’adressent également à tous les collaborateurs au projet, notamment les experts du Québec qui ont participé aux groupes de discussion, aux séances de

co-création du référentiel. Leurs connaissances et engagements ont été indispensables dans l'élaboration de l'outil à visée éducative.

Nous remercions également les jeunes de 15 à 29 ans qui ont partagé leurs expériences et opinions lors des événements organisés par le Printemps numérique ou par nos partenaires. Leurs témoignages ont enrichi notre compréhension du phénomène social de la cyberintimidation.

La première phase du projet repose sur la réalisation d'une revue de littérature permettant de mieux comprendre la cyberintimidation chez les jeunes. La revue de littérature expose des données statistiques, détaille les formes et actes de cyberviolence, et présente de bonnes pratiques telles que des initiatives internationales luttant contre les violences en ligne, etc.

Par la suite, la deuxième phase du projet repose sur une approche participative avec des experts pour élaborer le « Référentiel de compétences de prévention de la cyberintimidation chez les jeunes ». En recourant à des méthodes collaboratives et de co-création (discussion de groupes, séances de co-création inspirée du design thinking et d'ateliers inspirés de la méthode Dacum), nous proposerons un outil à visée éducative visant un impact positif sur les jeunes.

Le rayonnement de nos activités et événements nous permettra d'atteindre divers publics, des organismes aux écoles, du milieu de la recherche à une audience nationale et internationale. La diffusion du référentiel sur le site du **Printemps numérique**[1] et sur la plateforme du **Mois Numérique Jeunesse**[2], lors de l'événement jeunesse annuel, contribuera à toucher un public plus vaste intéressé par les problématiques de cyberviolences et cyberintimidation chez les jeunes.

[1] Printemps numérique : https://www.printempsnumerique.ca
[2] Mois Numérique Jeunesse : https://mnj.quebec

Pour finir, les résultats du projet seront présentés à l'événement phare du Printemps numérique, soit **MTL connecte : la Semaine numérique de Montréal**[3], cet événement mobilise une clientèle régionale, nationale et internationale.

En répondant au Programme de soutien financier ***Ensemble contre l'intimidation*** du ministère de la Famille, le Printemps numérique s'engage à poursuivre ses actions et recherches en faveur de la jeunesse québécoise. En effet, Printemps numérique et ses partenaires sont engagés depuis 2018 dans des actions, initiatives et recherches sur les jeunes et l'impact sociétal du numérique dans le cadre de notre **Projet Jeunesse QC 2030**. Plusieurs actions ont été déployées à Montréal et dans plusieurs régions du Québec[4] ainsi qu'auprès de **communautés autochtones** (**Motion Cafés numériques - Assemblée nationale du Québec**[5] et **Tournée des Cafés numériques dans les communautés Atikamekw**[6]).

Enfin, nous soulignons le travail exceptionnel de notre collaboratrice, la Docteure sociologue Amina Yagoubi Ph.D., responsable de la recherche du Projet Jeunesse QC 2030 et du présent projet portant sur la cyberintimidation. Son expertise et ses contributions significatives ont grandement contribué à enrichir les activités de recherche, de la revue de littérature au transfert de connaissances.

Notre initiative citoyenne s'inscrit dans la continuité responsable des actions du Printemps numérique, affirmant notre engagement envers la jeunesse québécoise et notre contribution à un environnement numérique inclusif, éthique et sécuritaire.

Mehdi Benboubakeur
Directeur général du Printemps numérique

---

[3] La Semaine numérique de Montréal : https://mtlconnecte.ca
[4] Tournée provinciale des Cafés numériques (2018) : https://youtu.be/8mm_jruZ11E)
[5] Motion Cafés numériques - Assemblée nationale du Québec (7 nov. 2019) : https://www.youtube.com/watch?v=X_XBRhRacjo
[6] Cafés numériques dans les communautés Atikamekw - Obedjiwan, Wemotaci Manawan (29 nov. 2019) : https://www.youtube.com/watch?v=hrJf8aGcwiU

SOMMAIRE EXÉCUTIF

Dans le cadre de la première phase du projet **« *Référentiel de compétences de prévention de la cyberintimidation chez les jeunes* »** (2022-2025), nous avons réalisé une revue de littérature afin de mieux comprendre le phénomène complexe de la cyberintimidation, en mettant particulièrement l'accent sur ses impacts sur la jeunesse. Les lecteurs ciblés, tels que les organismes travaillant avec les jeunes, les éducateurs et les ministères, trouveront dans ce rapport une synthèse des connaissances explorant les divers aspects de la cyberintimidation, de ses manifestations et ses impacts, mais aussi des exemples d'initiatives préventives et des recommandations permettant de contrer la cyberviolence en général.

La cyberintimidation, définie comme l'utilisation des technologies pour commettre des actes haineux et intimider autrui, représente un défi sociétal majeur à l'ère numérique (Descurninges, 2022). En examinant divers travaux de recherche et rapports gouvernementaux, notre rapport propose une analyse détaillée des facteurs de risques, des stratégies de prévention, en tenant compte des nouvelles formes de cyberviolence, notamment la cyberintimidation.

Au Québec, la cyberintimidation touche 57% des jeunes de 10 à 18 ans, un chiffre inquiétant qui met l'accent sur l'urgence d'agir (Descurninges, 2022). Plus préoccupant encore est le faible pourcentage de jeunes (22%) qui vont solliciter l'aide de leur entourage, ce qui révèle malheureusement des manques dans la sensibilisation et la prévention de la cyberintimidation (Descurninges, 2022). De plus, la pandémie, en favorisant l'accroissement du temps passé devant les écrans, a quant à elle participer à exacerber ce fléau numérique (Gervais et Fortier, 2021).

Les conséquences négatives de la cyberintimidation sur la santé mentale des jeunes, par exemple la « dépression », l'« isolement social » et les idées suicidaires, sont particulièrement inquiétantes (INSPQ, 2023; Schimele et *al.*, 2021; SCF, 2016; John et *al.*, 2018; Family Lives, 2021). Pour relever ces défis, il est essentiel de mobiliser et d'impliquer collectivement les parents, les établissements scolaires, les professionnels et les acteurs gouvernementaux.

Les divers comportements de cyberintimidation, allant du « *Text bullying* » au « *Sexting* », du « *Revenge Porn* » au « *Self Harm* », du « *Doxing* » aux « Deepfakes » ou encore au « *Trolling* », partagent la même intention de répandre la peur, propager des messages haineux et partager des informations compromettantes (Smith et *al.*, 2020). Il nous faut mieux comprendre la diversité de tels comportements et de ces menaces numériques afin de mieux les désamorcer.

L'examen des initiatives mondiales de lutte contre la cyberintimidation met en avant l'importance d'une approche multiscalaire (à plusieurs échelles), qui impliquerait à différents niveaux les parents, les établissements scolaires, les organismes et les autorités publiques. De telles initiatives ont généralement pour objectif d'éduquer les jeunes au bon usage du numérique et de leur apprendre à se protéger contre les diverses formes de cyberviolence. Des exemples de programmes tels qu'*Internet sans crainte*, *ReThink Summit School Program*, *School Wellbeing Framework*, *Cyber Friendly Schools* et le *ViSc Social Competence Program* ont d'ailleurs fait leurs preuves dans plusieurs pays (Internet sans crainte, 2021; ReThink Summit School Program, 2022; School Wellbeing Framework, 2020; Cyber Friendly Schools, 2019; ViSc Social Competence Program, 2018).

Les établissements scolaires sont encouragés à mettre en place de tels programmes préventifs afin de sensibiliser les jeunes aux risques du monde numérique et favoriser un environnement éducatif responsable, éthique et sécurisé (Gouvernement du Québec,

2021). Les parents jouent un rôle important en facilitant des conversations ouvertes avec leurs enfants sur des sujets tels que la cyberviolence, la cyberintimidation, etc., en régulant l'utilisation des réseaux sociaux numériques (RSN), ils peuvent aussi avoir recours par exemple à des solutions technologiques telles que le contrôle parental (McAfee, 2022; Hue, 2023; Zhu et *al.*, 2021).

Des études soulignent que des interactions positives entre les jeunes et leurs parents, ainsi que la perception du soutien parental par les jeunes, sont des facteurs positifs qui contribuent à réduire les risques de cyberintimidation (Gervais et Fortier, 2021; Hue, 2023; Zhu et *al.*, 2021). Une telle connexion familiale participe à renforcer la résilience des jeunes face aux défis du numérique.

L'implication des décideurs publics est également essentielle pour recommander l'établissement de lois et renforcer la sécurité de l'environnement numérique. La France, entre autres, a adopté des lois pour « sécuriser et réguler l'espace numérique » (Hue, 2023). Au Québec, il serait également recommandé de mettre en place un programme spécifique pour lutter contre la propagation de la haine en ligne, ainsi que de la falsification et la manipulation des informations. Bien que le Code criminel canadien sanctionne certaines formes de cyberintimidation, l'adoption d'une loi québécoise spécifique à la sécurité numérique renforcerait la protection en ligne pour lutter contre la cyberviolence (Gendarmerie royale du Canada, 2022; Code criminel, 1985). En s'inspirant d'initiatives inspirantes telles que l'application britannique *BullStop* ou encore *Respect Zone* en France, les gouvernements, y compris celui du Québec, sont encouragés à adopter des stratégies de régulation du cyberespace pour augmenter la protection numérique des jeunes (BullStop, 2019; Respect Zone, 2020).

En guise de conclusion, notre revue de littérature propose une meilleure compréhension de la cyberintimidation et de la violence en ligne, elle met en lumière ses impacts non seulement sur la jeunesse mais aussi sur l'ensemble de la société. Devant les défis

sociaux du numérique, il est recommandé d'adopter une approche holistique, intégrant la sensibilisation, la prévention et l'adoption de mesures législatives. Pour établir un environnement numérique plus sûr et équilibré, les acteurs institutionnels et de la société civile sont alors appelés à jouer un rôle pivot dans la protection des jeunes contre des comportements numériques nocifs. À une époque où les technologies numériques et l'intelligence artificielle (IA) se répandent de plus en plus et ce, dans toutes les sphères de la société, il est essentiel d'énoncer collectivement un contrat social responsable encadrant nos usages du numérique touchant aussi bien l'éducation que le travail, la sphère politique et d'autres domaines.

Acronymes

BDM : Blog du modérateur
CEST : Commission de l'éthique de la science et de la technologie
CFS : *Cyber Friendly Schools*
CSF : Conseil du statut de la femme
CSS : Centre de services scolaires
***DOP** : Departement of education*
EDI : Équité, diversité et inclusion
EMCDDA : *European Monitoring Center for Drugs and Drug Addiction*
EN : Espace numérique
GRC : Gendarmerie du Canada
IA : Intelligence artificielle
INSPQ : Institut national de santé publique du Québec
ISQ : Institut de la statique du Québec
MFA : Ministère de la Famille
MEES: Ministère de l'Éducation et de l'Enseignement supérieur
MENESR : Ministère de l'Éducation Nationale, de l'Enseignement supérieur et de la Recherche
MENJ : Ministère de l'Éducation Nationale et de la Jeunesse (France)
MSP : Ministère de la Sécurité publique
OCDE : Organisation de coopération et de développement économiques
PALVI : Plan d'action de lutte contre l'intimidation et la violence
PAN : Plan d'action numérique
RSN : Réseaux sociaux numériques
SPVM: Service de Police de la ville de Montréal
SREN : Sécuriser et réguler l'espace numérique
UE : Union Européenne
UNICEF : *United Nations International Children's Emergency Fund*| Fonds des Nations Unies pour l'enfance
ViSC : *Viennese Social Competence*

Index

Cyberfilature (Cyberstalking)
Cyberharcèlement (Harcèlement en ligne) ; Cyberharceleur/ Cyberharcelé
Cyberinterdépendance
Cyberintimidation (Cyberbulling) ; Cyberintimidateur/ Cyberintimidé
Cybermalveillant
Cybermenaces
Cybermonde
Cyberphénomène
Cybersécurité
Cybersexisme
Cybervictimisation ; Cybervictime
Cyberviolence

D

Deepfake (Technologie d'hyper-trucage)
Dénigrement ou *Denigration*
Désinformation
Divulgation (Divulguer des informations)
Données personnelles
Doxing

E

Écran (numérique)
Espace numérique
Exclusion ou *Ostracism*

F

Facebook
Faux (nom ; profil)
Film (filmer)
Flingue ou *Flaming*
Forum (en ligne)
Fraude (frauduleux)

G

Game (Gameuse, Gameur)
Groupe (en ligne, - de discussion)

H

Hacker
Hameçonnage
Harcèlement en ligne (Cyberharcèlement)
Hygiène numérique

I

Identité numérique
Image
Incitation au dévoilement (Outing and Trickery)
Information
Instagram
Internaute
Internet
Internet sécuritaire (*safer Internet*)

J

Jeux en ligne
Jeux vidéo

L

Like (liker)
Littératie numérique
Logiciel (de contrôle parental ; espion…)

M

Média social (médias sociaux)
Message (texte)
Messagerie instantanée
Mot de passe
Myspace

N

Navigation (privée)
Nudes

O

Ordinateur
Ostracism (Exclusion numérique)
Outil électronique
Outil multimédia
Incitation au dévoilement (Outing and Trickery)

P

Page
Partage en ligne (Shareting)
Partager (Share ; - une image ; une publication...)
Perpétration (en ligne)
Photo numérique
Photomontage
Piratage (Pirater)
Pirate
Plateforme
Poster (Post ; - un message)
Profil
Publication (média social)

R

Renseignement (personnel, financier...)
Réseaux sociaux numériques (RSN)
Revenge Porn

S

Salon (Clavarder, clavardage)
Sécurité numérique
Self-Harm
Sexting (Sextage)
Partage en ligne)
Site cybermalveillant
Slutshaming
Smartphone (cellulaire ; téléphone portable, mobile)
SMS (message)
Snapchat
Solliciter (sollicitation)
Système informatique

T

Tablette
Technologie d’hyper-trucage (Deepfake)
Technologies numériques
Téléphone portable, mobile (cellulaire, smartphone)
Temps d’écran
Text bullying
TikTok
Traces numériques
Transfert (- d’une image, …)
Trolling
Twitch
Twitter

U

Usager
Usurpation (Usuper)

V

Vidéo
Vidéolynchage (*Happy Slapping,* vidéo agression)
Vie privée
Viral
Virus
Vol d’identité ou *Impersonation*
Vulnérabilité numérique (technologique)

W

Web
WhatsApp
Wifi

INTRODUCTION

> « *Quelqu'un a mis une vieille photo de classe sur Internet et l'a envoyée à toute la classe. Tout le monde se moque de moi et fait des plaisanteries à cause de mon appareil dentaire* » (MENJ, 2011 :7)

Dans le contexte actuel d'un développement rapide des technologies disruptives accompagné par une « démocratisation d'Internet » (Li, 2020), nous assistons à l'avènement irréversible de la société numérique. Alors qu'une telle évolution technologique annonce des avancées prodigieuses, elle expose également à l'augmentation de risques. Les jeunes se trouvent ainsi être les « premiers habitants » du « cybermonde » (Alava, 2018), confrontés à divers « cyberphénomènes sociaux » (Niang et Nagem, 2018) qui ont le pouvoir de menacer leur intégrité et leur bien-être. C'est pourquoi il importe aujourd'hui, d'engager une réflexion collective portant sur la régulation sociétale du monde numérique, dans le but de prévenir les dérives potentielles du numérique pour les générations présentes et futures.

Selon le rapport de *We are social* (2023) portant sur les tendances du Web et des médias sociaux, une croissance exponentielle du nombre d'utilisateurs d'Internet et des réseaux sociaux numériques (RSN) est enregistrée. En effet, c'est

> [En effet, c'est plus] de 5,18 milliards d'individus (qui) utilisent aujourd'hui Internet, soit 64,6 % de la population mondiale. Le nombre mondial d'utilisateurs actifs des médias sociaux a atteint 4,80 milliards en avril 2023. Ce chiffre peut ne pas représenter des individus uniques, car les données que nous utilisons pour établir ce total comprennent inévitablement un certain degré de duplication et de « faux » comptes. Toutefois, pour faciliter la comparaison, ce total se rapproche dangereusement de 60 % de la population mondiale (*We are social,* 2023).

Parmi les différentes plateformes de RSN, Facebook est la plus fréquentée avec plus de trois milliards d'utilisateurs. YouTube occupe la deuxième position « avec plus de 2,5 milliards » d'utilisateurs, tandis qu'Instagram et WhatsApp se situent au même niveau « avec 2 milliards d'utilisateurs » chacun (BDM, 2023). TikTok et Snapchat connaissent également une progression significative. En l'espace de six mois, TikTok est passé « de 945 millions [...] à environ 1,1 milliard » en termes « d'utilisateurs actifs » (BDM, 2023), et le temps passé sur TikTok a considérablement augmenté, avec une moyenne mensuelle de 31,5 heures par internaute (BDM, 2023).

Snapchat a connu une augmentation de 25% en seulement 10 mois, comptant désormais « 383 millions d'utilisateurs quotidiens, soit une augmentation de 8 millions par rapport au trimestre précédent » (BDM, 2023). De son côté, Instagram demeure « le réseau social préféré des jeunes âgés de 16 à 24 ans » (BDM, 2023).

La densité du trafic sur les RSN ainsi que sur le Web contribue à augmenter le nombre d'échanges qui favorise malheureusement l'émergence de comportements cyber-agressifs (Gouvernement du Québec, 2023). De plus en plus de jeunes témoignent d'une nouvelle « vulnérabilité numérique » (Yagoubi, 2020), résultant d'une utilisation inappropriée d'Internet par des individus ou des groupes, qui se livrent par exemple à l'intimidation ou au harcèlement en ligne (Hackett, 2016). C'est pourquoi, la société civile et les politiques doivent réfléchir à la mise en place de réglementations régulant l'usage du cyberespace afin de garantir la protection de la vie privée, des données personnelles et le respect des individus. Les internautes, en particulier les jeunes, doivent pouvoir, en effet, naviguer en toute sécurité (Hackett, 2016).

Malheureusement, la réalité rapporte de plus en plus de cas de cyberviolence, de cyberintimidation, etc., et de nombreux pays membres de l'Organisation de coopération et de développement économiques (OCDE) sont confrontés aux défis de protéger leurs

jeunes (enfants et adolescents) particulièrement vulnérables, et donc plus susceptibles d'être victimes des violences en ligne (Gottschalk, 2022).

Contexte pandémique

Lors de la pandémie du Covid-19, l'utilisation croissante du numérique a exacerbé une augmentation significative des « cyber-incidents » et de la « détresse psychologique » (Gervais et Fortier, 2021). En raison de l'augmentation du temps passé devant les écrans, les établissements scolaires observent une hausse des menaces de suicide en ligne, ainsi qu'une « recrudescence » des comportements problématiques tels que « les insultes et les menaces virtuelles » (Gervais et Fortier, 2021). Marc Farand, un « agent de prévention et aux relations communautaires au service de police de Granby », a rapporté une augmentation des disputes entre les jeunes sur les réseaux sociaux depuis 2020 (Gervais et Fortier, 2021).

Cathy Tétreault, une experte en cyberinterdépendance et directrice générale du Centre Cyber-aide, a constaté une augmentation des cas de cyberintimidation au niveau primaire par rapport au niveau secondaire. Elle indique que de nombreuses écoles sollicitent son intervention pour résoudre « des crises liées à l'intimidation en ligne » (Gervais et Fortier, 2021). Ce phénomène s'est renforcé pendant la pandémie, car les jeunes qui avaient l'habitude de socialiser à l'école se sont tournés vers les réseaux sociaux pour maintenir leurs interactions, et souvent sans la supervision d'un adulte (Gervais et Fortier, 2021).

L'experte souligne qu'au niveau de l'école secondaire, lors des cours en ligne, il arrive que certains élèves prennent des photos d'autres élèves ou d'enseignants sans leur consentement, ce qui peut conduire à des cas de cyberintimidation. Pour aborder cette nouvelle réalité, l'école a fait appel à « une policière communautaire et à une éducatrice spécialisée » (Gervais et Fortier, 2021) afin de sensibiliser les jeunes. De plus, les parents

et les élèves sont encouragés à signaler de manière confidentielle les comportements inappropriés (Gervais et Fortier, 2021).

Pour prévenir la cyberintimidation et protéger leurs enfants, la spécialiste recommande alors aux parents de mettre en place un emploi du temps comprenant des activités obligatoires que les enfants doivent respecter après l'école, cela permettrait de réduire leur temps d'exposition aux écrans. Par exemple, les parents pourraient inclure un temps pour la réalisation des devoirs, pour le moment du bain, pour le repas et des activités en extérieur (Gervais et Fortier, 2021).

D'après Bruno Guglielminetti, journaliste, chroniqueur de presse et spécialiste des nouvelles technologies, il devient nécessaire d'éduquer les jeunes à adopter une citoyenneté numérique afin de les sensibiliser à l'importance d'une « bonne hygiène numérique » (Gervais et Fortier, 2021). Cette recommandation est d'autant plus urgente par le fait que les parents ont de plus en plus de mal à contrôler la croissance du temps d'écran chez leurs enfants. En effet, la pandémie a participé à augmenter de manière significative le temps passé devant les écrans. « Selon une enquête réalisée par l'Académie de la transformation numérique de l'Université Laval », ce sont 76% des jeunes âgés de 6 ans à 17 ans qui passent désormais « plus de temps devant leurs écrans à la maison qu'avant la crise ». De plus, « quatre élèves sur dix passent en moyenne plus de 10 heures par semaine » sur Internet, ce qui signifie une augmentation « de 15 points de pourcentage en un an ». Bien qu'une « majorité des parents (83 %) » déclarent superviser l'utilisation d'Internet par leurs enfants, on constate que depuis la pandémie « cette proportion a baissé de cinq points de pourcentage » (Gervais et Fortier, 2021).

1. Quelques données sur la cyberintimidation

Une prise de conscience croissante des risques liés à Internet et aux activités numériques se fait sentir parmi les parents et les jeunes. En effet, « la cyberintimidation, le vol de compte et l'utilisation non autorisée de données personnelles » sont en constante augmentation « à mesure que les adolescents grandissent ». Entre l'âge de 17 ans et 18 ans, « les signalements de cyberintimidation » atteignent « 18 %, les tentatives de vol de compte en ligne » représentent « 16 % et l'utilisation non autorisée de données personnelles » s'élève à 14 % (McAfee, 2022). Au Canada, en 2019, c'est un jeune sur quatre âgé de 12 à 17 ans qui dit avoir été victime de cyberintimidation (Statistique Canada, 2023 ; **Annexe 1**).

Au Québec, une étude[7] réalisée en 2022 révèle que « plus de la moitié (57 %) des québécois » âgés « de 10 à 18 ans » ont été victimes de cyberintimidation (Descurninges, 2022). Cependant, seulement 22 % d'entre eux ont déclaré avoir cherché de l'aide auprès de leurs parents, tandis que 22 % ont choisi de dissimuler cet événement (Descurninges, 2022). Selon Descurninges (2022), la moyenne de cyberintimidation chez les enfants au Canada s'élève à 60 %, tandis qu'au niveau mondial, ce chiffre atteint 63 %. De plus, plusieurs observations sont à noter concernant la cyberintimidation (Gravel, 2015) :

- La cyberintimidation affecte principalement les jeunes âgés de 15 à 24 ans.
- Les jeunes filles sont plus souvent touchées par la cyberintimidation que les garçons.
- Les auteurs de cyberintimidation sont généralement des personnes connues, telles que des amis, des camarades de classe ou des connaissances. Seulement environ un tiers des jeunes subissent une cyberintimidation de la part d'inconnus.
- En revanche, chez les adultes, la cyberintimidation est souvent exercée par des inconnus.

[7] L'étude commandée par l'entreprise de protection en ligne (McAfee, 2022)

Il est fréquent que le cyberharceleur soit une personne connue de sa victime. En effet, selon le même auteur, « 52 % des jeunes Canadiens » déclarent connaître leur harceleur. Cependant, ce pourcentage pourrait être encore plus élevé, car certains individus se dissimulent « derrière de faux comptes pour attaquer leurs connaissances » (Descurninges, 2022).

Une enquête réalisée par McAffee[8] (2022) révèle que les parents sont désignés par les trois quarts des enfants comme les personnes les plus compétentes pour les informer sur les meilleures pratiques de protection en ligne. Ce chiffre est « près de deux fois plus que les enseignants à l'école (39 %) et plus de deux fois plus que pour les ressources en ligne (34 %) » (McAffee, 2022). En effet, environ « 63 % des préadolescents et des adolescents du monde entier » comptent sur leurs parents pour les sensibiliser à la protection de leur vie privée en ligne. Ce pourcentage est plus élevé chez « les jeunes enfants (65 %) », mais diminue « à la fin de l'adolescence (55 %) » (McAffee, 2022).

D'après la même enquête, plus de la moitié des enfants (59 %) dissimulent leurs activités en ligne aux adultes. Les préadolescents et les adolescents avouent même effacer leur historique de navigation (26 %), fermer ou réduire leur navigateur lorsque leurs parents sont à proximité (21 %), masquer ou supprimer des messages instantanés ou des vidéos (15 %), utiliser la navigation privée (15 %), mentir ou omettre des détails concernant leurs activités en ligne (15 %), et utiliser un appareil que leurs parents ne contrôlent pas chaque fois que possible (10 %) (McAffee, 2022). De plus, les mesures de préservation de la confidentialité des activités en ligne, telles que l'effacement de l'historique de navigation ou l'utilisation du mode de « navigation privée », augmentent avec l'âge (McAffee, 2022).

[8] L'étude est effectuée par l'entreprise McAfee et conduite par la firme MSI-ACI en juillet 2022 auprès de 11687 répondants provenant de dix pays, soit le Canada, les États-Unis, la France, le Royaume-Uni, l'Allemagne, le Mexique, le Brésil, l'Australie, le Japon et l'Inde.

Par ailleurs, ce sont 33 % des parents qui reconnaissent avoir recours à des logiciels de contrôle sur les ordinateurs de bureau ou portables de leurs enfants pour assurer leur sécurité numérique. Ils utilisent également d'autres méthodes pour surveiller les activités de leurs enfants et leur temps d'écran. En ce qui concerne « la surveillance des activités sur l'appareil mobile » (McAffee, 2022) de leurs enfants, les parents déclarent :

- Limiter « le moment de la journée ou la durée pendant laquelle l'enfant passe du temps devant un écran », ce qui représente 59 % des parents.
- Vérifier « les sites Internet ou les applications que l'enfant visite ou utilise », ce qui concerne 56 % des parents.
- Consulter « les enregistrements d'appels ou les messages texte sur un téléphone intelligent » utilisé par leur enfant, ce qui est le cas de 40 % des parents.
- Être « ami » ou suivre leur enfant « sur les sites de réseaux sociaux », ce qui est pratiqué par 35 % des parents.
- Suivre « la localisation de l'enfant » grâce à des applications ou des « logiciels GPS », une pratique adoptée par 30 % des parents (McAfee, 2022).

Selon l'enquête de McAfee (2022), il est souligné que le contrôle parental est considéré comme étant plus important en ce qui concerne les activités en ligne surtout des jeunes filles par rapport à celles des garçons.

Au Québec, 78 % des parents déclarent prendre « des mesures concrètes pour protéger leur enfant », tandis qu'à l'échelle mondiale, ce chiffre s'élève à 85 %. Parmi ces mesures, on retrouve « la discussion (66 %), la surveillance des appareils électroniques (53 %), les entretiens avec la direction de l'école (28 %), la thérapie (11 %) et le changement d'école (8 %) » (Descurninges, 2022).

Une exposition excessive des jeunes aux médias sociaux accroît leur vulnérabilité numérique, en particulier si leurs activités en ligne ne sont pas supervisées par les parents. Plusieurs études mettent en garde contre les effets néfastes des réseaux sociaux numériques (RSN) sur les jeunes, en particulier lorsqu'ils sont utilisés de manière

intensive. Cela peut entraîner des conséquences telles que « l'isolement social, la solitude », des problèmes de « santé mentale et la cyberintimidation » (Schimele et *al.*, 2021). Le manque de sommeil, l'irritabilité, les difficultés de concentration et la diminution de l'activité physique sont également des conséquences possibles (Schimele et *al.*, 2021).

Au Canada, plusieurs actes de cyberintimidation commis sur les réseaux sociaux ont été recensés. Les statistiques montrent à ce propos que 46 % des jeunes Canadiens ont été victimes d'insultes, 34 % ont fait l'expérience d'exclusion, 20 % ont été l'objet de « fausses rumeurs », et 25 % ont subi « de l'intimidation à caractère raciste » (Descurninges, 2022). En ce qui concerne des actes plus graves de cyberintimidation, 11 % des jeunes ont déclaré avoir été victimes de « harcèlement » ou de « menaces physiques », tandis que 14 % ont signalé « avoir vécu du harcèlement sexuel » (Descurninges, 2022). Ces attaques peuvent être si extrêmes que 24 % des jeunes choisissent de supprimer définitivement leurs comptes de réseaux sociaux pour échapper à la cyberintimidation (Descurninges, 2022).

Il convient également de mentionner la « sollicitation sexuelle » par Internet, connue sous le nom de « leurre d'enfant », qui est une forme de victimisation en ligne, elle touche quant à elle environ un tiers des enfants victimes de cyberintimidation (33 %) (Gravel, 2015: 45).

1.1. Risques et prévention de la cyberintimidation

Certains facteurs sont identifiés comme favorisant les actes de cyberintimidation. Ce sont par exemple les

- « [facteurs] communautaires : le fait de vivre en milieu urbain
- facteurs relationnels : le fait d'avoir une relation parent-enfant dysfonctionnelle
- facteurs individuels : être une victime d'intimidation, être l'auteur de gestes d'intimidation, être auteur de cyberintimidation, éprouver de l'anxiété sociale, avoir des problèmes de santé mentale, avoir des comportements en ligne risqués, avoir une tendance au désengagement moral et avoir une utilisation fréquente d'Internet » (INSPQ, 2023).

Dans le cadre d'une étude de revue systématique de la littérature menée par Zhu et *al.* (2021), les chercheurs ont analysé de manière approfondie « la situation mondiale » de la « cyberintimidation, ainsi que les facteurs de risque et les mesures préventives » mises en place « pour lutter contre la cyberintimidation » chez les enfants et les adolescents (Zhu et *al.*, 2021:3, traduction libre). Ils ont constaté une augmentation significative du « taux de prévalence de la cyberintimidation », avec la forme la plus courante étant la « violence verbale ». L'étude a également identifié quatorze facteurs de risque et trois facteurs de protection associés à la cyberintimidation.

Des variables telles que « l'âge, le sexe, le comportement en ligne, la race, l'état de santé, l'expérience antérieure de victimisation et l'impulsivité » ont été identifiées « comme des facteurs de risque » associés à la cyberintimidation. De plus, « les relations parent-enfant, les relations interpersonnelles et l'emplacement géographique » ont aussi été étudiées. En ce qui concerne les « facteurs de protection », des éléments tels que « l'empathie et l'intelligence émotionnelle, la relation parent-enfant et le climat scolaire ont été fréquemment mentionnés » (Zhu et *al.*, 2021: 8, traduction libre).

Les jeunes cyberintimidés

Une étude examine la prévalence et la répartition entre les sexes des personnes victimes de cyberintimidation dans la tranche d'âge de 12 à 17 ans (Bouré et *al.*, 2022). L'échantillon, composé de 60,9 % de filles et de 34,8 % de garçons, révèle que 64,2 % des filles ont déjà été victimes de cyberintimidation et que 71% d'entre elles ont été témoins de telles agressions en ligne. En ce qui concerne les garçons, 62,5 % d'entre eux ont admis avoir été ciblés par la cyberintimidation, ce chiffre étant légèrement inférieur à celui des filles. Seulement 25 % des garçons affirment avoir été témoins de cyberintimidation, un pourcentage également inférieur à celui des filles. Dans l'ensemble de l'échantillon, 78,3 % ont déclaré connaître l'identité de leur agresseur en ligne, tandis que seulement 21,7 % ne connaissaient pas l'identité de leur cyberagresseur (Bouré et *al.*, 2022). Les résultats de l'enquête révèlent que la cyberintimidation a duré moins d'un an dans 50% des cas pour les filles et 57 % des cas pour les garçons. Environ 29 % des filles ont cherché de l'aide auprès de leurs amis, tandis qu'aucun garçon n'a fait de même lorsqu'il était victime de cyberintimidation. Cependant, les jeunes hommes sont plus susceptibles de demander de l'aide à leurs enseignants (29 %) (Bouré et *al.*, 2022).

En ce qui concerne les plateformes de médias sociaux sur lesquelles les garçons sont les plus victimes de cyberintimidation, Facebook est en tête avec 57 %, tandis que chez les filles, Instagram (29 %) et TikTok (Bouré et *al.*, 2022) sont plus fréquemment mentionnés.

La cyberintimidation cible particulièrement des groupes de personnes perçus comme différents en raison de préjugés ou de biais sociaux discriminatoires. La question de l'apparence physique est identifiée comme la principale cause de cyberintimidation chez les filles et les garçons. Par ailleurs, les garçons sont plus souvent attaqués sur les réseaux sociaux en raison de leurs « goûts personnels différents » (Bouré et *al.*, 2022: 19), ainsi que pour des raisons d'introversion (Bouré et *al.*, 2022).

Pour les filles âgées de 12 à 17 ans, une autre cause de cyberintimidation résulte des relations personnelles et « des liens sociaux » (Bouré et *al.*, 2022 : 19). La deuxième raison de la cyberintimidation concerne le « style vestimentaire » (Bouré et *al.*, 2022 : 19) et la troisième le « groupe d'amis » (Bouré et *al.*, 2022 : 19).

Pour ce qui est de la durée pendant laquelle les personnes subissent des actes de cyberintimidation, il ressort d'après l'enquête que cela dure moins longtemps chez les jeunes femmes, moins d'un an, que chez les hommes où cela peut aller jusqu'à deux ans (Bouré et *al.*, 2022).

Les jeunes cyberintimidateurs

Plusieurs facteurs peuvent contribuer à rendre une personne susceptible de se livrer à des actes de cyberintimidation. Parmi ceux-ci, on trouve les

- « Facteurs sociétaux : l'exposition à des contenus média présentant des comportements à risque ou antisociaux.
- Facteurs relationnels : avoir des problèmes de comportements à l'école, avoir une relation parent-enfant dysfonctionnelle, relations interpersonnelles conflictuelles comme ses pairs et les professeurs, avoir des comportements agressifs.
- Facteurs individuels : être une personne victime d'intimidation, être une personne autrice d'intimidation, avoir 15 ans et plus, avoir une tendance au désengagement moral, avoir un faible niveau d'empathie, avoir une utilisation fréquente d'Internet, avoir des comportements en ligne risqués, avoir une expérience antérieure de victimisation, avoir un comportement agressif » (INSPQ, 2023).

1.2. L'encadrement légal de la cyberintimidation

Certains actes de cyberintimidation sont sanctionnés par la loi et constituent des infractions au Code criminel, exclusivement de source fédérale et non provinciale. Voici quelques exemples de ces actes :

- « harcèlement criminel (appeler une personne ou lui envoyer des textos ou des courriels de manière à ce qu'elle craigne pour sa sécurité);
- pornographie juvénile (regarder, conserver et partager des photos et des vidéos intimes de mineurs [moins de 18 ans]);
- publication de l'image intime d'une personne en sachant qu'elle n'y a pas consenti;
- profération de menaces et extorsion (menacer de communiquer les renseignements personnels d'une personne à d'autres si elle ne fait pas ce qu'on lui demande);
- vol et fraude d'identité (créer un faux profil en ligne pour ruiner la réputation d'une personne);
- libelle diffamatoire (répandre des rumeurs sur une personne pour nuire à sa réputation ou amener les autres à la maltraiter)» (Gendarmerie royale du Canada, 2022).

Le Code criminel canadien prévoit des dispositions particulières pour les infractions reliées à la cyberintimidation (MSP, 2009). Voici quelques articles de lois provenant du Code criminel (Code criminel, 1985) :

- Diffamation (art. 301) :
  « Quiconque publie un libelle diffamatoire est coupable :
  a) soit d'un acte criminel passible d'un emprisonnement maximal de deux ans ;
  b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire ».
- Libelle délibérément faux (Art. 300) :
  « Quiconque publie un libelle diffamatoire qu'il sait être faux est coupable:
  a) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans;
  b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire ».
- Extorsion (Art. 346(1)) :
  « Commet une extorsion quiconque, sans justification ou excuse raisonnable et avec l'intention d'obtenir quelque chose, par menaces, accusations ou violence, induit ou tente d'induire une personne, que ce soit ou non la personne menacée ou accusée, ou celle contre qui la violence est exercée, à accomplir ou à faire accomplir quelque chose ».

- Harcèlement criminel (Art. 264 (1)) :
  « Il est interdit, sauf autorisation légitime, d'agir à l'égard d'une personne sachant qu'elle se sent harcelée ou sans se soucier de ce qu'elle se sente harcelée si l'acte en question a pour effet de lui faire raisonnablement craindre - compte tenu du contexte - pour sa sécurité ou celle d'une de ses connaissances ».
- Faux messages (Art. 372 (1)) :
  « Commet une infraction quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte que soient transmis par lettre ou tout moyen de télécommunication des renseignements qu'il sait être faux ».

L'article 4 de la Charte québécoise (1975) selon lequel « toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation » peut également être évoqué dans certains cas de cyberintimidation. Aussi, l'article 10 de la Charte québécoise (1975) protège à l'égard du harcèlement discriminatoire basé sur la race, la couleur, le sexe, la langue ou l'état civil, etc. (Gouvernement du Québec, 2024). Le gouvernement du Québec et ses nombreux ministères, organismes et personnes intervenantes, ont pris des mesures « pour intensifier les actions en matière de cyberintimidation », par exemple :

a. Soutenir la mise en place d'un modèle d'intervention organisées entre les corps policier, judiciaire et scolaire en cas de cyberintimidation liée au partage non consensuel de photos intimes (sexting). On suggère une collaboration étroite « entre les corps de police, les intervenants et intervenantes scolaires ainsi que le Directeur des poursuites criminelles et pénales (DPCP) », qui permettra de limiter la diffusion des images, de soutenir la victime, de prévenir d'autres incidents similaires ou de prendre des mesures qui s'imposent à l'égard des contrevenants et contrevenantes d'âge mineur et permettra d'éviter les préjudices associés à un long traitement judiciaire et à la médiatisation qui en découle ».
b. Informer la population sur les conséquences de l'hostilité en ligne visant les femmes, notamment celles qui prennent la parole en public, et sur les recours légaux que peuvent exercer les victimes à l'encontre de telles hostilités. Cela permettra de limiter la banalisation des propos d'intimidation en ligne. Cette mesure permet également la promotion de la réception positive de plaintes auprès de la police et de l'évaluation des recours juridiques actuels en matière de cyberintimidation.
c. Prévention dans les établissements d'enseignement primaire, secondaire, collégial et universitaire en implantant par des activités de sensibilisation et des formations concernant le traitement à privilégier pour la problématique du partage non consensuel d'images intimes (MFA, 2021).

En France, le gouvernement a instauré une législation connue sous le nom de Sécurisation et Régulation de l'Espace Numérique (SREN). Cette loi a pour objectif de garantir la sécurité et la régulation de l'environnement numérique, ainsi que de protéger les citoyens français, notamment les enfants, en mettant l'accent sur la prévention des escroqueries, « la lutte contre la haine en ligne ou le contrôle de l'accès des mineurs aux contenus pornographiques » (Hue, 2023).

Le projet de loi français est élaboré en vue d'accompagner la transition numérique de la société française. Les avancées technologiques dans le domaine numérique offrent des possibilités telles que « la diffusion du savoir », l'« accès à la culture » et l'innovation. Elles jouent également un rôle essentiel dans la « résilience de nos sociétés face aux crises telles que » la pandémie de Covid-19.

Cependant, ces progrès technologiques peuvent également être détournés, notamment lorsqu'ils sont utilisés pour propager « la haine en ligne », manipuler l'information, porter « atteinte aux données personnelles » ou mettre en danger le « bien-être des mineurs [...] exposés à des contenus inappropriés ou dangereux » (Légifrance, 2023). Le projet de loi vise donc à réguler ces aspects pour préserver les bénéfices de la transition numérique tout en assurant au mieux la protection des individus.

Avec ce projet de loi constitué d'une série de mesures, la France vise à restaurer l'ordre public dans l'espace numérique (Vie publique, 2023). Supervisé par le ministre délégué à la transition numérique, Jean-Noël Barrot, le projet de loi comporte une vingtaine de propositions. Ses objectifs principaux sont de :

- « (permettre) la mise en œuvre d'un filtre de cybersécurité anti-arnaque visant à protéger les Français contre les tentatives d'accès frauduleux à leurs coordonnées personnelles ou bancaires à des fins malveillantes qui se sont multipliées ces dernières années ;
- permettre un renforcement des sanctions des personnes condamnées pour cyberharcèlement, phénomène qui se propage sur les réseaux sociaux ;

- renforcer le dispositif visant à faire respecter les limites d'âge en ligne pour l'accès aux sites pornographiques et ainsi mieux protéger nos enfants ;
- sanctionner les sites en cas de non-retrait de contenus pédopornographiques en ligne ;
- restaurer l'équité commerciale sur le marché du cloud, aujourd'hui concentré dans les mains d'une poignée d'acteurs ;
- apporter des protections nouvelles contre la désinformation et les ingérences étrangères provoquées par la diffusion de médias frappés par des sanctions internationales ;
- adapter le droit national pour que puissent s'appliquer deux règlements européens majeurs que la France a fait adopter lors de sa présidence du Conseil de l'Union européenne en 2022 : le règlement sur les services numériques (DSA) et le règlement sur les marchés numériques (DMA)» (Vie publique, 2023).

Le premier chapitre du projet de loi porte plus spécifiquement sur la protection en ligne des mineurs (Légifrance, 2023) relatifs aux articles suivants :

- **L'article 1** vise à « élaborer un référentiel à valeur contraignante établissant les exigences techniques auxquelles doivent répondre les systèmes de vérification de l'âge mis en place pour l'accès aux sites comportant des contenus pornographiques ». Cela permettrait notamment de s'assurer que les utilisateurs désirant accéder à un contenu pornographique en ligne soient majeurs.
  L'article 2 confère aux autorités un pouvoir d'injonction administrative à l'encontre des sites problématiques qui ne se conformeraient pas à ces règles de réglementation de l'âge et « d'ordonner aux fournisseurs d'accès à Internet le blocage de l'accès à ces sites, sans contrainte, comme c'était le cas auparavant, de faire prononcer cette injonction par le juge ».
  L'article 3 « renforce la lutte contre la diffusion des contenus présentant un caractère pédopornographique. A l'instar des dispositions existantes en matière de retrait des contenus terroristes, cet article crée une obligation pour les hébergeurs de retirer les contenus pédopornographiques, sur injonction de l'autorité administrative, dans un délai de 24 heures ».
  L'article 5 « prévoit que le juge, lorsqu'il condamne une personne pour des faits de haine en ligne, de cyberharcèlement, ou d'autres infractions graves, pourra prononcer une peine complémentaire de suspension du compte d'accès au service de plateforme en ligne utilisé pour commettre ces infractions. La décision de condamnation sera signifiée au fournisseur de ce service de plateforme en ligne et celui-ci sera tenu de bloquer ce compte, sous peine de se voir condamné à une peine de 75 000 euros d'amende »

> **L'article 6** « porte sur le déploiement d'un filtre national de cybersécurité à destination du grand public permettant d'alerter les internautes via l'affichage d'un message d'avertissement dans leur navigateur lorsqu'ils souhaitent accéder à une adresse Internet pour laquelle il existe un risque avéré d'arnaque ou d'escroquerie, notamment vis-à-vis de leurs données personnelles ». Les sites cybermalveillants seront identifiés par des agents habilités et lorsque les faits persistent au-delà d'une période de 7 jours ou lorsque l'éditeur du service associé à l'adresse Internet n'est pas identifiable, les autorités pourront demander aux fournisseurs d'accès à Internet et aux fournisseurs de navigateur Internet de prendre toute mesure destinée à empêcher l'accès au site.
> **L'article 7** « vise à réguler certaines pratiques commerciales aujourd'hui répandues sur le marché des services d'informatique en nuage qui altèrent la liberté de choix et le jeu de la concurrence lorsqu'une entreprise souhaite contracter avec un fournisseur de services d'informatique en nuage ou changer de fournisseur ».

En définitive, l'objectif de ce projet de loi est de mettre en place un cadre réglementaire approprié pour l'environnement numérique, afin de garantir les droits et la sécurité des utilisateurs, tout en favorisant un développement numérique durable.

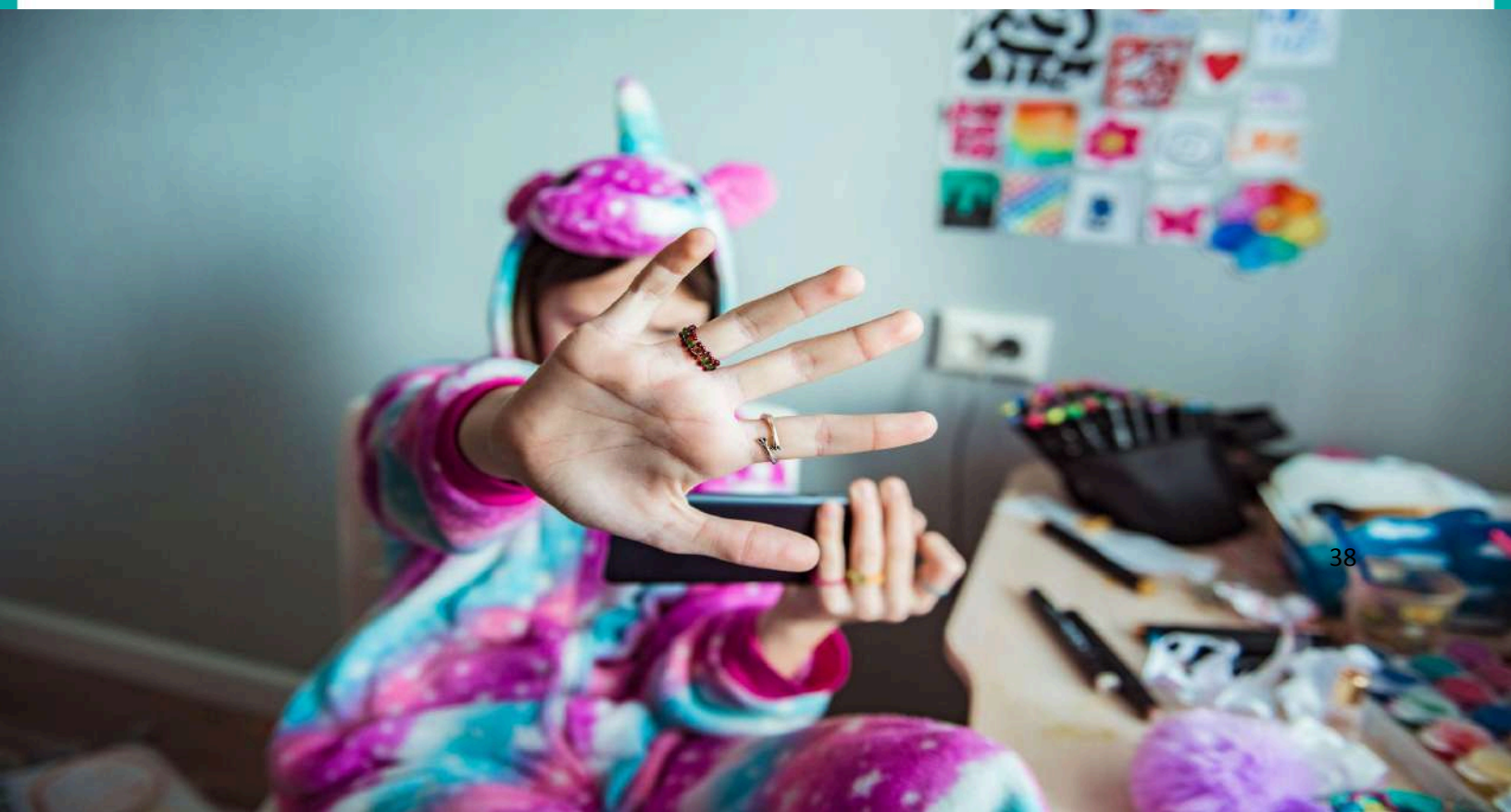
Le cas TikTok

TikTok, une plateforme sociale détenue par la société chinoise *ByteDance*, est accusée de collecter des données confidentielles des utilisateurs et de les transmettre aux autorités chinoises par le biais de sa société mère (Pierre, 2023). En plus de cela, TikTok représente une menace en raison de problèmes liés à son utilisation, tels que la dépendance à la plateforme et la propagation de « la désinformation, la censure de contenu, l'espionnage et la cyberintimidation, etc. » (Pierre, 2023). Inquiète des mesures de protection de la vie privée de ses citoyens, l'Union européenne (UE) lance un avertissement au PDG de TikTok et envisage de constituer une loi prévoyant des sanctions dissuasives, y compris une interdiction pour TikTok d'opérer dans la zone de l'UE en cas de violation répétée des lois en vigueur. Il convient de noter que TikTok est déjà interdite dans plusieurs pays, notamment l'Inde, le Pakistan, le Bangladesh et l'Azerbaïdjan (Pierre, 2023).

2. Les phénomènes de cyberviolence

Prévenir la répétition des violences et les intentions malveillantes dans le cyberespace représente un défi complexe, car le fonctionnement même du Web et des médias sociaux peut contribuer à leur propagation : « chaque like, commentaire ou partage d'un contenu » nuisible peut contribuer à sa diffusion et « à sa répétition » (Stassin, 2022 : 74-75). En effet, le numérique offre une diffusion rapide de l'information, tandis que « l'anonymat» favorise un « sentiment d'impunité » ou une moindre prise de « conscience des conséquences de ses actes ». De plus, en raison de cet anonymat, il est souvent difficile d'identifier l'auteur des actes (MENESR, 2016 : 6).

Les actes de cyberviolence peuvent se produire « à toute heure du jour ou de la nuit » et laisser « des traces numériques durables ». Une fois que les agressions sont publiées en ligne, l'auteur perd le contrôle sur la propagation des contenus, ce qui peut avoir des répercussions à long terme (MENESR, 2016 : 6). La mise en place d'un programme global de prévention de la cyberintimidation, du cyberharcèlement et plus généralement de la cyberviolence s'avère donc essentielle.



2.1. Les formes de cyberviolence

Nous avons organisé des données dans le tableau ci-dessous afin de présenter les différentes formes de cyberviolence.

CYBERVIOLENCE

La cyberviolence englobe différentes formes de violence en ligne, un large éventail de phénomènes (e-enfance, s.d), et partage des similitudes avec la cyberintimidation (Couchot-Schiex et *al.*, 2016). En effet, selon la littérature les frontières entre ces deux concepts restent floues. La cyberviolence est souvent caractérisée par des « incitations à la haine » (MENESR, 2016 : 6) pouvant être perpétrés par une ou « plusieurs personnes » à l'encontre d'une personne ou d' « un groupe » (MENESR, 2016 : 6). Elle se caractérise par une violation du consentement « de la victime » (Jehel, 2018) et repose sur « un système de normes » (Jehel, 2018) qui définit les limites « du consentement et des comportements » (Jehel, 2018) acceptables. « Les jeunes peuvent être exposés à des actes de cyberviolence » sans en être conscients et « sans être préparés » à y faire face (Jehel, 2018). La Cyberviolence est une

> [tentative] d'isolement de la victime par rapport au groupe de pairs ou aux membres du réseau. Plus particulièrement, les filles et les femmes peuvent être victimes de *slutshaming »* (cf. glossaire en fin de guide) (MENESR, 2016 :8).

L'auteur de la cyberviolence a un pouvoir de persuasion sur la victime pour l'inciter à se déshabiller alors qu'il la filme avec une webcam ou prend une photo dans le but de publier ce contenu sur les médias sociaux ou la partager par message à plusieurs personnes. Cette pratique dans l'espace numérique facilite un partage exponentiel à grande vitesse (MENESR, 2016 : 8).

CYBERHARCÈLEMENT

Le cyberharcèlement est « un acte agressif et intentionnel [...] à l'encontre d'une victime qui ne peut facilement se défendre seule » (MENESR, 2016 : 7), il se caractérise par

> [un] acte volontaire répété de la part de l'agresseur ou des agresseurs, qui se base sur un déséquilibre de pouvoir. C'est une situation de domination de violence répétée qui s'inscrit sur la durée [et qui] est perpétrée au moyen des outils électroniques de communication. [...] Il s'agit de violences ayant lieu au moins une fois par semaine sur une durée d'au moins un mois (Couchot-Schiex et *al.*, 2016 : 18, cit. Blaya dans CHA, 2014, pages 7-8).

Finalement le cyberharcèlement serait défini comme étant

> [des] cyberviolences répétées à l'encontre d'une personne avec intention de nuire et asymétrie des forces [...]. Pour permettre une prise en compte de cette violence fragmentée, la loi du 3 août 2018 contre les violences sexuelles et sexistes fait évoluer la notion de harcèlement en introduisant celle de « harcèlement en meute » et de « raid numérique ». Ainsi, toute personne participant au dénigrement ou à l'humiliation d'une autre en réagissant ne serait-ce qu'une seule fois à un contenu peut désormais être reconnue coupable de cyberharcèlement. En outre, **la** répétition peut venir de la pérennité des traces numériques faisant qu'un contenu peut ressurgir à tout moment, des mois voire des années après sa publication initiale et entacher à nouveau l'image et la réputation d'une personne. Enfin, l'intention de nuire n'est pas toujours avérée : on peut par exemple *liker* un contenu par habitude ou par inadvertance, ou bien encore réagir sous le coup de l'émotion sans réfléchir aux conséquences de son action. Les émotions sont d'ailleurs une composante essentielle du mécanisme de harcèlement scolaire et de cyberharcèlement (Stassin, 2022 : 74-75).

La peur ressentie par les victimes représente un « indicateur de cyberharcèlement » lorsqu'elles reçoivent « des messages non souhaités par courriels, messages texte, Facebook ou d'autres réseaux sociaux » (Hango, 2016 : 12). « Le cyberharcèlement, contrairement à la cyberintimidation, intègre de façon plus explicite la peur que ressentent les participants quant à leur sécurité » (Hango, 2016 : 2).

CYBERINTIMIDATION

La cyberintimidation (*Cyberbulling* en anglais*)* est aussi appelée : « « perpétration d'actes d'intimidation en ligne » ou « perpétration en ligne » » (Zych, 2019 : 2). Étant une forme de cyberagression (Ollagnier and *al.*, 2022 : 3, trad. libre), elle est un acte d'intimidation exprimé à partir des médias numériques, par exemple sur les réseaux sociaux, les blogues, les jeux en ligne, la messagerie instantanée, les courriels ou textes, etc. (Gouvernement du Québec, 2023a). Un tel acte répété est commis « par un ou des individus [...] qui communique d'une façon hostile ou agressive un message texte, photo ou vidéo destiné à infliger un préjudice ou un inconfort chez l'autre » (Tokunaga, 2010).

L'acte de cyberintimidation a une grande capacité à devenir virale, surtout sur les réseaux sociaux (Institut national de santé publique du Québec, 2023). Nous sommes en présence de cyberintimidation lorsqu'un individu ou un groupe utilise les technologies numériques, des « outils électroniques de communication comme le courriel, le téléphone cellulaire ou l'assistant personnel numérique » (Begin, 2016 : 22-23, cit. Li, 2008 – trad. libre) pour effectuer certains actes (cf. *section 2.2.*).

Après avoir proposé plusieurs définitions de la cyberintimidation, l'auteur Begin (2016) retient finalement la suivante :

> Conceptuellement, il y a quelques éléments nécessaires sur lesquels presque tout le monde peut s'entendre pour définir exactement ce qu'est la cyberintimidation. Essentiellement, la cyberintimidation consiste à utiliser la technologie pour intimider une autre personne. Cette technologie pourrait être un ordinateur, téléphone portable, tablette, appareil photo numérique wifi ou autre appareil électronique. Deuxièmement, cela implique un préjudice. La victime ou la cible du comportement est négativement impactée (psychologiquement, émotionnellement, socialement, etc.) par l'incident. Ce qui est inclus dans la plupart des définitions de la cyberintimidation est que le comportement est répété (Bégin, 2016 : 22-23).

Toutefois le caractère répétitif de la cyberintimidation est remis en cause, car l'information partagée peut rester longtemps sur Internet et sera par conséquent visible par un nombre exponentiel de personnes (Zych, 2019). Les résultats d'une étude montrent que généralement, les intimidateurs dans la *vraie vie* auraient tendance à reproduire ce comportement dans le monde numérique. Ils seraient environ cinq fois plus susceptibles de devenir des cyberintimidateurs que les autres (Estevez et *al.,* 2020).

Finalement, les intimidateurs « traditionnels » et les cyberintimidateurs partagent des caractéristiques communes (Estevez et *al.*, 2020 : 10). Les intimidateurs qui sévissent à l'école continuent d'intimider leurs victimes en ligne.

Tandis que les victimes d'intimidation dans la cour d'école peuvent également subir davantage de l'intimidation en ligne que les non-victimes (Marciano et *al.,* 2020). Par ailleurs, l'augmentation d'internautes actifs sur les réseaux sociaux devient proportionnelle au nombre de victimes de cyberintimidation (INSPQ, 2023). Le caractère persistant et omniprésent des actes de cyberintimidation conduit à des sentiments de désespoir, qui sont associés à des comportements suicidaires chez les adolescents (John and *al.*, 2018).

Finalement, bien que l'environnement numérique prolonge les phénomènes sociaux (Estevez et *al.*, 2020 – trad. libre), la cyberintimidation comme les autres formes de cyberviolence se distingue de l'intimidation traditionnelle. Nous retenons quatre grands traits de distinction : (1) l'anonymat du cyberintimidateur ; (2) le partage rapide, répété de l'information ou de l'événement ; (3) (4) « le caractère omniprésent de la cyberintimidation qui peut survenir à toute heure de la journée et enfin son absence de limite physique (Li et *al.*, 2012) » (Boudreault, et *al.*, 2020 : 72).

Pour prévenir ce phénomène, des interactions saines avec les parents, un milieu scolaire épanouissant et le développement de l'empathie sont des éléments qui participent à diminuer les comportements de cyberintimidation (Marciano et *al.*, 2020).

CYBERVICTIMISATION

La cyberintimidation est un type de cybervictimisation (Gravel, 2015), elle est caractérisée par

> « 1) l'intention de porter préjudice à la victime, 2) le déséquilibre de pouvoir entre l'auteur de la violence et la victime, 3) la nature répétée du geste, 4) l'utilisation d'appareils électroniques, y compris les téléphones et les ordinateurs, et 5) la possibilité d'agir de façon anonyme » (Hango, 2023 : 2).

CYBERHAINE

Le terme de cyberhaine désigne les discours de haine prononcés en ligne. Le discours de haine a été défini comme toutes les formes d'expression qui répandent, incitent, promeuvent ou justifient la haine, la discrimination, la xénophobie et d'autres formes de haine fondées sur l'intolérance (Conseil de l'Europe, 2018), (Ollagnier and *al.*, 2022) (trad. Libre).

2.1. Les actes de cyberviolence

Nous avons regroupé dans le tableau ci-dessous des actes commis par des auteurs de cyberviolence ou de cyberagression, exprimés sous forme de verbes. Des questions et exemples permettant d'identifier ces situations sont présentés dans l'**Annexe 2**, basés sur les travaux de Hango (2016).

ACTES DE CYBERVIOLENCE

Plusieurs actes commis intentionnellement par un individu ou un groupe « de manière répétée ou au fil du temps, contre une victime qui ne peut pas facilement se défendre » (Begin, 2016 : 22-23, cit. Smith et *al.*, 2008 : 376 – trad. libre) représentent des actes de cyberviolence.

Par exemple,

- « Commettre des actes délibérés, répétés et hostiles, afin de blesser les autres intentionnellement » (Begin, 2016 : 22-23, cit. Besley, 2009 – trad. libre).
- « Insulter ou menacer quelqu'un » (Begin, 2016 : 22-23, *cit.* Juvoven et Gross, 2008 : 497– trad. libre).
- Commettre « un acte d'agression déclaré et intentionnel en direction d'une autre personne en ligne » (Begin, 2016 : 22-23, cit. Ybarra et Mitchell, 2004 – trad. libre).
- Agresser quelqu'un « par le biais de dispositifs technologiques modernes et plus spécifiquement les téléphones mobiles ou Internet (Begin, 2016 : 22-23, cit. Slonje et Smith, 2008 : 147 – trad. libre).

Nous formulons les actes de cyberviolence du côté des auteurs qui commettent ces actes et nous les divisons en plusieurs thèmes. Ces actes répondent aussi bien aux situations de cyberharcèlement que de cyberintimidation ou cybervictimisation, bref à toutes les formes de cyberviolence.

DIFFUSION ET PARTAGE DE CONTENUS NUMÉRIQUES

Dans les actes de cyberviolence sur le Web, « les contenus sont envoyés, rendus publics ou partagés au moyen de formes électroniques de communication – applications, en particulier réseaux sociaux accessibles sur Internet, et/ou à partir de smartphones, tablettes, ordinateurs » (MENESR, 2016 : 6). Quelques exemples de ces actes sont :

- Infliger « des torts [...] de manière intentionnelle et répétée par le biais du médium que sont les messages textes » (Begin, 2016 : 22-23, cit. Patchin and Hinduja, 2006: 152 – trad. libre).
- Diffuser des contenus numériques violents (images, messages), haineux, sexuels, etc. (Jehel, 2018). Il peut s'en suivre des violences (en ligne ou non) en direction de la victime (Jehel, 2018).
- « Envoyer ou publier des textes ou des images blessants ou violents en utilisant Internet ou d'autres dispositifs numériques de communication » (Begin, 2016 : 22-23, cit. Willard, 2007 : 1 – trad. libre).
- Diffuser des « images intimes sans le consentement de la personne qu'elles représentent afin de nuire à son image ou à sa réputation » (Stassin, 2022 : 74-75).

- « Prendre une photo » ou « une vidéo embarrassante ou intime d'une personne sans son autorisation et la faire circuler sur les réseaux sociaux » (Gouvernement du Québec, 2023 ; MFA, 2021).
- Publier une « photo ou vidéo embarrassante ou humiliante de la victime » (e-enfance, s.d).
- Publier des « photos ou des renseignements inappropriés, indésirables ou personnels au sujet de la victime sur un site de médias sociaux » (Hango, 2016 : 2).
- Publier des « propos diffamatoires et discriminatoires ou à visée diffamatoire ou discriminatoire ; [...] [des] propos humiliants, agressifs, injurieux » (MENESR, 2016 : 6).
- Publier des « commentaires insultants ou [...] rumeurs sur le mur ou le profil de la victime » (MENESR, 2016 : 8).
- Publier des photos humiliantes ou des photomontages (MENESR, 2016).
- Publier ou distribuer, ou menacer « de publier ou de distribuer, des vidéos ou des images intimes ou sexuellement explicites de la victime » sans son consentement (Hango, 2023 : 3).
- Publier « des messages à caractère raciste, antisémite ou homophobe » (MENESR, 2016 : 8).
- Envoyer des « photos embarrassantes ou qui ont semblé menaçantes pour le participant » (Hango, 2016 : 2).
- Envoyer des « courriels ou messages instantanés menaçants ou agressifs » en ciblant un « seul destinataire » ou une « personne faisant partie d'un groupe » (Hango, 2016 : 2).
- Envoyer « des menaces ou d'autres actes offensants (excluant la sollicitation sexuelle) » ou publier ces « menaces » ou « autres actes offensants [...] pour que d'autres jeunes les voient » (Begin, 2016 : 22-23, cit. Finkelhor et *al.,* 2000 – trad. libre).
- « Envoyer des courriels ou des messages textes blessants ou menaçants » à une personne (Gouvernement du Québec, 2023a).
- Envoyer des « contenus pornographiques [...] à la victime » (MENESR, 2016 : 8).
- Envoyer « des images ou des messages sexuellement suggestifs ou explicites à la victime, alors qu'elle ne voulait pas les recevoir » (Hango, 2023 : 3).
- Partager une vidéo ou photo compromettante avec des amis de la victime par SMS (MENESR, 2016) ou autres moyens numériques

- Partager « de la violence physique (scènes d'agression filmées et diffusées sur les médias sociaux) » (Stassin, 2022 : 74-75).
- Inciter des personnes « à écrire des commentaires désobligeants » (MENESR, 2016 : 8).
- « Persuader la victime de se déshabiller devant une webcam, prendre une photo ou enregistrer une vidéo et la publier » (MENESR, 2016 : 8).
- Propager des rumeurs (MENESR, 2016), des secrets à propos « d'une personne via les réseaux sociaux, les messages courriels ou messages textes » (Gouvernement du Québec, 2023a).
- Commettre des violences « verbale et psychologique (insultes, moqueries, menaces) » (Stassin, 2022 : 74-75).
- Créer une page sur les réseaux sociaux pour publier des « commentaires ou photos désagréables » en humiliant « un ou plusieurs élèves » (MENESR, 2016 : 8). Cela se fait à l'encontre de la personne ou des personnes concerné.e.s.
- Obliger une « victime d'envoyer, de partager ou de publier des images ou des messages sexuellement suggestifs ou explicites » (Hango, 2023 : 3).

GESTION DES ACCÈS ET DES IDENTITÉS (GAI)

Nous avons retenu dans les actes de cyberviolence des enjeux en gestion des accès et des identités (GAI). Par exemple,

- Pirater un compte (MENESR, 2016 : 6).
- Usurper une identité numérique pour « utiliser la messagerie d'une personne » Stassin, 2022 : 74-75).
- Usurper une identité numérique pour « ouvrir un profil [au] nom [d'une personne] pour envoyer ou publier des contenus compromettants » (Stassin, 2022 : 74-75) ; « pour envoyer ou publier des renseignements gênants ou menaçants » (Hango, 2016 : 2).
- Usurper une identité numérique divulguer des informations ou des « images personnelles (volées et/ou modifiées et/ou choquantes) » (MENESR, 2016 : 6).
- « Utiliser le mot de passe d'une personne pour accéder à ses comptes de réseaux sociaux et y afficher un contenu embarrassant » (Gouvernement du Québec, 2023a).

VULNÉRABILITÉ TECHNOLOGIQUE

Nous avons identifié et sélectionné plusieurs actes illustrant des situations de vulnérabilité technologique ::

- Menacer des « systèmes informatiques (propagation de virus, installation de logiciel espion) » (Stassin, 2022 : 74-75).
- Envoyer des « virus à la victime » (MENESR, 2016 : 8).
- Utiliser une « carte de crédit ou débit, ou des détails de ces cartes, à partir d'une source Internet pour effectuer des achats ou retirer des fonds du compte sans l'autorisation du détenteur » (Gravel, 2015 : 46). Cet acte est une forme de cyberintimidation en lien avec la cybervictimisation et se nomme « la fraude bancaire » (Gravel, 2015 : 46).
- Envoyer des « courriels frauduleux provenant de quelqu'un qui se fait passer pour une organisation fiable et légitime, et qui demande des renseignements personnels ou financiers » (Gravel, 2015 : 50). Cet acte est une forme de cyberintimidation en lien avec la cybervictimisation et se nomme l'hameçonnage (Gravel, 2015).

EXCLUSION SOCIALE NUMÉRIQUE

Concernant l'exclusion sociale numérique, cette catégorie d'actes se distingue par des situations particulières de cyberviolence, notamment :

- Exclure ou bannir la victime « d'un groupe ou d'un forum en ligne » (Stassin, 2022 : 74-75).
- Exclure une personne d'une « communauté en ligne » (Hango, 2023 : 3).
- « Créer des sondages Internet sur une personne et la « coter » d'une manière négative » (Gouvernement du Québec, 2023a).

AUTRES ACTES

Nous avons identifié plusieurs autres actes qui renseigne une situation de cyberviolence :

- Effectuer des « appels insistants » avec un numéro masqué (MENESR, 2016 : 8).
- Émettre des « menaces, insultes, silence » en ligne ou par SMS (MENESR, 2016 : 8) ou encore « par des messages texte » (Hango, 2023 : 3).
- Envoyer des « courriels blessants ou [des] menaces, anonymes ou non » (MENESR, 2016 : 8).

- Envoyer des « commentaires menaçants ou agressifs [...] au moyen de courriels de groupe, de messages textes de groupe, ou de publications dans les médias sociaux » en ciblant un destinataire (Hango, 2023 : 3).
- Afficher sur Internet des informations blessantes (Hango, 2023 : 3).
- Envoyer des « messages non souhaités par courriel, messagerie texte, Facebook ou tout autre média social » (Hango, 2016 : 2).
- Envoyer des « messages électroniques qui intimident ou menacent leur destinataire » (Hango, 2016 : 2).
- Formuler des avances sexuelles ou des sollicitations sexuelles en ligne en envoyant un courrier électronique, un message instantané ou en abordant la victime dans un salon de clavardage (Gravel, 2015). Cet acte est une forme de cyberintimidation en lien avec la cybervictimisation et se nomme le « leurre d'enfant » (Gravel, 2015).

2.3. Plusieurs formes de cyberintimidation

> « *Une élève m'a confié, terrorisée, qu'un de ses contacts la harcèle sur MSN, lui demandant de se déshabiller devant la webcam et de simuler des actes sexuels. Il la menace si elle refuse* » (MENJ, 2011 :7)

2.3.1. Cybersexisme ou *Cybersexism*

Des chercheurs s'intéressant aux questions de genre (Couchot-Schiex et *al.*, 2016) proposent la définition du cybersexisme. C'est un phénomène qui représente

> [En effet, c'est plus des] faits qui font violence, se déploient à travers le cyberespace, contaminent l'espace présentiel ou réciproquement et qui visent à réitérer les normes de genre ciblant distinctement garçons et filles ; bref, à mettre ou à remettre chacune et chacun à la « place » qui lui est assignée dans le système de genre (Couchot-Schiex et *al.*, 2016 : 57)

Ces faits peuvent être « des actes / commentaires / messages à caractère sexuel ou qui critiquent la manière de s'habiller, l'apparence physique, le comportement amoureux ou sexuel » (Centre Hubertine Auclert, s.d. Kit de campagne). On retient que des « dimensions sexistes et/ou homophobe / lesbophobe » motivent ces actes (Couchot-Schiex et *al.*, 2016 : 18). Et même si tout le monde peut être victime des « actes de cybersexisme », ils « s'exercent majoritairement auprès des filles et des garçons aux comportements et aux préférences atypiques par rapport au genre – considérés comme homosexuels ou « ambigu-e-s » » (Couchot-Schiex et *al.*, 2016 : 57).

Le cas des gameuses québécoises

Selon Tison (2019), sur les plateformes des réseaux sociaux les *gameuses* québécoises sont souvent victimes de harcèlement, parfois de manière violente. Selon l'auteur, il existe une hostilité de la part de certains joueurs envers les femmes jouant aux mêmes jeux qu'eux, ce qui se traduit par des menaces de viol et des incitations à abandonner les jeux vidéo.

Pauline Zampolini, une étudiante en communication, a été contrainte d'arrêter de jouer à *League of Legends* en raison du climat toxique envers les femmes et les minorités. Sophie Déziel, une développeuse Web et *gameuse*, témoigne également de la présence fréquente de commentaires racistes et homophobes sur ces plateformes.

La plateforme Twitch, qui permet de suivre des parties de jeu vidéo en direct, est souvent la cible d'attaques de trolls. Une croyance erronée mentionnée dans l'article prétend que ces hostilités envers les joueuses auraient commencé lorsqu'elles ont commencé à « montrer de larges décolletés en jouant à des jeux vidéo sur Twitch ». Cependant, Lyne Bouthillette, joueuse et directrice des communications et du marketing chez Randolph, affirme que le harcèlement existait bien avant cette pratique (Tison, 2019).

Stéphane Villeneuve, professeur à l'UQAM et chercheur spécialisé en cyberintimidation, observe que le harcèlement en ligne subi par les joueuses peut exercer une pression si forte qu'elles peuvent être amenées à prendre un congé de travail, à éprouver de l'anxiété voire à souffrir de « troubles du sommeil ». Malgré la nature virtuelle des messages, leur effet préjudiciable et la détresse qu'ils causent ne sont en rien atténués. Les commentaires reçus peuvent avoir des répercussions négatives tangibles sur la santé mentale des femmes. Selon l'expert, les joueurs qui attaquent les joueuses en ligne considèrent le jeu vidéo comme un univers exclusivement masculin, où les femmes sont souvent perçues comme des intruses.

La manifestation de la supériorité des femmes dans un jeu peut être interprétée comme étant une atteinte à la masculinité des joueurs. D'après le professeur Villeneuve, deux facteurs prédisent le harcèlement sexuel, que ce soit en ligne ou en personne : d'une part, l'« orientation de dominance sociale », où certains individus croient en la supériorité sociale des hommes par rapport aux femmes, et d'autre part, le « sexisme hostile » qui exprime « une forme d'antipathie envers les femmes » (Tison, 2019).

De plus, la culture sexiste des jeux vidéo se reflète dans la représentation des femmes, qui sont soit dépeintes comme des « princesses fragiles qu'il faut soutenir », soit comme des « dominatrices aux vêtements provocateurs assez suggestifs » (Tison, 2019). Selon l'article, cette forme de représentation contribue à légitimer « le harcèlement en ligne » et favoriser « le harcèlement sexuel » dans la réalité (Tison, 2019).

2.3.2. Vidéolynchage ou *Happy Slapping*

L'usage de l'expression *Happy Slapping* remonte à 2005 (Chan, 2012). Selon le journal américain *The Association Press,* le *Happy Slapping* se produit lorsqu'on « filme à l'aide d'une caméra rudimentaire une victime à son insu » (Chan, 2012 cit. *Associated Press*, 2006). Le mot anglais « *Slapping* » qui signifie « gifler » s'apparente à la violence physique que subissent les victimes des auteurs du *Happy Slapping* (Chan, 2012). Le terme « happy » qui veut dire « heureux » caractérise le divertissement que représente le *Happy Slapping* pour ceux qui en sont les initiateurs (Chan, 2012). C'est dire le manque d'empathie et le plaisir pervers que peuvent ressentir les auteurs d'un tel acte.

Selon Begin (2016) « le vidéolynchage (*video recording of assaults/happy slapping and hopping*) » concerne « l'enregistrement vidéo de scènes de violence ou d'humiliation commises à l'endroit de victimes dans le but de les publier en ligne et d'accroître la portée de l'acte de violence » (Begin, 2016 : 28)

Selon Chan (2012), le ***Happy Slapping*** **ou vidéolynchage ou vidéo agression** aurait trois composantes principales.

- D'abord, la victime qui est impliquée est agressée, cette agression peut être psychologique, physique ou sexuelle.
- Ensuite, cette agression est filmée et enregistrée par une partie impliquée dans cette agression. Ce facteur est davantage relié aux enregistrements vidéo, soit des images en mouvement accompagnées d'un son, plutôt qu'aux photographies. Selon le journal *Agence Allemagne Presse* (2005), le *Happy Slapping* est surtout effectué à l'aide de caméras de téléphones portables.
- Enfin, ce genre de vidéos sont distribuées à d'autres usagers de téléphones portables, par exemple, via les messages textes ou à travers d'autres outils multimédias. Les victimes d'un tel acte peuvent vivre de nombreux traumatismes en raison de l'humiliation provoquée par la circulation de telles vidéos dans leur entourage (Chan, 2012).

Faits divers

En 2005, deux adolescentes anglaises mettent en feu une personne sans domicile fixe et en profitent pour filmer son agonie en se moquant d'elle : « C'est la chose la plus drôle que j'ai jamais vu… on va le tuer !… Il est en feu ! » (Chan, 2012 cit. *Agence Allemagne Presse*, 2005). Un autre exemple, le *Tampa Tribune* rapporte le cas de huit adolescents qui ont été arrêtés le 30 mars 2008 pour avoir agressé Victoria Lindsay, une étudiante de 16 ans, en filmant cette altercation pour ensuite la publier sur YouTube et Myspace (Chan, 2012 cit. *New York Times*, 2008).

Les adolescents voulaient ainsi se venger de la jeune victime qui aurait tenu des propos désobligeants à leur égard par messages textes et sur la plateforme Myspace (Chan, 2012 cit. *New York Times*, 2008).

2.3.3. Intimidation par message ou *Text bullying*

Le « Text Bullying » se traduit par l'envoi de messages textes via des téléphones portables de messages « blessants, humiliants, embarrassants et faussement

accusatoires » (*Bullying Statistics*, s.d. Trad. libre). Avec l'essor de l'usage des téléphones portables par des adolescents et des enfants, ce genre de cyberintimidation a accusé une véritable augmentation (*Bullying Statistics*, s.d.).

Parmi les adolescents qui utilisent des téléphones portables, 20% d'entre eux subiront des situations de « *text bullying* » tandis que 10% d'entre seront les auteurs d'un tel acte (*Bullying Statistics*, s.d.).

2.3.4. Auto-mutilation ou *Self-Harm*

Les adolescents victimes de cyberintimidation sont davantage à risque de manifester des comportements d'auto-mutilation ou *Self-Harm* et des tendances suicidaires que les adolescents qui ne subissent pas ce type d'intimidation (John and *al.*, 2018).

2.3.5. Porno divulgation ou *Revenge Porn*

Le terme « Revenge Porn » décrit les situations ou du contenu pornographie impliquant une personne est partagé sans le consentement de cette dernière, et dans le but d'humilier publiquement celle-ci (Hackett, 2016).

Les jugements moraux de l'entourage et de la société sur la sexualité des victimes de cyberharcèlement les livrent aux harcèlements. Après de telles publications, la victime subit des insultes, menaces ou agressions de la part de ceux qui ont accès à l'enregistrement vidéo (Wikipédia, 2023).

2.3.6. Sextage ou *Sexting*

Le sextage ou « sexting » revient à envoyer des photographies, des messages textes ou des enregistrements vidéo avec du contenu sexuellement explicite (*National Crime Prevention Council,* s.d.). Selon une étude mené par le *National Campaign to Prevent Teen and Unplanned Pregnancy* (2008), 39% des adolescents admettent avoir reçu ou avoir envoyé des messages de nature sexuelle, comme des photos de parties intimes ou

de corps dénudés ou semi-dénudés, des messages textes et des vidéos avec un contenu sexuellement explicite (*National Campaign to Prevent Teen and Unplanned Pregnancy*, 2008 : 3 , Trad. Libre)

Selon Begin (2016), le sextage « désigne l'envoi ou la publication en ligne de photos ou de vidéos présentant une personne nue ou partiellement nue, dans le but de la mettre dans un certain état de vulnérabilité » (Bégin, 2016 : 28).

Une étude montre que la prévalence de la transmission sans consentement d'un « sexto » était d'environ 12% au sein d'une population (Gottschalk, 2022). Les filles seraient plus à risque de ressentir de la pression à envoyer des messages de cette nature d'elles-mêmes que les garçons, elles sont également celles qui souffrent le plus des jugements les plus sévères de leur entourage quand ces images circulent entre les mains d'autres personnes (Gottschalk, 2022).

Certaines études font état d'une « association entre le « sexting » et la victimisation par cyberintimidation » (Gottschalk, 2022 : 20).

2.3.7. Technologies d'hyper-trucage ou *Deepfakes*

> « *Des photos retouchées d'un de mes élèves circulent dans le collège, via les téléphones mobiles, montrant celui-ci dans une situation dégradante…* » (MENJ, 2011 :7)

Avec l'évolution rapide des technologies numériques et de l'intelligence artificielle (IA), nous assistons à la naissance d'un nouveau phénomène appelé les *deepfakes* (Naffi et *al.*, 2021). Les *deepfakes* sont des reproductions audiovisuelles ultraréalistes. Ils permettent, par exemple, de concevoir numériquement un individu et lui faire dire ce que l'on désire ou « le faire agir, sans son consentement, de façon à tromper la vigilance humaine » (Naffi et *al.*, 2021 : 4).

Selon Naffi et *al.* (2021) la désinformation en ligne est un phénomène qui génère de plus en plus d'inquiétudes. L'hypertrucage malveillant (*deepfake*), en particulier, représente une véritable menace pour les bases perceptuelles de la connaissance humaine.

En effet, la désinformation de type *deepfake* risque de tromper les perceptions humaines entre les faits véridiques et représente aussi un risque pour la démocratie dans un avenir rapproché. Les experts prédisent que les *deepfake* seront utilisés pour « la cyberintimidation, la destruction de réputations, le chantage, la diffusion de discours haineux, l'incitation à la violence et la perturbation des processus démocratiques » (Naffi et *al.*, 2021 : 5).

Cette technologie rend la distinction entre le vrai et le faux si difficile qu'elle représente des risques alarmants pour la légitimité des informations partagées en ligne, favorisant la diffusion sur Internet d'informations erronées ou déformées qui contribuent à la création de théories du complot pour manipuler les populations à des fins politiques (Naffi et *al.*, 2021).

Les experts prédisent que ces *deepfakes* seront utilisés pour « la cyberintimidation, la destruction de réputations, le chantage, la diffusion de discours haineux, l'incitation à la violence et la perturbation des processus démocratiques (Maras et Alexandrou, 2019) ainsi que pour la cybercriminalité et les fraudes (Stupp, 2019) » (Naffi et *al.*, 2021 : 5). Rendant presque impossible la distinction entre le vrai et les faux, ces *deepfakes* représentent une véritable menace pour la légitimité des informations en ligne (Agence Allemagne-Presse, 2019).

Les solutions pour contrôler les *deepfakes* peuvent se regrouper en famille de :

> « [quatre] grandes catégories d'interventions :
> 1) les réglementations et les actions législatives ;
> 2) les politiques et la gouvernance des plateformes ;
> 3) les outils technologiques ;
> 4) l'éducation aux médias et à la citoyenneté numérique » (Naffi et *al.*, 2021 : 8).

2.3.8. Trollage ou *Trolling*

Une étude effectuée par l'entreprise McAfee (2022) révèle également d'autres formes de cyberintimidation telles que le « *trolling* », ce qui revient à « instiguer volontairement un conflit pour son propre amusement » ainsi que le « *doxing* », qui se caractérise par la révélation publique « des informations permettant de trouver quelqu'un, comme son nom, son adresse ou son école » (Descurninges, 2022).

Un *troll* est un terme faisant référence à une personne malveillante et nuisible, qui cherche à provoquer des conflits. Ce genre de personne souhaite porter des préjudices, « notamment à travers la perturbation d'un espace d'expression tel que les forums ou les réseaux sociaux, en particulier Facebook et Twitter » (JDN, s.d.). On retrouve ces *trolls* dans les sections des commentaires des plateformes.

Ces *trolls* ont tendance à envoyer des messages incendiaires sur les réseaux sociaux numériques, dans l'intention de provoquer des fortes réactions émotionnelles de la part d'autres personnes et d'orienter la conversation hors du sujet initial (Vann, 2020). En effet, ce genre d'individu cherche à semer la discorde au sein des groupes de discussions sur les réseaux sociaux, « diviser pour mieux régner » est sa devise (JDN, s.d.).

Ce type d'internaute souhaite exacerber les différences d'opinions, il peut même parfois agir simultanément sur de nombreux comptes de réseaux sociaux (JDN, s.d.). Les trolls affichent certaines caractéristiques qui nous permettent de les reconnaître (JDN, s.d.) :

- « Ils ne supportent pas la contradiction et ont toujours raison.
- Ils sont égocentriques et le traduisent par une forte propension à la victimisation.
- Ils sont lâches : sous couvert de l'anonymat, ils estiment pouvoir faire tout et n'importe quoi derrière leur écran et leur clavier.
- Ils possèdent un caractère aigri nourri par une grande frustration. Cela se voit dans leurs attaques, principalement fondées sur l'affect et non sur des arguments valables : les attaques *ad hominem* sont fréquentes pour ceux qui dialoguent avec lui.

- Ils envahissent la conversation de leurs publications et n'arrêtent pas de poster de nouvelles contributions tant qu'ils ont des réponses ».

2.3.9. Divulgation malveillante d'informations personnelles ou *Doxing*

Le *doxing* est une forme de cyberintimidation qui se traduit par la divulgation de données personnelles. Il s'agit d'une pratique qui consiste à divulguer sur Internet des informations sur l'identité et la vie privée d'un individu dans l'intention de le nuire. Ce genre d'informations peut être son adresse, le détail de son identité, son numéro de sécurité sociale, son numéro de compte bancaire, etc. (Wikipédia, 2023).

Le terme « *doxing* » est apparu pour la première fois dans les années 1990 lorsque des pirates informatiques ou « hackers » ont commencé à exposer des documents sur des personnes qui se cachaient derrière de faux noms. De cette façon, ces pirates pourraient en exposer d'autres avec lesquels ils étaient en concurrence (Fortinet, 2023).

2.3.10. Surpartage parental ou *Sharenting*

Le *sharenting* se définit par la « sur-exposition des enfants sur les réseaux par les parents », le mot « *share* » signifie partager et le mot « *parenting* » signifie « paternité » (Gutiérrez, 2022). Cette pratique vise les parents qui affichent des photos de leurs enfants sur les réseaux sociaux. Cela peut avoir des conséquences néfastes à l'égard des enfants qui se retrouvent excessivement sur les réseaux sociaux. Les enfants ne sont pas assez formés et sensibilisés pour « faire face aux conséquences de l'exposition devant un monde entier de spectateurs de tout type » (Gutiérrez, 2022).

2.3.11. Partage non consenti d'images intimes ou *Nudes*

Avec l'évolution des nouvelles technologies et l'utilisation de plus en plus fréquente, l'envoi de *nudes* fait partie des nouvelles pratiques sexuelles qui inquiètent. Les *nudes* sont des médias exposant un ou plusieurs corps nus ou partiellement dénudés ou sexualisés. Un *nude* peut être pris par soi-même ou par une autre personne. Ce *nude*

peut être partagé, selon une étude, par soi-même, ce qu'on qualifie de partage primaire, ou il peut être partagé par le transfert de l'image par une personne, ce qu'on qualifie de partage secondaire (Blécot et *al.,* 2022 : 148).

Cette étude s'intéresse aux échanges de photos et vidéos chez les jeunes de 13 à 25 ans de France et de Belgique. L'échantillon sur lequel a été effectué l'étude est de 10 700 participants, dont 7.545 sont des femmes et 3.155 sont des hommes (Blécot et *al.,* 2022 : 150). Pour ce qui est du partage primaire, l'étude a démontré que 74.50 % des participants avouent avoir déjà envoyé un ou des *nude(s),* les proportions de ce pourcentage sont semblables autant chez les filles que chez les garçons.

Les chances d'envoyer des *nudes* augmentent également avec l'âge, plus on est vieux et plus on aurait tendance à partager ce type de contenu (Blécot et *al.,* 2022 : 150).

En ce qui a trait au partage secondaire, 19,6 % des participants de cette étude qui ont reçu des *nudes* de leur partenaire déclarent avoir conservé au moins certains de ces *nudes* après une rupture. Cette tendance s'observe davantage chez les hommes (33,45 %) que chez les femmes (13,86 %). Ajoutons aussi que plus de la moitié des répondants à cette étude ont affirmé qu'on leur a déjà envoyé le *nude* d'une autre personne, cela arrive davantage chez les hommes (53.78 % contre 42.38 % pour les femmes) (Blécot et *al.,* 2022 : 151).

Les conclusions de cette recherche révèlent que l'échange de *nudes* fait partie intégrante de la sexualité des jeunes hommes et des jeunes femmes. Le partage primaire semble toutefois concerner un plus grand nombre de jeunes (Blécot et *al.,* 2022 : 151). En effet, il a été démontré que le partage primaire était majoritairement une pratique de couple. Le partage secondaire, en revanche, est rarement désiré. Davantage d'hommes que de femmes avouent avoir reçu des *nudes* d'un partage secondaire et davantage de femmes que d'hommes affirment avoir été « victimes ou avoir été menacé de partages secondaires non consentis » (Blécot et *al.,* 2022 : 153).

Le grooming comme prolongement des Nudes

Cette normalisation des Nudes augmente également les cas de grooming en ligne, ou « cyberprédation », une forme de manipulation psychologique utilisée par des individus pour exploiter les jeunes à des fins sexuelles (Kmetrix, 2024). Sur Discord, les prédateurs profitent des fonctionnalités de la plateforme, telles que les serveurs et les messages privés, pour se faire passer pour des amis ou des personnes bienveillantes partageant des intérêts communs, et ainsi gagner la confiance des adolescents (Cybertip.ca, 2023). Selon des enquêtes, des adultes ont utilisé Discord pour manipuler, exploiter ou agresser sexuellement des mineurs. Certains cas ont mené à des poursuites judiciaires pour diffusion de contenu à caractère sexuel impliquant des enfants, soulignant les risques persistants liés aux interactions sur cette plateforme (Goggin, 2023). Ces pratiques débutent souvent par des échanges anodins, mais évoluent vers des demandes explicites d'images ou de vidéos compromettantes, obtenues sous la menace ou par des promesses de relations privilégiées (RAINN, 2020). Discord, initialement conçu comme un outil de communication pour les joueurs, a vu émerger des serveurs de rencontres pour adolescents. Ces espaces, en raison de l'absence de vérification stricte de l'âge, attirent fréquemment des prédateurs qui exploitent la vulnérabilité des jeunes utilisateurs, amplifiant ainsi les risques de grooming et de sextorsion (Ichi.pro, 2024 ; Cybertip.ca, 2023).

2.3.12. Humiliation sexiste ou *Slutshaming*

Le *slut-shaming* est un

> [néologisme] composé des mots anglais slut (salope) et shame (honte) désigne le fait de critiquer, stigmatiser, culpabiliser ou encore déconsidérer toute femme dont l'attitude, le comportement ou l'aspect physique sont jugés provocants, trop sexuels ou immoraux. Les attaques peuvent être physiques ou morales et elles entretiennent l'idée que le sexe est dégradant pour les femmes (CSF, sd).

Le *slut-shaming*, qui signifie « stigmatisation des salopes », se produit quand une femme se fait « rabaisser ou culpabiliser » en raison de ses pratiques sexuelles (nombre de partenaires, vêtements « provocants » (Dylan, 2017). Par exemple, « c'est votre camarade de classe qui raconte à tout le monde qu'une telle est « une vraie salope » parce que c'est elle qui l'a dragué pour qu'elle finisse dans son lit. C'est votre copine qui dit que cette fille est une pute parce qu'elle coucherait avec n'importe qui » (Dylan, 2017).

2.3.13. Cyberfilature ou *Cyberstalking*

Ce phénomène de cyberviolence « [désigne] l'acte de suivre les activités en ligne d'un autre internaute, dans le but de récolter des informations personnelles à son sujet » (Begin, 2016 : 28).

2.3.14. Propos incendiaires ou *Flaming*

Ce phénomène de propos incendiaire ou Flaming

> [désigne] un échange bref et enflammé entre deux ou de nombreux jeunes, généralement dans un espace en ligne qui est public, comme des salles de clavardage (chat rooms) ou des forums de discussion, autour d'un sujet quelconque, mais qui amène les jeunes à s'insulter l'un et l'autre. La flingue est moins marquée par un déséquilibre de pouvoir que le harcèlement (Begin, 2016 : 27).

2.3.15. Dénigrement ou *Denigration*

Le dénigrement

> [désigne] la publication en ligne, sur une page web ou un média social par exemple, d'informations dérogatoires et fausses au sujet d'une personne ou des images montrant une représentation négative d'elle, généralement dans le but de nuire à sa réputation » (Begin, 2016 : 28).

2.3.16. Vol d'identité ou *Impersonation*

Le vol d'identité

> [désigne] l'acte de se faire passer pour une autre personne en ligne en faisant usage de son mot de passe et de son profil dans un média social, généralement dans le but de nuire à sa réputation (Begin, 2016 : 28).

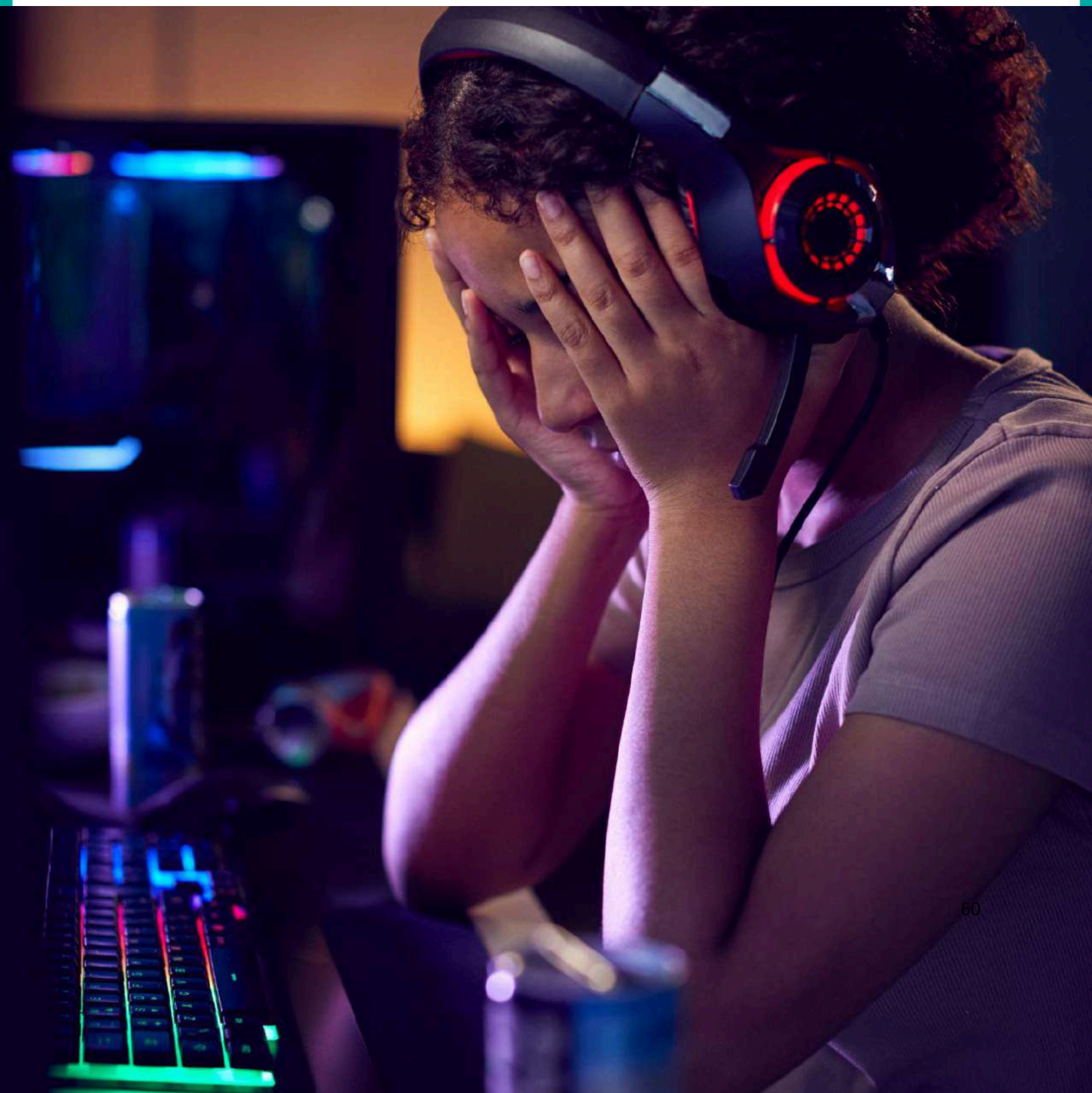
2.3.17. Incitation au dévoilement ou *Outing and Trickery*

Le *Out and Trickery,* c'est ce que l'on nomme l'incitation au dévoilement ou le dévoilement d'informations personnelles d'une autre personne, « il désigne le partage d'informations personnelles et/ou de photos embarrassantes à propos d'une personne par renvoi de messages à plusieurs personnes » (Begin, 2016 : 28).

2.3.18. Exclusion ou *Ostracism*

Ce phénomène

> [désigne] l'exclusion de certains jeunes dans différents environnements, dont les jeux en ligne ou les forums de discussion, notamment par la mobilisation de certaines stratégies techniques de blocage d'accès (Begin, 2016 : 28).



3. Impacts et prévention de la Cyberintimidation

> *Un groupe d'élèves du collège a créé un faux compte Facebook au nom de ma fille et publie des contenus désobligeants en son nom*... (MENJ, 2011 :7)

La cyberintimidation peut avoir des répercussions sur plusieurs aspects de la vie des personnes qui en sont les victimes (Hackett, 2016). En effet, les enfants et adolescents qui ont des outils technologiques à leur portée sont joignables en tout temps, ils sont donc susceptibles de faire l'objet d'attaques à n'importe quel moment de la journée, que ce soit après l'école ou durant le week-end (Hackett, 2016).

La cyberintimidation peut conduire les jeunes victimes à

> [En effet, c'est une] faible estime de soi, l'isolation et l'éloignement de la famille, la réticence à laisser des adultes ou des membres de la famille chercher leurs outils technologiques, la recherche d'excuses afin de ne pas se rendre à l'école et même le refus total d'y aller, la perte de poids ou le changement d'apparence afin de faire partie du groupe, la présence de plaies d'auto-mutilation sur le corps et un changement dans l'humeur et dans la personnalité comme les excès de colère, la dépression et l'isolement (Family Lives, 2021).

Selon l'UNICEF (United Nations International Children's Emergency Fund), les personnes victimes de cyberintimidation peuvent se sentir honteuses, humiliées, angoissées et soucieuses de ce que le monde pense d'elles (Hackett, 2016). En raison d'attaques répétées, elles peuvent perdre leur motivation et leur intérêt pour des activités qu'elles appréciaient auparavant, ce qui peut entraîner une détérioration de leur santé mentale (Hackett, 2016).

3.1. Impacts à court ou moyen terme

Une personne peut être la cible de gestes de cyberintimidation en tout temps et partout, à l'école comme à la maison et ces attaques peuvent être effectuées souvent sous le sceau de l'anonymat et sans que cette personne ne puisse nécessairement se défendre (INSPQ, 2023).

Les répercussions sur les victimes peuvent inclure

> [En effet, c'est la consommation] de drogue et d'alcool, l'automutilation, les symptômes dépressifs et la dépression, la diminution de la confiance et de l'estime de soi, les comportements d'isolement social, les comportements agressifs, l'absentéisme scolaire, les problèmes de comportements, les problèmes émotionnels, le stress, l'anxiété sociale, le suicide ou les idées suicidaires, la détresse psychologique, etc. (INSPQ, 2023).

Par ailleurs, il en est de même pour le cyberharcèlement. Plusieurs études démontrent que cette forme de cyberviolence a aussi des impacts « sur le bien-être et la santé mentale des victimes ». Voici une liste non exhaustive de ses conséquences :

- « [une] faible **estime de soi** ;
- des répercussions sur le cheminement scolaire (absentéisme répété, **manque de concentration** ou difficultés de raisonnement) ;
- des troubles psychiques et de la **détresse émotionnelle** (stress, troubles alimentaires, sentiment de colère ou de frustration dû à l'anonymat de l'agresseur ou au sentiment d'impuissance, troubles du sommeil, anxiété, état dépressif, etc.) ;
- Un sentiment d'insécurité, de **culpabilité** et de honte ;
- Un **isolement social** vis-à-vis de la famille et des ami-e-s ;
- Des **idées suicidaires** et/ou tentatives de suicide » (SCF, 2016 :12).

Illustration de l'impact du Shareting sur les enfants

Divers impacts, à court ou à long terme, du *Shareting* (partage en ligne) sur les enfants sont identifiés (Gutiérrez, 2022). C'est pourquoi les parents et éducateurs doivent demeurer vigilants face à plusieurs pratiques numériques susceptibles d'accroître le risque d'exposition des jeunes au Shareting. Il est par exemple, important de prévenir la mise en contact des enfants avec des individus aux intentions moins bienveillantes « que celles d'un membre de la famille ou d'un ami » (Gutiérrez, 2022). Malheureusement, ce risque est fréquent sur Internet, et il est recommandé de prendre des mesures afin d'éviter que nos enfants ne deviennent le centre d'attention de ces personnes.

Par ailleurs, à mesure qu'ils grandissent, les enfants peuvent ressentir de l'embarras face à certaines photos publiées par leurs parents ou leurs proches sans l'obtention de leur consentement. Cette pratique soulève des questions sur le respect de la vie privée, le consentement des enfants, et les conséquences potentielles de ces publications à long terme.

Enfin, en matière d'éducation des enfants pour une utilisation appropriée et responsable des réseaux sociaux, il est essentiel, en tant que parents et éducateurs, de réfléchir aux apprentissages liés à la gestion de leur présence en ligne et à la bonne utilisation des outils numériques, en particulier lorsqu'ils sont sensibilisés dès leur plus jeune âge à « un modèle de sur-exposition » (Gutiérrez, 2022).

3.2. Modèles préventifs

> *L'une de mes élèves a été accusée d'avoir insulté sur Facebook ses camarades de classe. Or, celle-ci n'avait plus accès à son compte. Elle a découvert que son compte Facebook avait été piraté par une personne malintentionnée* (MENJ, 2011 :7)

Dans le « cybermonde », les jeunes développent des « espaces numériques de médiation » (Alava, 2018) pour tenter de lutter contre diverses formes de violence numérique, telles que le cyberharcèlement, la « cyberviolence sexiste » et le « cybersexisme » (Niang et Nagem, 2018). Ces initiatives, fondées sur une communication horizontale entre pairs, de « jeunes à jeunes », représentent des approches novatrices contribuant à atténuer l'impact de ces violences. Par ailleurs, ces déploiements sur les réseaux a encouragé l'émergence de nouvelles figures, telles que les « veilleurs citoyens », les « médias pure players » et les « journalistes citoyens » (Alava, 2018), mettant en lumière l'importance du déploiement de modèles préventifs pour garantir un écosystème numérique responsable et éthique. Dans cette section nous proposons de survoler diverses approches de prévention de la cyberintimidation.

3.2.1. Diverses approches

Au cours des dernières années, diverses approches de prévention de la cyberintimidation ont été mises en œuvre, certaines d'entre elles sont abordées dans l'étude "*Approaches to Automated Detection of Cyberbullying : A survey*" (Salawu et *al.*, 2017).

- ***L'approche Lexicon***

Développée par Pérez et *al.* (2012) et Fahrnberger et *al.* (2014), cette approche préventive met en place un système appelé MISAAC conçu pour détecter du contenu cyberintimidation dans les messages instantanés. Les messages sont d'abord traités par

un analyseur lexical et comparés avec des schémas d'agressivité établis dans un module d'analyse de contenu. Un système de contrôle par couleur permet alors d'identifier les propos allant du rouge, au jaune puis au vert, comme une échelle mesurant les niveaux d'agressivité dans les messages.

- ***L'approche Rule-Based***

Serra et Venter (2011) proposent un système de détection pour identifier les enfants à risque de subir de la cyberintimidation en examinant leurs habitudes d'utilisation de leur téléphone portable en lien avec les activités de cyberintimidation. Chen *et al.* (2012) ont incorporé des fonctionnalités telles que l'historique de conversations et le style d'écriture et de messagerie dans le développement de leur cadre syntaxique lexical (*Lexical Syntactic Framework*). En utilisant ce type de fonctionnalités lexicales et syntaxiques, le système détecte et analyse les phrases de commentaires compromettantes sur YouTube (Salawu et *al.* 2017).

- ***L'approche Mixes-Initiative***

Une telle approche permet de détecter les messages d'intimidation fait de manière indirecte en implantant un mécanisme de détection de raisonnabilité dans un système de détection (Salawu et *al.* 2017). Ce système de détection a regroupé un ensemble de 200 affirmations sous forme de phrase, converti en un schéma appelé le *BullySpace Knowledge base* mettant en relation certains messages avec des affirmations.

Par exemple, la phrase « *es-tu parti magasiner des rouges à lèvres avec ta mère ?* » adressé à un homme hétérosexuel sera reliée à l'affirmation « *le rouge à lèvres est utilisé par les filles* », ainsi ce type de message sera automatiquement signalé comme une forme de cyberintimidation implicite, caractérisée par des propos homophobes (Salawu et *al.* 2017).

- ***L'approche par agents normatifs***

Bosse et Stam (2011) ont instauré une intervention visant à contrer la cyberintimidation en introduisant plusieurs agents normatifs dans un environnement virtuel. Ces agents sont chargés de surveiller et enregistrer les activités des utilisateurs dans le monde virtuel (Salawu et *al.* 2017). Ils utilisent un système de récompenses et de punitions pour imposer le comportement souhaité aux utilisateurs. Chaque utilisateur se voit attribuer un score de réputation en fonction des comportements observés (Salawu et *al.,* 2017).

- ***L'approche de l'Institut national de santé publique du Québec***

L'Institut national de santé publique du Québec (INSPQ, 2023) recommande de favoriser une approche positive et globale pour lutter contre la cyberintimidation. Il faut mettre en place des interventions.

> [En effet, en visant] à agir directement sur les contextes relationnels, communautaires ou sociétaux ou visant à agir sur certains facteurs de risque ou de protection qui auront un impact sur les différents contextes (INSPQ, 2023).

Cette approche impliquerait de modifier et d'organiser la vie scolaire « dans le but d'offrir un milieu de vie stimulant et soutenant tous ceux qui s'y trouvent » et « d'améliorer la qualité de vie » des jeunes en favorisant « l'acceptation des différences » et en évitant « certains comportements problématiques en créant des opportunités d'apprentissages multiples et stimulantes » (INSPQ, 2023). Il est aussi possible de mettre en place des interventions préventives en ciblant spécifiquement la cyberintimidation, par exemple, « à travers l'enseignement de l'utilisation saine et sécuritaire des technologies de l'information et des communications ». Aussi, puisque le fait de commettre des gestes d'intimidation se révèle être un facteur de risque de cyberintimidation, « les programmes visant la prévention de l'intimidation peuvent aussi contribuer à prévenir la cyberintimidation » (INSPQ, 2023).

3.2.2. Rôle des parents ou éducateurs

Avec l'essor des technologies numériques et de l'IA, les jeunes courent un risque accru d'être victimes de « criminalité informatique » (PPC, 2022). Cependant, restreindre l'accès au numérique n'est pas une solution appropriée. L'objectif est de trouver un équilibre entre la vie privée et sociale en favorisant des interactions en ligne sécurisées.

> Il revient aux adultes de discuter avec leurs enfants afin de prévenir les problèmes reliés à la cyberintimidation. Les parents devraient également savoir reconnaître et identifier les signes de cyberintimidation et être à l'écoute de leurs enfants. Il est aussi conseillé aux parents d'apprendre à leurs enfants à s'affirmer, pour qu'ils sachent quand dire « ça suffit », « stop » ou « c'est assez » (PPC, 2022).

Chehab et *al.* (2016) suggèrent une intervention directe des parents afin de lutter contre la cyberintimidation. Cependant, comment un éducateur ou un parent peut-il déterminer qu'il a atteint « le juste milieu » (Capeluto, 2023) de cette prévention ? En effet, la mission des parents pour prévenir les risques de cyberintimidation auxquels leurs enfants pourraient être confrontés est difficile. Ils doivent constamment superviser les activités en ligne de leurs enfants afin de les protéger contre ce fléau (DOP, s.d.).

Une approche efficace pour surveiller l'accès à Internet des enfants consiste à établir des limites à leur utilisation en ligne, en restreignant les activités autorisées et en limitant l'accès à Internet en cas de non-respect de ces règles (DOP, s.d.). De plus, l'utilisation des paramètres de confidentialité, des contrôles parentaux et des fonctionnalités de sécurité Internet intégrées offertes par de nombreux fournisseurs de services Internet est également préconisée (DOP, s.d.).

Par ailleurs, il est essentiel que les parents discutent avec leurs enfants des raisons qui sous-tendent les limites d'âge imposées par les réseaux sociaux, généralement fixées à 13 ans. Expliquer que l'accès précoce à ces plateformes peut exposer les enfants à des risques de cyberintimidation et à d'autres actes indésirables est primordial.

Il convient également de créer un environnement où les enfants se sentent à l'aise pour partager leurs expériences en ligne. En engageant cette conversation, les parents peuvent mieux comprendre comment leurs enfants utilisent Internet, les réseaux sociaux et leurs téléphones portables. Sensibiliser les enfants à adopter un comportement responsable en ligne revêt une importance particulière, car il a été observé que ceux qui ont été victimes de cyberintimidation peuvent parfois se retrouver à perpétrer des actes similaires à l'encontre d'autres personnes (DOP, s.d.). Pour résumer, voici quelques recommandations pour encadrer la prévention de la cyberintimidation pour les parents.

- « **Offrir aux jeunes une éducation sur la cyberintimidation** » (Bouré et *al.*, 2022 : 22-23) : Le soutien et l'implication des parents sont cruciaux dans la prévention de la cyberintimidation. Il est recommandé d'engager des discussions avec l'enfant sur ses interactions sociales et de parvenir à un accord sur l'utilisation d'Internet. Il est également essentiel que les parents encouragent leurs enfants à solliciter l'aide d'adultes s'ils sont confrontés à des attaques en ligne.

- « **Parler des risques des réseaux sociaux** » (Capeluto, 2023) : Il est primordial d'engager une conversation avec les jeunes pour les sensibiliser aux risques des réseaux sociaux, sans toutefois adopter une approche alarmiste. Cette démarche vise à établir une relation de confiance qui encourage les jeunes à se confier à un adulte en cas de problème.

- « **Réglementer l'utilisation** » (Capeluto, 2023) : Il est suggéré de limiter le temps d'utilisation des réseaux sociaux, car un usage excessif d'Internet peut « entrainer des troubles du sommeil et du comportement, de l'anxiété ou de l'isolement » (Capeluto, 2023). Il est donc conseillé de superviser les activités en ligne de ses enfants et être au fait des indicateurs de cyberintimidation (Chehab et *al.*, 2016).

- « **Demander et écouter** » (Capeluto, 2023) : Il est fortement conseillé de favoriser une communication basée sur la confiance afin d'amener son enfant à se sentir en sécurité et avoir un espace pour exprimer ses émotions (Capeluto, 2023). Les parents doivent ainsi créer un environnement propice à la communication, encourageant ainsi leurs enfants à partager leurs expériences en ligne (MSP, 2009).

- « **Surveiller les signes de danger et s'impliquer si nécessaire** » (Capeluto, 2023) : Il est essentiel de surveiller et d'identifier les comportements inhabituels chez les jeunes afin d'adopter des mesures appropriées. Par exemple, si un jeune manifeste une "humeur instable sans raison apparente, s'il modifie sa manière de communiquer" (Capeluto, 2023), ou s'il refuse subitement d'aller à l'école, ou encore s'il présente de l'anxiété lorsqu'il utilise ses appareils numériques.

La recherche conduite par Zhu et *al.* (2021) préconise une approche éducative parentale caractérisée par un engagement élevé, une attention soutenue et un soutien constant pour réduire les risques d'implication des enfants dans la cyberintimidation. La « communication ouverte », en cas de difficultés, est soulignée comme un moyen efficace pour renforcer « le sentiment de sécurité » (Zhu et *al.*, 2021 :7). Ainsi, les parents sont encouragés à « être bienveillants », à maintenir une bonne communication et surveiller les activités de leurs enfants et « participer activement » à leur vie (Zhu et *al.*, 2021 :7). En cherchant « un équilibre entre le contrôle et l'ouverture », une communication transparente peut aider les parents à « parvenir à un accord avec leurs enfants sur l'utilisation des ordinateurs et téléphones intelligents » (Zhu et *al.*, 2021 :7).

Le Conseil aux parents : A-M-OU-R

Les parents doivent manifester de l'amour envers leurs enfants, car ceux qui bénéficient d'un fort soutien parental sont moins enclins à être victimes de cyberintimidation (Fanti et *coll.*, 2012).

- **A**ssurer d'écouter son enfant : Encourager l'enfant à s'exprimer sans porter de jugement afin de maintenir des lignes de communication ouvertes. Éviter les menaces de retirer son téléphone ou de le priver d'Internet.
- **M**ontrer un appui à l'enfant et se porter à sa défense : Travailler en collaboration avec l'enfant pour recueillir les courriels ou messages liés à la cyberintimidation, susceptibles d'être signalés à la police ou à un fournisseur Internet. En cas d'implication d'une personne de l'école, il est recommandé, en concertation avec l'enfant, de décider de signaler les incidents de cyberintimidation à l'enseignant ou au directeur.
- **Ou**vrir la porte aux sentiments de l'enfant et les valider : Informer l'enfant que ressentir certaines émotions, telles que la tristesse ou la peur, est une réaction normale, encourageant ainsi l'expression de ces sentiments
- **R**echercher des ressources ensemble (Sécurité publique, 2015)

« Être parents »

Le site Internet *« Être parents »* offre des recommandations précieuses aux parents concernant le *Shareting* pour contrer ce phénomène croissant (Gutiérrez, 2022).

- « **Essayez de ne partager d'informations sur la routine de vos enfants**. Ne publiez pas le lieu où vous vivez ou où ils réalisent leurs activités extra-scolaires.
- **Ne publiez pas de photos de vos enfants nus ou peu vêtus.** Bien que cela semble logique, les photos à la plage ou à la piscine montrent nos enfants en maillot de bain. Nous ignorons comment s'en serviront d'autres photos.
- **Prenez des photos avec des vêtements de rue.** Si nous publions des photos de nos enfants avec leur uniforme d'école -le cas échéant, il sera plus facile d'identifier l'école dans laquelle ils se trouvent.
- **Ne publiez pas de plaques d'immatriculation, l'adresse de votre maison** ou quelconque autre information qui peut être personnelle sur votre famille ». (Gutiérrez, 2022).

3.2.3. Rôle des établissements scolaires

Chehab et *al.* (2016) proposent l'adoption d'« une approche de prévention universelle », selon laquelle il faut sensibiliser les élèves et les aider à développer des compétences sociales leur permettant de bâtir des liens positifs et d'interagir sainement les uns avec les autres, ce qui laisse place à la création d'un climat scolaire positif ou les élèves pourront s'épanouir. Certaines interventions effectuées individuellement auprès d'élèves qui se sont fait intimider se sont également avérées efficaces. C'est par exemple :

- Instruire l'élève victime sur la manière de **s'affirmer de manière positive** afin de prévenir l'aggravation de situations tendues en des dynamiques d'intimidation.
- Offrir à l'élève victime la possibilité d'établir des liens avec « **des pairs prosociaux** », susceptibles de dissuader les intimidateurs.
- Collaborer avec la **famille de la victime** pour renforcer sa sécurité en ligne en dehors des heures de cours (Chehab et *al.*, 2016, cit. Pearce et coll, 2011).

Climat scolaire

L'éducation des jeunes concernant la cyberintimidation, comme suggéré par Bouré et *al.* (2022 : 22-23), demeure essentielle pour les éducateurs. Il est fortement recommandé de développer et d'intégrer des programmes d'intervention éducative, mais aussi de former le personnel pour prévenir les cyberviolences dans les établissements scolaires.

Ces programmes visent à sensibiliser les enfants à la problématique de la cyberintimidation, tout en les informant sur les ressources disponibles en cas de confrontation à une telle situation. Cette approche proactive du corps professoral peut jouer un rôle significatif dans la prévention et la gestion de la cyberintimidation ou toute forme de cyberviolence au sein de l'environnement éducatif.

« Les cyberviolences peuvent contribuer à dégrader le climat scolaire ; et un climat scolaire dégradé peut favoriser l'apparition de violences et de cyberviolences. Ce lien à double sens peut conduire à mettre en place une démarche d'amélioration du climat scolaire dans l'école ou l'établissement, telle qu'elle est présentée sur le site **Climat scolaire**. Cette démarche repose sur sept piliers :

- stratégies collectives ;
- apprentissages, pédagogie, relation éducative ;
- justice en milieu scolaire ;
- prévention et gestion des violences et du harcèlement ;
- coéducation ;
- environnement partenarial ;
- qualité de vie et bien-être à l'École » (MENESR, 2016 : 17).

Éducation critique des médias

L'éducation numérique et aux médias des jeunes se révèle incontournable pour « développer leur pensée critique et favoriser leur agentivité » (Naffi et *al.*, 2021 : 11). Une telle éducation pourrait encourager des comportements stratégiques pour contrer la désinformation, notamment face aux *Deepfakes* qui se développent de plus en plus, surtout avec les nouveaux développements de l'intelligence artificielle (IA).

Dans des pays comme le Danemark ou la Finlande, les programmes scolaires proposent une éducation critique des médias qui favorise « la résilience de leurs jeunes à l'égard de la désinformation » (Naffi et *al.*, 2021 : 11).

En France, c'est une éducation transversale aux médias et à l'information (EMI) qui est adoptée. L'EMI initie les élèves « à des notions comme celles d'identité et de trace numérique, dont la maîtrise sous-tend des pratiques responsables d'information et de communication » (MENESR, 2016 : 22). Grâce à ce type d'apprentissage, les jeunes apprennent à repérer les formes de désinformation, mensonges, ou tromperies sur le Web (Naffi et *al.*, 2021 : 11).

Solution numérique

« La création d'une interface » ou d'une application constitue une réponse innovante à la problématique de la cyberintimidation. Cette interface offre aux élèves la possibilité de signaler anonymement leur harceleur en fournissant des preuves tangibles telles que des captures d'écran de conversations, des publications sur les réseaux sociaux, ou des messages intimidants dirigés vers la victime : « les photos de conversations, les publications sur les réseaux sociaux, les propos haineux ou intimidants mentionnés » (Bouré et *al.*, 2022 : 24-25).

Une fois la dénonciation effectuée, le personnel scolaire pourrait être alerté par l'application et sera chargé de mettre en œuvre des interventions en classe afin de résoudre le problème et sensibiliser les élèves aux « dangers de la cyberintimidation », soulignant les impacts négatifs associés à ces agressions. À titre d'exemple, « les chercheurs Ryan et Smith-Moncrieffe (2017) » ont développé une plateforme baptisée « STOPit », une initiative concrète pour dénoncer les « actes de cyberintimidation » (Bouré et *al.*, 2022 : 24-25). Pour finir, la recherche de Zhu et *al.* (2021) insiste sur l'importance pour les écoles de créer un environnement éducatif positif et sécurisé pour assurer une égalité de traitement pour chaque élève.

En favorisant un tel environnement, les élèves peuvent se concentrer davantage sur leurs études, améliorer leurs performances scolaires et développer un fort sentiment d'appartenance à l'école. Mettre en avant « les valeurs de la collectivité entre étudiants » peut participer à réduire les risques de cyberintimidation, que ce soit du côté des agresseurs ou du côté des victimes.

De plus, la collaboration des écoles « avec des agences ou des organismes de santé mentale » est préconisée pour élaborer « des programmes de prévention », en intégrant « des activités parascolaires et des formations ». Il est nécessaire d'ajuster ces « mesures préventives en milieu scolaire » en fonction des différentes classes d'âge des jeunes.

Le développement de « politiques scolaires » favorisant « la diversité » et incarnant « le respect mutuel entre étudiants » est recommandée afin de promouvoir un climat scolaire positif et inclusif (Zhu et *al.* 2021 : 9).

4. Initiatives internationales

De nombreux gouvernements ont adopté différentes « approches, plans d'action et politiques » au sein du système scolaire afin de contrer le phénomène de la cyberintimidation (Gottschalk, 2022). Différents programmes et initiatives sont déployés dans de nombreux pays pour contrer la cyberintimidation et les cyberviolences en général. Certains ont été développés et implantés dans des pays de l'OCDE (Gottschalk, 2022). Il s'agit, par exemple, d'interventions qui permettent d'améliorer les relations des étudiants entre eux et aussi des approches qui comprennent de la psychoéducation, du matériel multimédia, des formations pour les parents et pour les enseignants (Gottschalk, 2022).

4.1. Initiatives québécoises

Un Plan d'action concerté pour contrer l'intimidation et la cyberintimidation (2020-2025) est déployé par le ministère de la Famille du Québec. Ce Plan d'action préconise quelques mesures à respecter en milieu scolaire afin d'« offrir un climat sain, sécuritaire et positif aux jeunes » (MFA, 2021 : 23 – Orientation 2). Il recommande aussi de :

- « **Accompagner les établissements scolaires** dans l'élaboration de lignes directrices pour baliser les interventions et les responsabilités relatives à l'utilisation éthique du numérique » (MFA, 2021 : 23)
- « **Soutenir les apprentissages** sur l'utilisation responsable des médias sociaux et des technologies chez les jeunes pour les amener à devenir des citoyens et citoyennes responsables à l'ère du numérique » (MFA, 2021 : 23).

Par ailleurs, il énonce plusieurs mesures pour « intensifier les actions pour réduire la cyberintimidation » (MFA, 2021 : 18 – Orientation 1). Cette orientation totalise un budget de 2.5M$ (MFA, 2021) afin de porter ces mesures soutenues par plusieurs ministères.

- « Soutenir la mise en place d'un **modèle d'intervention concertée** entre les milieux policier, judiciaire et scolaire en cas de cyberintimidation découlant d'incidents de partage non consensuel de photos intimes (SEXTO) » (MFA, 2021 : 19). Cette initiative sera soutenue par le Ministère de la Sécurité publique (MSP) avec un budget de 1.5M$.
- Le déploiement et la réussite de la mesure reposent sur une forte **collaboration** des services de policiers, le Directeur des poursuites criminelles et pénales (DPCP), les intervenant.e.s scolaires. Elle vise « de limiter la diffusion des images, de soutenir la victime, de prévenir d'autres incidents similaires ou de prendre les mesures qui s'imposent à l'égard des contrevenants et contrevenantes d'âge mineur, et permettra d'éviter les préjudices associés à un long traitement judiciaire et à la médiatisation qui en découle » (MFA, 2020, p. 19).
- « **Informer la population** sur les conséquences de l'hostilité en ligne visant les femmes, notamment celles qui prennent la parole dans l'espace public, et sur les recours légaux possibles pour les victimes » (MFA, 2021 : 19). La mesure est supportée par le Secrétariat à la condition féminine (SCF) avec un budget de 350 K$.
- « **Prévenir les situations** de demandes répétées et de partage non consensuel d'images à caractère sexuel ou intime chez les jeunes de 11 à 24 ans et intervenir de façon éthique dans ces situations » (MFA, 2021 : 20). Initiative soutenue par le ministère de l'Éducation (MEQ) et ministère de l'Enseignement supérieur (MES) avec un budget de 375K$.
- « **Étudier les facteurs de risque**, de protection et de prévention pour mieux prévenir la cyberintimidation auprès des personnes aînées » (MFA, 2021 : 20). Cette mesure est supportée par le ministère de la Santé et des Services sociaux (MSSS) avec un budget de 275K$.

Dans le cadre de l'Orientation 3: « Accroître les initiatives pour les personnes en contexte de vulnérabilité » (MFA, 2021 : 31), le Plan d'action recommande de déployer des campagnes de communication (affiches, capsules vidéo, etc.) afin de sensibiliser le grand public à la cyberintimidation (MFA, 2021).

Le gouvernement du Québec invite tous les établissements à respecter un Plan d'action de lutte contre l'intimidation et la violence (PALVI, 2018-2023) prévoyant de (CSS, s.d.) :

- renseigner les actes d'intimidation et de violence ;
- mettre en place des mesures de prévention pour contrer ces actes ;
- mettre en place des mesures pour encourager l'implication des parents ou éducateurs ;
- mettre en place des mesures pour soutenir ou encadrer un élève qui a été victime de ses actes, mais aussi une personne qui a témoigné de ses actes ou même l'auteur de ses actes ;
- proposer des processus facilitant le signalement de ces actes tout en respectant la confidentialité ;
- informer sur les actions à prendre si de tes actes sont rapportés ;
et enfin, formuler des sanctions.

Les directions de chaque établissement doivent s'assurer d'élaborer, de réviser annuellement et d'actualiser le PALVI afin d'assurer aux élèves un environnement sain et sécuritaire (**Annexe 3**). Ce sont essentiellement les policiers communautaires qui sont mobilisés en cas de violence ou intimidation. Depuis 2023, le ministère de l'Éducation (MEQ) a mis en place un *Plan de prévention de la violence et de l'intimidation dans les écoles* (2023-2028), visant à renforcer les efforts pour garantir le bien-être des jeunes tout au long de leur parcours scolaire. Ce Plan s'appuie sur quatre mesures préventives réparties en quatre axes suivants :

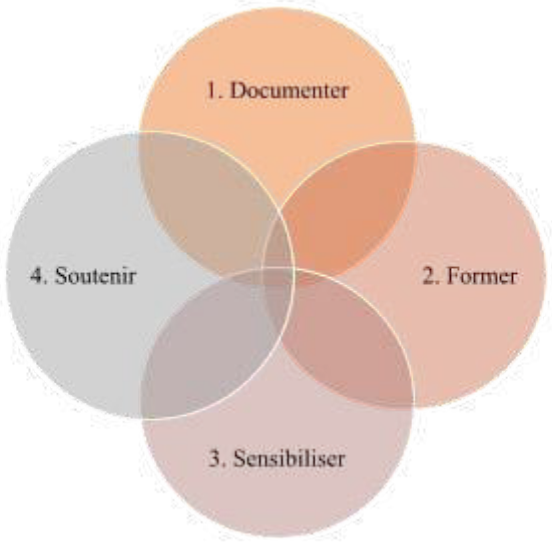


Figure 1. Quatre mesures préventives

Ces mesures consistent à assurer une analyse de ces phénomènes scolaires de violence et d'intimidation afin de mieux les prévenir et les combattre (1) ; à former les élèves à l'acquisition de « compétences sociales et personnelles » et émotionnelles, mais aussi à outiller les enseignants et le personnel scolaire afin qu'ils puissent accompagner leurs élèves à s'épanouir (2) ; à sensibiliser le plus grand nombre à la prévention de ces phénomènes (3) et enfin, à soutenir les écoles afin qu'elles deviennent des milieux d'épanouissement de bien-être en mettant en place par exemple « des équipes d'intervention » spécialisées, une « ressource professionnelle responsable de la coordination de la mise en œuvre des actions du Plan de prévention de la violence et de l'intimidation », « un modèle de plan de lutte contre l'intimidation et la violence » (4), etc., (Gouvernement du Québec, 2023b).

4.2. Initiatives américaines

Aux États-Unis, les politiques qui encadrent la gestion de la cyberintimidation au sein des écoles sont réglementées en fonction des États (Gottschalk, 2022). Par exemple, en Californie, les districts scolaires doivent avoir :

> [En effet, c'est une] déclaration officielle qui interdit l'intimidation ainsi que la cyberintimidation, des procédures d'enquête et de dénonciation d'actes de cyberintimidation, de la publication de lois contre la cyberintimidation, et de mettre en place des ressources disponibles pour soutenir les étudiants qui sont plus à risque de subir des actes de cyberintimidation, comme les étudiants issus de la communauté LGBTQI+, des protections en place pour ceux qui déposent des plaintes en crainte de représailles et de la nomination d'un agent de district responsable d'assurer la conformité du district aux exigences énoncés par la loi (Stop Bullying, 2021), (Gottschalk, 2022).

Par ailleurs, aux États-Unis, de nombreux États appliquent des sanctions, pénales ou scolaires, envers les auteurs d'actes de cyberintimidation (Gottschalk, 2022).

4.3. Initiatives australiennes

Le programme *Cyber Friendly Schools* (CFS), développé en Australie, adopte une approche socio-écologique et systémique. Cette approche tient compte de divers facteurs et niveaux, lesquels peuvent influencer la vulnérabilité de certains élèves face à la cyberintimidation (Gottschalk, 2022).

À travers des modules d'entraînement, des ateliers de ressources pour les familles, cette approche se concentre sur « la construction de la compréhension et la promotion des attitudes et comportements qui encouragent des comportements positifs dans l'environnement numérique tout en décourageant le cyberharcèlement » (Gottschalk, 2022, cit. Cross et *al.*, 2015).

Une autre initiative en Australie, le « *School Wellbeing Framework* », aide les écoles à créer des environnements inclusifs, encourage les comportements positifs entre élèves pour réduire le problème de la cyberintimidation et forme également des partenariats avec les familles (Burns and Gottschalk, 2019).

Pour finir, La loi australienne ***Online Safety Amendment (Social Media Minimum Age) Act 2024*** (Legislation.gov.au, 2024)., adoptée en novembre 2024, interdit l'accès aux réseaux sociaux pour les moins de 16 ans, une première mondiale visant à protéger les jeunes contre la cyberintimidation et les impacts négatifs des plateformes numériques (France24, 2024). Les entreprises disposent d'un an pour se conformer, avec une entrée en vigueur prévue en novembre 2025 (Forbes, 2024). Plusieurs pays envisagent de suivre l'exemple de l'Australie (Espagne, États-Unis, ...) (La Tribune, 2024).

4.4. Initiatives européennes

Internet Sans Crainte représente une initiative française de « sensibilisation des jeunes aux risques et enjeux d'Internet », intégrée dans le cadre du « programme *Safer Internet*

de la Commission européenne ». Ce programme, regroupant « 31 pays européens au sein du réseau Insafe », est une référence auprès des acteurs de l'écosystème de « l'éducation au numérique ». Son objectif principal est d'opter pour une sensibilisation de tous les jeunes « aux risques et usages d'Internet », en les encourageant à s'interroger de manière pertinente et à acquérir des réflexes adaptés aux situations parfois critiques. En parallèle, le programme vise à promouvoir des pratiques en ligne « plus sûres, citoyennes et créatives », tout informant et sensibilisant les « parents et enseignants » afin de les guider dans l'accompagnement des jeunes. De plus, le programme outille les « animateurs et enseignants » afin de leur permettre d'organiser aisément « des ateliers de sensibilisation et de création destinés auprès des jeunes » tout en offrant des formations aux professionnels (MENESR, 2016 : 25).

4.4.1. Initiatives autrichiennes

Le *Viennese Social Competence* (ViSC) est un programme qui a pour but de réduire les comportements agressifs de cyberintimidation, et de « favoriser les compétences sociales et interculturelles » (Gottschalk, 2022, cit. Gradinger et *al.*, 2014). Les enseignants sont formés pour reconnaître le harcèlement, mais aussi à la gestion de cas complexes et la mise en œuvre de mesures de prévention de l'intimidation à l'école et en classe (Gottschalk, 2022, cit. Strohmeier et *al.*, 2012).

Cette formation multimodale de prévention de la cyberintimidation, testée dans des établissements scolaires en Autriche et dans d'autres pays tels que l'Allemagne, Chypre et la Turquie, a pour objectif de responsabiliser des élèves de 5 à 14 ans. Elle les sensibilise aux comportements non-harcelants dans des situations de conflit, que ce soit en tant que victime, spectateur ou auteur. La réussite de ce programme expérimental dépend de l'implication des enseignants et du soutien du ministère de l'Éducation pour garantir des résultats positifs (EMCDDA, s.d.).

4.4.2. Initiatives françaises

« *Non au harcèlement* » est un site proposé par le Ministère de l'Éducation Nationale et de la Jeunesse français dans lequel on retrouve nombreuses ressources pour comprendre et contrer le cyberharcèlement ou la cyberviolence (MENJ, s.d.) : des campagnes de sensibilisation comprenant des vidéos réalisées chaque année avec des élèves, un programme Phare de prévention du harcèlement en milieu scolaire, un groupe Facebook « *Non au harcèlement à l'école* », et des canaux de signalement en ligne pour des contenus illégaux ou pour avoir recours à une intervention policière ou de la gendarmerie, etc. À titre d'exemple, un guide anti-cyberharcèlement a été élaboré en collaboration avec les associations e-Enfance, Net écoute, et Facebook.

net ecoute.fr

net ecoute.fr : Issu d'un partenariat institutionnel et associatif, le site **netecoute.fr** met à la disposition des enfants et des adolescents des informations sur la protection de leur vie privée et la sécurité sur Internet, sur les questions du harcèlement et des discriminations en ligne, sur les pratiques à risques, sur les moyens électroniques de communication et les jeux en ligne. Il met à disposition de tous des supports de sensibilisation et d'apprentissage. Ce site est également une plateforme de discussion avec des conseillers : par téléphone (0800 200 000 ou en demandant à être rappelé), par courriel, par chat, ou par Skype » (MENESR, 2016 : 32).

Pointdecontact.net

Pointdecontact.net est, depuis 1998, le service français de signalement en ligne, soutenu par la Commission européenne, permettant à tous les internautes de signaler par le biais d'un formulaire simple, anonyme et adapté aux terminaux mobiles, tout contenu choquant rencontré sur Internet. Point de contact est une initiative de l'Association

française des prestataires de l'Internet (AFPI), créée en 1997, qui regroupe fournisseurs d'accès Internet, hébergeurs, moteurs de recherche et plates-formes du Web 2.0 (MENESR, 2016 : 33).

Respect Zone

Respect Zone est une Organisation non-Gouvernementale française qui « se spécialise dans la prévention, l'encadrement et la prise en charge face aux cyber-violences, au cyber-harcèlement et à la haine en ligne » (Respect Zone, sd). Depuis 2014, cette organisation est principalement active en France, mais déploie également des activités en Suisse, Belgique, Italie, au Portugal et aux États-Unis (Respect Zone, sd). Respect Zone suit quatre missions principales (Respect Zone, sd) :

- La première est de produire des connaissances et de les partager, par exemple « mener des études sur les cyber-violences (harcèlement, haine, désinformation) et informer largement des causes et effets sur les individus et la société ».
- La seconde est de sensibiliser et former le public (familles, écoles, universités, entreprises, centres sportifs et culturels, associations, collectivités territoriales). Cela consiste à « ouvrir des espaces de discussion collective sur ces sujets et équiper d'outils pour prévenir et (ré)agir face aux cyber-violences ».
- La troisième porte sur l'« aide aux victimes : assister juridiquement les victimes de cyber-violences et se constituer partie civile dans les affaires liées à son objet social via son Cercle des Juristes ».
- Enfin la quatrième vise la plaidoirie soit de « porter ces sujets dans le débat public et participer à des chantiers législatifs en tant qu'auditeur avec des propositions pour « détoxer » l'espace digital (Internet, réseaux sociaux, metaverses…) ».

Pour se protéger des cyberviolences, la Charte « Respect Zone » peut être adoptée. Cette adhésion publique montre que l'internaute respecte l'autre et qu'il modère son contenu posté sur sa page Internet ou encore sur son mur dans les réseaux sociaux numériques (RSN). Cet engagement consiste à retirer tout contenu préjudiciable ou à

prendre ses distances envers des contenus haineux, racistes, homophobes, violents, sexistes, etc., publiés dans des espaces Internet partagés ou personnels.

Il est possible de télécharger le logo, un label, sur le site www.respectzone.org et de l'apposer sur sa page Facebook ou sur son site personnel, blog, etc., afin d'exprimer son intransigeance en matière de cyberviolence (MENESR, 2016 : 21).

Par ailleurs, le site labélisé par *Respect Zone* devra s'engager à respecter la charte de bonne conduite qui est disponible en plusieurs langues.

4.4.3. Initiatives allemandes

Le Programme *Mediehelden* a été élaboré en Allemagne dans le but de modifier les attitudes et les croyances tout en encourageant le développement des compétences sociales et numériques des élèves (Gottschalk, 2022). Les participants sont formés sur divers aspects de la cyberintimidation, incluant des définitions variées, des informations sur les aspects légaux et juridiques, ainsi que les impacts sur les victimes. De plus, ils apprennent à cultiver l'empathie les uns envers les autres (Gottschalk, 2022, cit. Schultze-Krumbholz et *al.*, 2016). Ce modèle intègre également des éléments d'apprentissage social tels que les jeux de rôle et l'apprentissage avec des éléments comportementaux tels que le renforcement positif (Gottschalk, 2022).

5. Des solutions technologiques

Les avancées récentes dans les nouvelles technologies et l'intelligence artificielle (IA) représentent des perspectives prometteuses pour prévenir la cyberviolence en ligne. Cependant, ces possibilités semblent applicables principalement dans les espaces numériques publics, tels que les réseaux sociaux, et non dans des environnements

comme les messageries instantanées, et ce, en raison de l'application des politiques de confidentialité des données.

> *Within the Natural Language Processing (NLP) community,in the past few years there have been severalefforts made to deal with the problem of online hatespeech detection, leading to the creation of a numberof datasets for hate speech detection in different languages,mainly containing messages publicly posted onTwitter (in which the level of interactivity among usersis very limited)* (Poletto et *al.*, 2021) » (Ollagnier and *al.*, 2022 : 2).

5.1. Centre de sécurité Facebook

Pour protéger sa communauté en ligne, Facebook a mis en place plusieurs mesures : « Contactez et signalez » (*fb.me/Reporting)* permet de signaler du contenu ou une personne ; choisir son audience permet de choisir les informations partagées et les personnes qui peuvent voir ces informations (fb.me/AudienceSelector) ; acceptez des invitations de personnes connues, ayant un vrai profil (fb.me/FriendRequests) ; retirer des personnes de sa liste d'ami.e.s sans que la personne n'en soit informée (*fb.me/Unfriending)* ; bloquer une personne, ce qui la retire immédiatement de votre liste d'ami.e.s, le blocage sera réciproque (fb.me/Blocking) ; signalez un problème à Facebook (Meta, s.d.).

Deepfake Detection Challenge

En 2019, Facebook a mis en place le *Deepfake Detection Challenge*, une initiative visant le contrôle de la désinformation par la création d'outils ayant pour fonction de détecter des « contenus médiatiques manipulés » (Naffi et *al.*, 2021 : 9). Des chercheurs proposent d'avoir recours à « la technologie de la chaîne de blocs (blockchain) pour déterminer la source d'origine et l'historique du contenu numérique » (Naffi et *al.*, 2021 : 9). Toutefois, ces « solutions technologiques de détection des *deepfakes* » (Naffi et *al.*, 2021 : 9) ne peuvent pas empêcher la circulation et le partage des *deepfakes*.

5.2. Application *BullStop*

L'application anti-cyberintimidation *BullStop* (BullStop, s.d.) sert à protéger les internautes des cyberintimidateurs et des trolls afin d'assurer un Internet sécuritaire (*safer Internet*). Ce sont des informaticiens de l'Université Aston de Birmingham qui ont mis en place cet algorithme d'intelligence artificielle (IA) pour lutter contre l'intimidation en ligne (Aston University, 2020). Conçue avec la collaboration de jeunes, cette application peut également servir aux adultes qui utilisent des médias sociaux, tels que Twitter, qui peuvent être propices aux attaques et aux abus (Aston University, 2020).

Bullstop permet de surveiller les profils de médias sociaux des utilisateurs et de rechercher les messages offensants ou désobligeants pour s'assurer que les utilisateurs ne les reçoivent pas (Aston University, 2020).

Cela est possible grâce à un algorithme d'intelligence artificielle (IA) conçu pour comprendre et décoder des messages écrits malveillants.

L'algorithme « analyse les messages et signale le contenu offensant comme les cas de cyberintimidation, le langage abusif, insultant ou menaçant, la pornographie et le spam » (Aston University, 2020). Testée sur plus de 60 000 tweets, cette application de détection de la cyberintimidation vise à identifier non seulement le langage abusif et offensant, mais aussi des formes plus subtiles d'intimidation telles que le sarcasme et l'exclusion, qui sont des méthodes rendant plus difficile la détection par des mots-clés (Aston University, 2020).

Les messages offensants peuvent être effacés instantanément avant que l'utilisateur ne les voie, mais une copie sera néanmoins conservée si l'utilisateur souhaite les consulter. *Bullstop* offre ainsi une flexibilité à l'utilisateur, lui permettant de définir le type de messages à supprimer (Aston University, 2020).

5.3. *ReThink Summit School Program*

Le *ReThink Summit School Program* (RSSP), qu'on appellera *ReThink* pour le reste du texte (signifie « repenser »), est une technologie visant à éliminer le contenu haineux en ligne ainsi que contrer la cyberintimidation (Rethink, s.d.).

ReThink possède une approche non intrusive qui permet de détecter et d'arrêter la cyberintimidation avant même que le geste illicite ne soit commis. La technologie fonctionne sur toutes les plateformes telles que Twitter et Instagram, et permet de détecter les messages offensants et donne aux utilisateurs une seconde chance de les reconsidérer. En effet, parfois dans le feu de l'action et sous l'effet d'émotions fortes, les adolescents et les préadolescents veulent publier du contenu offensant, *ReThink* détecte ce contenu avant même qu'il ne soit publié et offre aux jeunes un moment pour repenser les mots qu'ils souhaitent vraiment publier. Avec son approche directe, *ReThink* cherche à responsabiliser de manière proactive les cyberintimidateurs. Les statistiques démontrent que 93 % du temps, les adolescents décident de ne pas publier de contenu offensant sur les réseaux sociaux après avoir « repensé » (Rethink, s.d).

Le *ReThink Summit School Program* (RSSP) est un programme académique destiné aux écoles ayant un intérêt qui rejoint particulièrement la mission de *ReThink,* soit de s'impliquer dans un mouvement pour vaincre la haine en ligne. En joignant le programme *ReThink Summit School*, les établissements scolaires ont un accès à des ressources et à des méthodes qui peuvent aider à mettre fin à la négativité ainsi qu'à promouvoir la positivité dans la communauté scolaire, à mettre terme à la cyberintimidation et à encourager l'adoption d'un climat positif au sein de l'environnement scolaire.

Le programme *ReThink Summit School* a été développé pour mobiliser les enseignants, les conseillers d'orientation, les parents et les élèves, créant ainsi un réseau international d'écoles engagées dans l'élimination de la haine en ligne et l'autonomisation des jeunes d'aujourd'hui. Ce programme éducatif est adapté aux différents niveaux d'âge et fournit

une plateforme de discussion portant sur des aspects numériques pertinents présentés aux élèves en classe. En fin de compte, le programme aide à éduquer les élèves sur le pouvoir de leurs actions en ligne et les encourage à adopter un comportement numérique responsable.

Les écoles qui désirent participer au RSSP recevront : 1) un programme d'études *ReThink* organisé et spécifique pour chaque niveau académique, qui aide à faciliter la discussion dirigée par les éducateurs sur la cyberintimidation dans les salles de classe et qui permettra aux élèves d'être des citoyens numériques responsables ; 2) des instructions détaillées sur le téléchargement de l'application *ReThink* sur les appareils scolaires ; 3) des ressources pour la création d'un module *ReThink* - un groupe parascolaire pour les jeunes de l'école qui veulent diriger un mouvement *ReThink* local ; 4) un ensemble de marchandises qui comprend des t-shirts *ReThink*, des bracelets et d'autres articles attractifs ; et 5) des billets d'entrée gratuits (uniquement) au sommet *ReThink* d'une journée, une célébration stimulante et inspirante du travail de l'école pour mettre fin à la haine en ligne (Rethink, s.d.). Mettant en vedette des leaders mondiaux, des conférenciers et la fondatrice Trisha Prabhu, c'est un événement phare.

Afin de soumettre une demande pour faire partie des écoles bénéficiant du programme *ReThink*, il faut que l'établissement soit une institution desservant au moins 100 étudiants âgés de 5 à 18 ans, de niveau d'enseignement primaire et secondaire. Les Universités ou les Centres de formations techniques ne font pas partie de la communauté visée par le programme *Rethink*. Pour être éligible à un tel programme, il est aussi important d'avoir un enseignement ou un membre de la direction ou de l'administration de cet établissement désigné pour suivre le contact avec l'équipe de *ReThink*. L'établissement doit appliquer via un formulaire sur le site Internet de *ReThink*, et les places pour rejoindre ce programme sont limitées.

6. Autres initiatives

Certaines initiatives que nous n'avons pas classées dans les sections précédentes se retrouvent dans cette partie. Nous avons donc retenu des initiatives d'un côté en lien avec le cybersexisme et de l'autre, la désinformation.

6.1. *#StopCybersexisme*

Le Centre Hubertine Auclert en France, Centre pour l'égalité des femmes et des hommes, a lancé, en mai 2015, une campagne de sensibilisation intitulée « Stop cybersexisme », visant à sensibiliser au caractère sexiste des cyberviolences. Cette initiative a introduit le néologisme « cybersexisme », qui a depuis été largement repris dans les médias et les institutions (Couchot-Shiex et *al.*, 2016 : 7 ; Centre Hubertine Auclert, s.d.).

La campagne se distingue par l'utilisation d'un hashtag #STOPCYBERSEXISME, et un Kit comprenant les « 5 bons réflexes » a été élaboré spécifiquement pour un public cible, à savoir les adolescent.es, étudiant.es, professionnel.les de l'éducation, et professionnel.les de la santé (Centre Hubertine Auclert, s.d., Kit de campagne ; Centre Hubertine Auclert, 2016 ; **Annexe 4**).

La campagne offre des exemples concrets de cybersexisme, notamment des messages à caractère sexuel susceptibles de mettre mal à l'aise les personnes visées. Elle souligne également des comportements tels que le partage et des menaces de diffusion non consensuels de photos ou de vidéos intimes. De plus, la campagne dénonce les pratiques consistant à prendre des photos à l'insu d'une personne et à les partager en ajoutant des commentaires insultants ou dégradants. Ces exemples mettent en lumière la diversité des formes de cybersexisme abordées par cette campagne (**Annexe 4**).

La prévention du sexting

Dans le cadre de la sensibilisation et de la prévention de la pratique du sexting, les travaux de Patchin et Hinduja (2010) mettent en lumière une approche éducative axée sur l'autonomie et la sécurité. Voici quelques points saillants de leurs recommandations :

- **Approche éducative positive** : Ils préconisent un modèle éducatif constructif, allant au-delà de l'abstinence et de la peur.
- **Intégration du sexting dans l'éducation sexuelle** : Ils suggèrent de considérer le sexting comme une composante essentielle de l'éducation sexuelle.
- **Conscience des conséquences** : Ils mettent en avant l'importance de sensibiliser les jeunes aux possibles répercussions du sexting.
- **Outillage des jeunes** : Ils reconnaissent la nécessité de fournir aux jeunes les compétences nécessaires pour faire face aux défis liés à la pratique du sexting et en diminuer les risques et conséquences.
- **Sensibilisation au consentement** : Ils soulignent l'importance de promouvoir une compréhension approfondie du consentement, en mettant en avant des thèmes essentiels tels que le consentement préalable avant l'envoi de photos intimes et avant la diffusion de ces images à des tiers (Patchin et Hinduja, 2010).

À la lumière de ces considérations, deux approches sont proposées pour prévenir le phénomène du sexting (Barrense-Dias et *al.*, 2022) :

- ***L'approche par l'abstinence de sexting***

Elle préconise de dire aux jeunes de s'abstenir totalement de pratiquer le sexting. Cette approche est déployée lorsqu'on définit la pratique du sexting « comme un comportement négatif et déviant » (Barrense-Dias et *al.*, 2022 : 8). En enseignant aux jeunes de s'abstenir de partager des contenus compromettants, tels que des photos intimes, nudes, textes ou vidéos d'une personne non consentante, ils sont sensibilisés aux conséquences négatives de cette pratique. Cependant, ces campagnes d'intervention ont été critiquées pour leur propension à stigmatiser les victimes de l'intimidation ou de harcèlement, en particulier les filles. Les auteurs pensent que ces campagnes « nourrissaient les stéréotypes et ouvraient la porte à des jugements » (Barrense-Dias et *al.*, 2022 : 8).

- ***L'approche par la pratique responsable du sexting (Safer sexting)***

Elle vise à adopter une perspective plus positive en considérant le sexting « comme une activité sexuelle normale dont l'issue n'est pas toujours négative » (Barrense-Dias et *al.*, 2022 : 8). Cette approche met l'accent sur l'éducation des jeunes à une utilisation prudente et respectueuse du sexting, contribuant ainsi à changer la perception de cette pratique.

6.2. *World Wide Web Foundation*

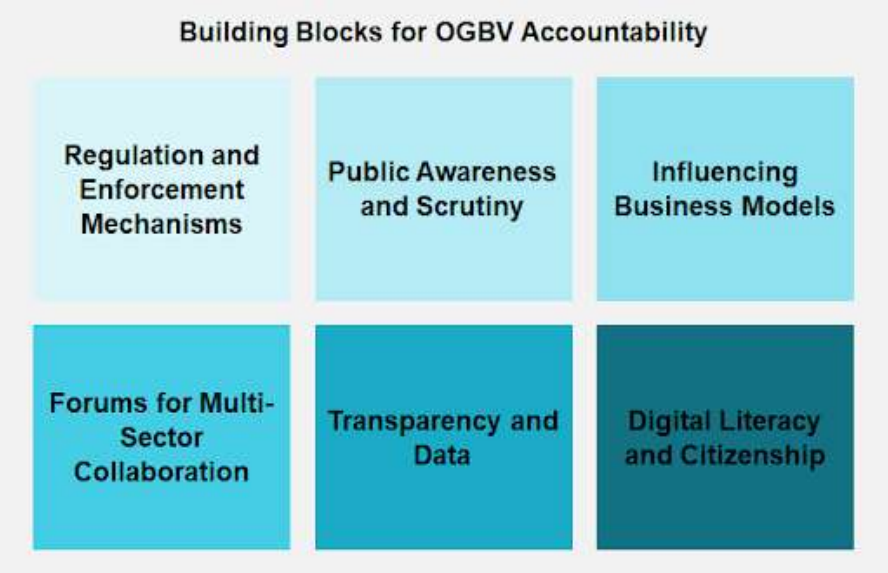
La Fondation *World Wide Web* a adopté une approche exemplaire dans la lutte contre la violence sexiste en ligne en lançant un laboratoire de cocréation. Cette initiative met en avant l'importance d'intervenir à plusieurs niveaux et de promouvoir une responsabilisation collective, établissant ainsi un modèle à suivre dans la recherche de solutions contre la cyberintimidation et la cyberviolence, particulièrement préoccupantes pour les jeunes. Par le biais de l'initiative « *Building Blocks for Online Gender-Based Violence* (OGBV) », la Fondation a développé des solutions technologiques collaboratives, soulignant son engagement collectif pour contrer la violence sexiste en ligne (Web Foundation, 2022a).

À la suite de ces efforts, des réseaux sociaux tels que Facebook (Meta), TikTok, Twitter, et Google ont pris des engagements similaires lors du Forum sur l'égalité des générations des Nations Unies à Paris (2021) (Web Foundation, 2021).

Les consultations subséquentes ont identifié six éléments importants (Web Foundation, 2022b ; Tableau 1) nécessaires pour proposer des solutions durables en vue de prévenir les violences sexistes et sexuelles en ligne (Web Foundation, 2022b).

Cette approche globale et collaborative souligne l'efficacité d'une réponse concertée pour aborder ces problématiques complexes et protéger les jeunes des risques en ligne.

Tableau 1. Éléments constitutifs pour l'obligation de rendre compte des violences sexistes en ligne



Nous exposons ci-dessous la description des six éléments fondamentaux (cf. ***Tableau 1***).

1) Mécanismes de réglementation et d'application

Ces mécanismes sont mis en place par des organismes de réglementation qui ont le pouvoir de contribuer à modifier les lois pour y intégrer les valeurs d'équité, de diversité, et d'inclusion (ÉDI). Les parties prenantes impliquées sont appelées à sensibiliser les environnements tels que les intermédiaires d'Internet et les entreprises technologiques, où la réglementation de protection des données est limitée ou absente, favorisant ainsi les violences sexistes en ligne (Web Foundation, 2022b).

2) Sensibilisation du public et contrôle

Il est essentiel de diffuser des informations sur toute forme de cyberviolence par le biais de médias tels que la radio, les journaux, les magazines, contribuant ainsi à démocratiser la connaissance sur les violences sexistes en ligne.

L'objectif est de sensibiliser et d'informer la population, ce qui se traduit finalement par l'autonomisation d'un plus grand nombre pour lutter contre ces cybermenaces (Web Foundation, 2022b).

3) Influencer les modèles d'affaires

Il est impératif que les entreprises technologiques adoptent une responsabilité proactive dans la lutte contre les cyberviolences, en particulier celles liées au genre. Cela implique un engagement concret à intégrer dans leurs modèles d'affaires, en ajoutant par exemple des critères spécifiques visant à contrer ces formes de violences en ligne. En incorporant ces normes dans leur cadre économique, les entreprises peuvent jouer un rôle essentiel dans la promotion d'un environnement en ligne plus sécuritaire et éthique. Cette approche démontre la nécessité de lier la responsabilité sociale des entreprises à la lutte contre les cyberviolences basées sur le genre (Web Foundation, 2022b).

4) Forums de collaboration multisectorielle

L'instigation de forums de collaboration multisectorielle se révèle essentielle pour aborder les enjeux sociétaux de manière novatrice, et ce, en favorisant des partenariats entre divers secteurs. Cette approche collaborative peut catalyser des changements significatifs et des améliorations de pratiques. En particulier, ce type de réseaux jouent un rôle essentiel dans la recherche de solutions pour prévenir les violences sexistes en ligne. La mobilisation de compétences et de perspectives variées au sein de ces forums renforcerait la capacité collective à élaborer des approches porteuses et holistiques (Web Foundation, 2022b).

5) Transparence et données

Afin d'assurer la responsabilisation en matière de violences sexistes et sexuelles, il est nécessaire d'établir « des normes et des principes partagés de transparence et de partage des données » (Web foundation, 2022b, Libre trad.) tant à l'échelle régionale que

nationale. Cette démarche pourrait donner naissance à une plateforme « commune de données sur les violences sexuelles » envers les femmes, en renseignant avec précision des indicateurs et des paramètres de mesure. Cette approche vise à instaurer l'accessibilité d'une base de données transparente, permettant de procéder à des évaluations objectives de ce phénomène (Web Foundation, 2022b, Libre trad.).

6) Littératie et citoyenneté numériques

L'élément souligne l'importance de maîtriser la littératie et la citoyenneté numériques afin de lutter contre la cyberviolence sexiste et sexuelle. Selon la sociologue Amina Yagoubi (2020), l'accès à une éducation au numérique ainsi que le renforcement des compétences du XXIe siècle sont essentiels pour adopter un usage responsable d'Internet. Il devient donc impératif de former les utilisateurs afin qu'ils soient capables de réguler leurs comportements dans le cyberespace. Cette responsabilité incombe aux gouvernements, aux entreprises technologiques et aux acteurs de l'écosystème, qui doivent investir dans l'éducation du public en termes de littératie et de citoyenneté numériques (Web Foundation, 2022b, trad. libre). Cette approche holistique vise à habiliter les individus à naviguer en toute sécurité dans le monde numérique tout en contribuant de manière active à atténuer la cyberviolence.

6.3. Contrer la désinformation

La propagation de la désinformation peut avoir des conséquences préjudiciables, particulièrement chez les jeunes. Dans le domaine de l'éducation, le Centre canadien d'éducation aux médias et de littératie numérique, connu sous le nom d'HabiloMédias, répond à la nécessité de contrer la désinformation en ligne, en particulier en sensibilisant les jeunes aux conséquences néfastes de ce phénomène. En effet, ce centre propose des ressources pédagogiques pour enseigner aux plus jeunes comment vérifier l'authenticité des informations circulant dans les médias (Naffi et *al.*, 2021).

Ces ressources incluent une variété d'outils tels que des textes, des jeux, des questionnaires, des ateliers, des plans de leçons et des affiches, offrant ainsi une approche complète pour renforcer la littératie numérique des jeunes générations (Naffi et *al.*, 2021 : 5).

D'autres initiatives sont répertoriées pour faire face à ce phénomène. Nous avons retenu quelques exemples (Naffi et *al.*, 2021 : 10-11).

Journalists for Human Rights

L'Organisme est financé par Patrimoine Canada, il lance un programme de formation de 9 mois « *Fighting Disinformation Through Strengthened Media and Citizen Preparedness in Canada ».*

Les décrypteurs

Pour sensibiliser le grand public, Radio-Canada propose une émission « *Les décrypteurs »* dans laquelle l'animateur, Alexis De Lancer, grâce à un chatbot, apprend aux participants ce que sont les *deepfakes* afin de contrer la désinformation.

Agence de Presse Reuters

L'agence de presse Reuters propose une formation en ligne en 16 langues sur « les contenus médiatiques manipulés » (Naffi et *al.*, 2021 : 11).

Checkology

Le site Internet du *News Literacy Project* a mis en place une plateforme d'apprentissage *Checkology* qui « partage des programmes et des ressources afin d'aider le personnel de l'éducation à enseigner la littératie médiatique aux élèves et aider les adultes à déterminer la crédibilité d'une information » (Naffi et *al.*, 2021 : 11).

InfoZones

Le *News Literacy Project* propose une formation virtuelle *InfoZones* pour aborder la technique du « zonage de l'information » qui invite le « public à s'interroger sur l'objectif principal de l'information, soit divertir, vendre, persuader, provoquer, documenter ou informer », puis explique comment « zoner l'information » dans chacune « des six catégories correspondantes : nouvelles, opinion, divertissement, publicité, propagande ou information brute ». Ce qui permet d'avoir une compréhension d'une information et de « ressortir l'objectif principal qui peut être dissimulé sous diverses apparences » (Naffi et *al.*, 2021 : 11).

Web Civic Online Reasoning

Le *Stanford History Education Group* diffuse des ressources « avec des groupes éducateurs et étudiants à travers leur site *Web Civic Online Reasoning* » (Naffi et *al.*, 2021 : 11) pour leur apprendre à reconnaître la véracité des informations recueillies en ligne.

Navigating Digital Information

La collaboration de *CrashCourse, Mediawise* et le *Stanford History Education Group* débouche à la création de la série *Navigating Digital Information.* La série a pour mission de diffuser « des vidéos éducatives pour développer des compétences pratiques dans l'évaluation des informations en ligne » (Naffi et *al.*, 2021 : 11).

Moon Disaster

Moon Disaster est un « projet artistique immersif » qui propose aux visiteurs d'« entrer dans une histoire alternative en leur demandant de réfléchir à la façon dont les nouvelles technologies peuvent déformer, réorienter et obscurcir la vérité qui nous entoure » (Naffi et *al.*, 2021 : 11).

7. Recommandations

D'après Begin (2016), les actions destinées à contrer la cyberintimidation peuvent être organisées en deux grandes catégories : celles développées par des entités gouvernementales ou non gouvernementales, et celles mises en place par la société civile; le grand public ou un citoyen lambda.

Malgré les limitations des recherches sur les interventions scientifiques contre la cyberintimidation, Zhu et *al.* (2021) parviennent à identifier des stratégies prometteuses visant à prévenir la cyberintimidation, protéger les jeunes et réduire les incidents liés à cette forme de harcèlement en ligne. Les auteurs proposent deux recommandations principales :

- **Mobilisation d'efforts collectifs pour assurer un milieu exempt de cyberintimidation** : Ces efforts impliquent des individus, des communautés, des éducateurs ou parents, des établissements scolaires.
- **Accès à des apprentissages de gestion des émotions** : Ce type de formation doit être accessible aux enseignants, conseillers, éducateurs ou parents afin qu'ils acquièrent des compétences dans ce domaine. Cela leur permettrait d'être réceptifs aux émotions négatives des jeunes afin de les accompagner dans la gestion et l'autorégulation émotionnelles, et prévenir des problèmes sociaux ou psychologiques (Zhu et *al.,* 2021).

En complément des nombreuses recommandations présentées dans ce rapport, nous choisissons de conclure cette section avec quelques recommandations clés.

- ***Recommandation #1 : Développer de bons réflexes***

En cas de cyberintimidation, le Service de police de la ville de Montréal (SPVM) recommande aux internautes d'adopter des réflexes prudents. Autrement dit, si une situation devient problématique avec un quelconque auteur « exerçant une cyberintimidation » (SPVM, s.d.), l'internaute devrait

- quitter « l'environnement en ligne », c'est par exemple le cas s'il reçoit «un courriel menaçant ;
- ne pas divulguer ses « renseignements personnels », par exemple : son numéro de téléphone, son nom et prénom, son adresse de domicile, ses mots de passe, son âge, etc. ;
- « éviter d'échanger avec l'intimidateur » ;
- s'abstenir de répondre « aux messages intimidants »;
- informer rapidement de la situation « le fournisseur de services Internet ou de téléphonie cellulaire, selon le cas et d'alerter le service de police local lorsqu'il y a soupçon d'une infraction criminelle » (SPVM, s.d.)

- ***Recommandation #2 : Adopter une politique de tolérance Zéro***

La Commission de l'éthique de la science et de la technologie (CEST) a publié un document faisant état de quatre recommandations visant la lutte contre la cyberintimidation au Québec.

a) [Il est nécessaire] que le **ministère de l'Éducation, du Loisir et du Sport (MELS)**, de concert avec les fonds subventionnaires québécois, encourage la recherche sur les causes et les effets de la cyberintimidation afin de mieux comprendre ce phénomène. [Il importe que ce ministère], dans la mise en œuvre de son plan d'action pour contrer la violence à l'école, mette sur pied des campagnes d'information et de sensibilisation afin de faire connaître la problématique de la cyberintimidation dans la société.

b) Pour mieux outiller les parents, les enseignants, les acteurs sociaux et communautaires, les corps policiers à faire face à la cyberintimidation, la CEST recommande que le ministère de l'Éducation, du Loisir et du Sport, en collaboration avec le ministère de la Santé et des Services sociaux (MSSS) et le ministère de la Sécurité publique (MSP), produise un document informatif pour aider ces personnes à savoir comment agir en cas de cyberintimidation.

c) Puisque la cyberintimidation peut avoir des conséquences graves, une politique de tolérance zéro devrait être adoptée et le ministère de la Sécurité publique (MSP) devrait favoriser l'intervention policière en cas de cyberintimidation.

d) La CEST-jeunesse recommande également que les enseignants, et les intervenants scolaires et pédagogiques discutent avec les jeunes de la problématique de la cyberintimidation pendant leurs cours d'Éthique et culture religieuse, au primaire et au secondaire, et au cours d'Éthique et politique, au collégi*al.*

- ***Recommandation #3 : Proposez des scénarios pédagogiques***

Proposer des scénarios d'accroche stimulants destinés aux élèves afin de favoriser une expression libre, est une approche recommandée (Couchot-Schiex et *al.*, 2016). Un exemple concret de scénario d'accroche est présenté dans l'étude de Couchot-Schiex et *al.* (2016 : 22). Un libellé de scénario d'accroche pertinent pourrait être le suivant (Couchot-Schiex et *al.*, 2016 : 22) :

> « *Manon*[9] *fait une photo d'elle, elle veut se mettre en valeur. Elle envoie sa photo à des ami-e-s en toute confiance. La photo est récupérée et diffusée sur les téléphones portables et les réseaux sociaux. Beaucoup de personnes commentent la photo… Elle a peur qu'on se moque d'elle à l'école ».*

- ***Recommandation #4 : Renforcer la compétence numérique***

Pour finir, afin de faciliter la mise en œuvre du Plan d'action numérique en éducation et en enseignement supérieur (PAN) du Québec, il est important de se référer au **Cadre de référence de la compétence numérique** établi par le Ministère de l'Éducation et de l'Enseignement supérieur (MEES, 2018, 2019).

[9] Le prénom féminin peut être remplacé par un prénom masculin.

Ce cadre définit la compétence numérique comme « un ensemble d'aptitudes relatives à une utilisation confiante, critique et créative du numérique pour atteindre des objectifs liés à l'apprentissage, au travail, aux loisirs, à l'inclusion dans la société ou à la participation à celle-ci » (MEES, 2029 : 7). Parmi les 12 dimensions de la compétence numérique, deux sont particulièrement pertinentes pour aborder les préoccupations liées à la lutte contre l'hostilité en ligne : 1) **agir en citoyen éthique à l'ère du numérique** (1ère dimension) et 2) **développer sa pensée critique envers le numérique** (11ème dimension).

Nous nous référons au tableau suivant incluant ces deux dimensions extrait du rapport « L'hostilité envers les femmes » publié par le Conseil du statut de la femme pour une présentation plus détaillée (CSF, 2022 : 66). Il met en lumière des exemples de thèmes importants pouvant être abordés en classe en lien avec le Cadre de référence de la compétence numérique.

Tableau 2. Dimension de la compétence numérique pour lutter contre l'hostilité en ligne

Dimensions	Exemples de thèmes pouvant être abordés en classe
Agir en citoyen éthique à l'ère du numérique	• Cyberintimidation • Violences à caractère sexuel « liées au numérique » • Inclusion sociale « par le numérique »
Développer sa pensée critique envers le numérique	• Fausses nouvelles • Influenceurs des réseaux sociaux • Trolls • Algorithmes • *Social bots* (comptes de réseaux sociaux automatisés) • Géants du Web • Publicités ciblées

Source : MEES, 2019, p. 9 et 30.

CONCLUSION

L'essor des médias sociaux et la révolution numérique redéfinissent profondément les pratiques politiques, transformant à la fois l'accès à l'information et les modes de participation citoyenne. Acteurs majeurs de cette transformation, les jeunes adoptent massivement ces plateformes pour débattre et défendre leurs causes, jouant un rôle déterminant dans des mouvements tels que *Black Lives Matter, March for Our Lives* ou *DREAMer* (Garcia et al., 2021).

Les réseaux sociaux bouleversent les mécanismes traditionnels de diffusion de l'information en supprimant les filtres auparavant imposés par les médias classiques. Cette accessibilité permet une circulation rapide et globale des discours politiques, modifiant non seulement leur portée mais aussi leur nature. Ces outils numériques offrent aux jeunes de nouvelles opportunités pour amplifier leurs revendications et mobiliser des communautés, participant ainsi à une redéfinition des normes sociales et politiques (Garcia et al., 2021).

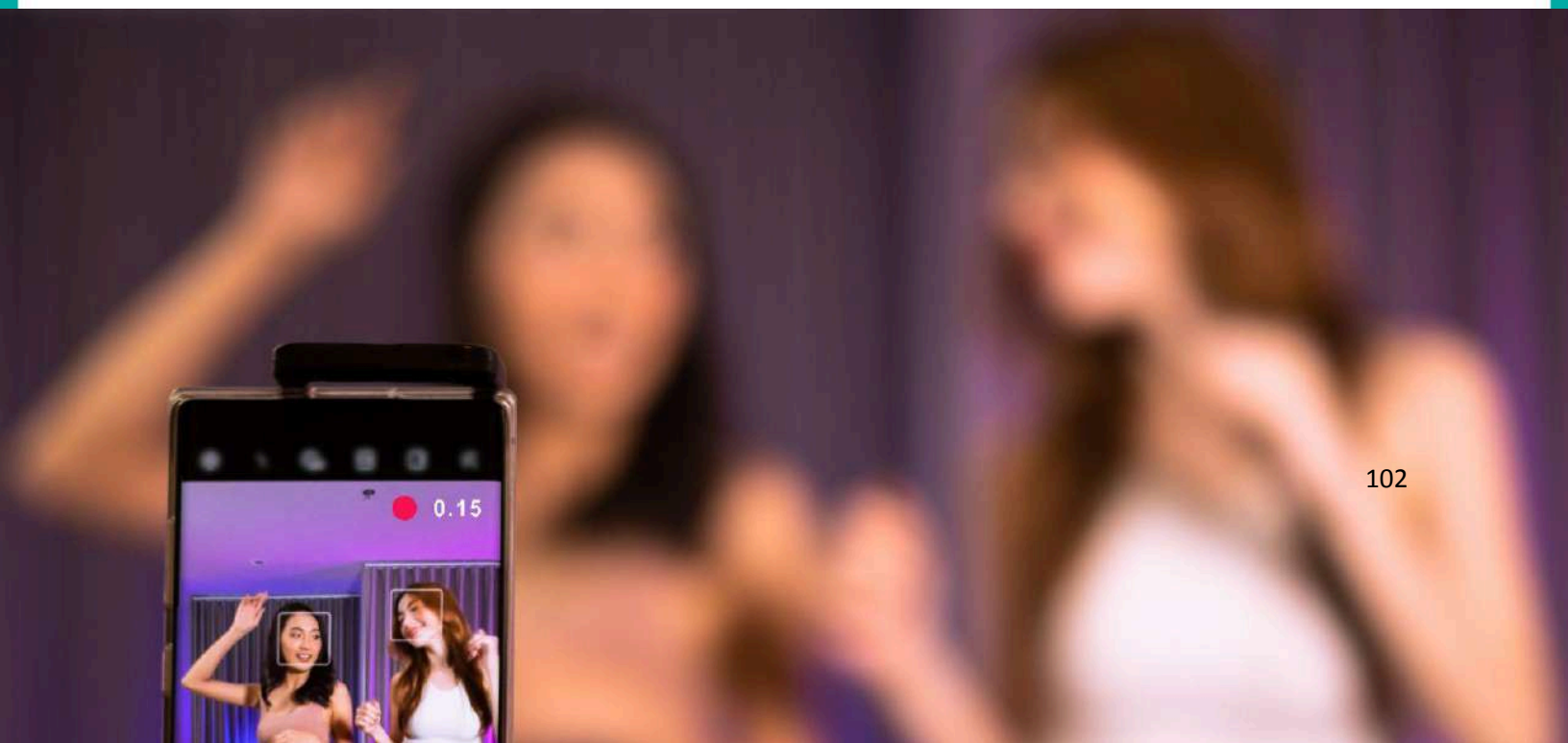
Cependant, cette transition vers une politique numérique n'est pas sans défis. La prolifération de fausses nouvelles et d'informations non vérifiées favorise la désinformation et la manipulation, fragilisant l'intégrité des débats politiques et sociaux. Ce phénomène souligne l'urgence de développer des mécanismes pour préserver la qualité et la fiabilité de l'information diffusée sur ces plateformes (Garcia et al., 2021).

La culture numérique et les outils qui lui sont associés transforment en profondeur la relation des individus à l'apprentissage, la communication et le raisonnement. Il y a plus de dix ans, Henry Jenkins (2006) décrivait cette évolution comme l'émergence d'une culture participative, où les gens ne se contentent plus de consommer des médias, mais les produisent, les modifient et les développent également (Garcia et al., 2021).

Dans ce contexte, l'engagement politique en ligne se distingue par une répartition plus équitable entre les races et les classes sociales par rapport à d'autres formes de participation politique, comme l'exemple du vote. Les jeunes, notamment ceux issus de la diversité, se distinguent par leur capacité à faire preuve de créativité et de résilience face aux défis qu'ils rencontrent. Cet engagement a nourri certains des mouvements sociaux les plus influents de notre époque, abordant des problématiques cruciales essentielles telles que le racisme, le sexisme, les droits des citoyens et les questions environnementales. Si cet engagement en ligne est encadré de manière éthique, il pourrait participer à enrichir les pratiques politiques et favoriser une participation plus équitable (Garcia et al., 2021).

Cependant, cette participation accrue expose également les jeunes à des risques de cyberviolence, incluant la désinformation, la diffamation et les attaques en ligne, qui peuvent avoir des conséquences graves sur leur bien-être à moyen et long terme. Face à ces menaces, l'éducation à l'information devient nécessaire. L'acquisition de compétences telles que la recherche, l'évaluation critique et la sélection des informations en ligne est désormais indispensable. Ces compétences permettent non seulement de discerner la crédibilité des sources et de comprendre les motivations derrière les contenus partagés, mais aussi de sensibiliser les jeunes aux dangers de la cyberintimidation et de renforcer leur résilience face à la désinformation.

Dans ce contexte, la citoyenneté numérique émerge comme un concept central. Elle englobe la responsabilité, le respect et la participation éthique en ligne. En promouvant une compréhension approfondie des enjeux numériques, il devient possible de préparer les individus à naviguer dans l'espace numérique de manière éthique et responsable. La promotion de la citoyenneté numérique représente ainsi un levier essentiel pour lutter contre la cyberviolence, encourager des comportements respectueux et collaboratifs en ligne, et garantir un environnement numérique plus sain et équitable.



BIBLIOGRAPHIE

Aston University (2020, 17 july). Cyberbullying ‘shield’ app uses AI to combat social media trolls. Repéré le 2 décembre 2024 à https://www.aston.ac.uk/latest-news/cyberbullying-shield-app-uses-ai-combat-social-media-trolls#

Agence France-Presse (2019, 6 sept.). Les géants de la technologie lancent le « deepfake challenge » pour contrer la désinformation. *Radio-Canada*. Repéré le 3 décembre 2024 à https://ici.radio-canada.ca/nouvelle/1288876/deepfake-challenge-lutte-facebook-desinformation

Alava, S. (2018). Haine et violence numérique : le côté obscur du Cyberespace. *Terminal. Technologie de l’information, culture & société*, 123.

Alonso, C., & Romero, E. (2019). Sexting behaviours in adolescents : Personality predictors and psychosocial outcomes in a one-year follow-up. *Anales de Psicología/Annals of Psychology, 35*(2), 214-224.

Barrense-Dias, Y., Surís, J. C., & Chok, L. (2022, mai). *Sexting, harcèlement, intimidation : le point de vue des témoins.* Raisons de santé, 333. Lausanne : Unisanté – Centre universitaire de médecine générale et santé publique, 1–48.

BDM (2023). Les chiffres clés d’Internet et des réseaux sociaux dans le monde en avril 2023. Repéré le 03 décembre 2024 à https://www.blogdumoderateur.com/chiffres-cles-internet-reseaux-sociaux-monde-avril-2023/

Bégin, M. (2016, juillet). *Agir contre la cyberintimidation avec la vidéo numérique et YouTube : Une étude de sociologie cognitive sur la communication socio-éducative médiatisée chez des adolescents.* [Thèse de doctorat, Université de Montréal]. Dépôt institutionnel de l'Université de Montréal https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/18441/Begin_Mathieu_2016_these.pdf?sequence=2&isAllowed=y

Blécot, L., Lakrary, A., Laloux, M., & Kempeneers, P. (2022). L'échange de nudes chez les jeunes français et belges francophones de 13–25 ans: une étude exploratoire. *Sexologies, 31*(3), 147–155.

Bosse, T., & Stam, S. (2011, August). A normative agent system to prevent cyberbullying. In *2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, Vol 2, 425–430.

Boudreault, A., Beaulieu, J., Lessard, J., & Fournier, S. (2020). Le rôle de l'intimidation traditionnelle et de la cyberintimidation sur les problèmes internalisés et le bien-être des adolescents. *Nouveaux cahiers de la recherche en éducation, 22*(2), 69–92.

Bouré, M., Couttignane, D., & Muça, K. (2022, 12 avril). La cyberintimidation : une étude auprès des jeunes. [Rapport présenté dans le cadre du cours HOR 1200, *Horizon : Risques et défis du XXIe siècle*, Université de Montréal], 1–31. Repéré le 12 septembre 2024 à https://fas.umontreal.ca/public/FAS/fas/Documents/3-Etudes/horizon/Cyberintimidation_.pdf

BullStop (s.d.). *Application.* Repéré le 20 septembre 2024 à https://www.bullstop.io/

Bullying statistics (s.d.). *Text Bullying – Bullies That Use Text Messaging to Harass Others*. Repéré le 18 septembre 2024 à http://www.bullyingstatistics.org/content/text-bullying.html

Burns, T., & Gottschalk, F. (2019). *Educating 21st Century Children: Emotional Well-being in the Digital Age. Educational Research and Innovation*. OECD Publishing, Paris.

Capeluto, S. (2023, 2 janvier). Comment protéger les ados des risques des réseaux sociaux? Dans *Être parents*. Repéré le 2 décembre 2024 à https://etreparents.com/comment-proteger-les-ados-des-risques-des-reseaux-sociaux/

Centre Hubertine Auclert (s.d.). *Les missions du Centre.* Repéré le 2 décembre 2024 à https://www.centre-hubertine-auclert.fr/les-missions

Centre Hubertine Auclert (2016). *Spot de sensibilisation au cybersexisme* [Vidéo]. YouTube.Repéré le 25 novembre 2024 à https://www.youtube.com/watch?v=A6DyiswioE4

Centre Hubertine Auclert (s.d.). *Kit de campagne. #STOPCYBERSEXISME*. Repéré le 30 septembre 2024 à https://www.centre-hubertine-auclert.fr/egalitheque/campagne/stopcybersexisme

CSS (s.d.). *Fiche 6. Plan-lutte-intimidation-violence.* Centre de services scolaire (CSS) - Éducation, Gouvernement du Québec. Repéré le 5 septembre 2024 à https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/education/publications-adm/Centre_de_services_scolaire/Fiche_6_Plan-lutte-intimidation-violence.pdf

Chan, S., Khader, M., Ang, J., Tan, E., Khoo, K., & Chin, J. (2012). Understanding 'Happy Slapping'. *International Journal of Police Science & Management, 14*(1), 42–57.

Chehab, Y., Levasseur, C., & Bowen, F. (2016). De l'école au cyberespace, le phénomène de l'intimidation en ligne chez les jeunes : État de la recherche et de l'intervention. *McGill Journal of Education, Revue Des Sciences De l'éducation De McGill, 51*(1), 495-515.

Chen, Y., Zhou, Y., Zhu, S., & Xu, H. (2012, September). Detecting Offensive Language in Social Media to Protect Adolescent Online Safety. In *2012 International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 international conference on social computing Social Computing (SocialCom)*, IEEE, 71-80.

Code criminel (1985). *Chapitre C-46*. Repéré le 17 novembre 2024 à https://laws-lois.justice.gc.ca/fra/lois/c-46/

Cybertip.ca (2023, avril). *Risk for kids: Discord*. [En ligne]. Consulté le 18 décembre 2024 à https://www.cybertip.ca/en/online-harms/alerts/2023/risk-for-kids-discord/.

CSF (s.d.). *Slutshaming*. Conseil du Statut de la Femme (CSF), Gouvernement du Québec. Repéré le 17 novembre 2024 à : https://csf.gouv.qc.ca/article/publicationsnum/bibliotheque-des-violences-faites-aux-femmes/slutshaming/

CSF (2022, juin). *L'hostilité en ligne envers les femmes*. Conseil du statut de la femme, Gouvernement du Québec, 1–99. Repéré le 8 septembre 2024 à : https://csf.gouv.qc.ca/wp-content/uploads/Etude-hostilite-en-ligne-envers-les-femmes.pdf

Couchot-Schiex, S., Moignard, B., & Richard, G. (2016). *Cybersexisme et cyberviolences, une étude sociologique dans des établissements franciliens* [Thèse de doctorat]. UPEC; Centre Hubertine Auclert.

Cross, D., Monks, H., Campbell, M., Spears, B., Slee, P., & Salmivalli, C. (2015). A social–ecological framework for understanding and reducing cyberbullying behaviours. In *Aggression and Violent Behavior, 23*, 109–117.

Descurninges, C. (2022). 57 % des jeunes Québécois ont déjà subi de la cyberintimidation. Dans *La Presse*. Repéré le 29 novembre 2024 à : https://www.lapresse.ca/actualites/2022-09-03/57-des-jeunes-quebecois-ont-deja-subi-de-la-cyberintimidation.php

DOP (s.d.). *Advice for parents and carers on cyberbullying.* In Department of Education. Repéré le 5 aout 2024 à : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf

Dylan, L. (2017, 28 février). Je veux comprendre… le slut-shaming. *Madmoizelle*. Repéré le 17 novembre 2024 à : https://www.madmoizelle.com/slut-shaming-115244

e-Enfance. (s.d). *Cyberharcèlement : Qu'est-ce le cyberharcèlement ?* Repéré le 10 novembre 2024 à : https://e-enfance.org/informer/cyber-harcelement/

EMCDDA (s.d). *Vienna Social Competence Training (ViSC) - a multimodal training for school classes to strengthen pupils' sense of class commitment, the perception of responsibility and to foster non-bullying and nonaggressive behaviour in conflict situations.* Best practice, European Monitoring Center for Drugs and Drug Addiction (EMCDDA). Repéré le 15 novembre 2024 à Vienna Social Competence Training (ViSC)

Estevez, E., Canas, E., Estevez, J. F., & Povedano, A. (2020). Continuity and overlap of roles in victims and aggressors of bullying and cyberbullying in adolescence: A systematic review. In *International Journal of Environmental Research and Public Health, 17*(20), 7452.

Family Lives (2022). Effects of cyberbullying. *Family Lives, UK*. Repéré le 24 novembre 2024 à : https://www.familylives.org.uk/advice/bullying/cyberbullying/effects-of-cyberbullying?referer=/browse/50188/bullying,impact-of-social-media-online

Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. *European Journal of Developmental Psychology, 9*(2), 168–181.

France24 (2024, 28 novembre). *L'Australie adopte une loi interdisant l'accès aux réseaux sociaux aux moins de 16 ans.*[En ligne]. Consulté le 18 décembre 2024 à https://www.france24.com/fr/asie-pacifique/20241128-l-australie-adopte-une-loi-interdisant-l-acc%C3%A8s-aux-r%C3%A9seaux-sociaux-aux-moins-de-16-ans

Forbes (2024). *L'Australie interdit les réseaux sociaux aux moins de 16 ans : Tout ce qu'il faut savoir.* [En ligne]. Consulté le 18 décembre 2024 à https://www.forbes.fr/societe/laustralie-interdit-les-reseaux-sociaux-aux-moins-de-16-ans-tout-ce-quil-faut-savoir

Fortinet (s.d.). *What is Doxing? Cyberglossary.* Repéré le 7 décembre 2024 à : https://www.fortinet.com/resources/cyberglossary/doxing

Garcia, A. G., McGrew, S., Mirra, N., Tynes, B., & Kahne, J. (2021). Rethinking digital citizenship : Learning about media, literacy, and race in turbulent times. In *Educating for civic reasoning and discourse,* 319–352.

Goggin, B. (2023, 21 juin). *Discord faces challenges in protecting child safety on its platform*. NBC News. [En ligne]. Consulté le 18 décembre 2024 à https://www.nbcnews.com/tech/social-media/discord-child-safety-social-platform-challenges-rcna89769

Gendarmerie royale du Canada (2022, 2 février). Les faits : La cyberintimidation. *GRC*. Repéré le 4 octobre 2024 à : https://rcmp.ca/fr/gazette/faits-cyberintimidation

Gervais, L.-M., & Fortier, M. (2021, 25 février). Hausse de l'intimidation chez les jeunes avec les cours en ligne. *Le Devoir, Éducation*. Repéré le 3 décembre 2024 à : https://www.ledevoir.com/societe/education/595874/coronavirus-hausse-de-l-intimidation-chez-les-jeunes-avec-les-cours-en-ligne

Gottschalk, F. (2022). Cyberbullying: An overview of research and policy in OECD countries. *OECD Education Working Papers* (No. 270). OECD Publishing, Paris.

Gouvernement du Québec (2024). *C-12 - Charte des droits et libertés de la personne*. Chapitre C-12, Légis Québec . Repéré le 17 avril 2024 à : https://www.legisquebec.gouv.qc.ca/fr/document/lc/C-12

Gouvernement du Québec (2023a). *Cyberintimidation*. Repéré le 29 mars 2024 à : https://www.quebec.ca/famille-et-soutien-aux-personnes/violences/intimidation/cyberintimidation?instagramhybrid=&cHash=54ce0a7a85b5c00fafbbf0da6ef9c069

Gouvernement du Québec (2023b, 27 oct.). *Plan de prévention de la violence et de l'intimidation dans les écoles 2023-2028*. Repéré le 29 novembre 2024 à : https://www.quebec.ca/gouvernement/ministere/education/publications/plan-prevention-violence-intimidation-ecoles-2023-2028

Gradinger, P., Yanagida, T., Strohmeier, D., & Spiel, C. (2015). Prevention of cyberbullying and cyber victimization: Evaluation of the ViSC Social Competence Program. *Journal of School Violence, 14*(1), 87–110.

Gravel, M.-A. (2015, fév.). *La victimisation de la population québécoise : victimisation criminelle et cybervictimisation*. Institut de la statistique du Québec, Gouvernement du Québec, 90 p. Repéré le 17 juin 2024 à : https://statistique.quebec.ca/fr/fichier/la-victimisation-de-la-population-quebecoise-victimisation-criminelle-et-cybervictimisation.pdf

Gutiérrez, L. M. F. (s.d.). *Le sharenting : exposition excessive de vos enfants sur les réseaux sociaux*. Être parents. Repéré le 30 sept. 2024 à : https://etreparents.com/le-sharenting-exposition-excessive-de-vos-enfants-sur-les-reseaux-sociaux/

Hango, D. (2016, 19 déc.). *Regards sur la société canadienne : La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada*. Statistique Canada. Repéré le 3 juin 2024 à : https://www150.statcan.gc.ca/n1/pub/75-006-x/2016001/article/14693-fra.htm#:~:text=La%20cyberintimidation%20consiste%20généralement%20en,d%27effrayer%20une%20autre%20personne

Hackett, L. (2016). Cyberbullying and its implications for human rights. *UN Chronicle, 53*(4), 41–43.

Hue, B (2023, 10 mai). C*e que contient le projet de loi pour « sécuriser Internet » dévoilé ce mercredi.* RTL - Radio Télévision Luxembourg. Repéré le 12 novembre 2024 à : https://www.rtl.fr/actu/sciences-tech/ce-que-l-on-sait-du-projet-de-loi-pour-securiser-internet-devoile-ce-mercredi-7900263091.

Ichi.pro (2024). *À l'intérieur du réseau de rencontres pour adolescents non modéré et potentiellement dangereux de Discord*. [En ligne]. Consulté le 18 décembre 2024 à https://ichi.pro/fr/a-l-interieur-du-reseau-de-rencontres-pour-adolescents-non-modere-et-potentiellement-dangereux-de-discord-113564173950608

INSPQ (2023). *La cyberintimidation chez les jeunes*. Institut national de santé publique du Québec. Repéré le 28 mars 2024 à : https://www.inspq.qc.ca/intimidation/jeunes/cyberintimidation

ISQ (2019). *Regard statistique sur la jeunesse : État et évolution de la situation des Québécois âgés de 15 à 29 ans, 1996 à 2018*. Institut de la statistique du Québec, 298 p. Repéré le 29 mars 2024 à : https://statistique.quebec.ca/fr/fichier/regard-statistique-sur-la-jeunesse-etat-et-evolution-de-la-situation-des-quebecois-ages-de-15-a-29-ans-1996-a-2018-edition-2019.pdf

JDN (s.d.). *Troll sur Internet : définition et conseils pratiques pour bien réagir*. Journal du Net. Repéré le 2 novembre 2024 à : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445206-troll-sur-internet-definition-et-conseils-pratiques-pour-bien-reagir/

Jehel, S. (2018). Les adolescents face aux violences numériques, entre adhésion et résistances aux logiques de violence. *Terminal. Technologie de l'information, culture & société*(123).

John, Ann, et *al.* (2018) Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review.In *Journal of medical internet research* 20.4 (2018): e9044..

Kmetrix (2024, 18 octobre). *Le grooming : un danger croissant pour les adolescents en ligne*. [En ligne]. Consulté le 18 décembre 2024 à https://kmetrix.fr/le-grooming-un-danger-croissant-pour-les-adolescents-en-ligne/

La Tribune (2024, 28 novembre). *L'Australie interdit l'accès aux réseaux sociaux aux moins de 16 ans*. [En ligne]. Consulté le 18 décembre 2024 à https://www.latribune.ca/monde/2024/11/28/laustralie-interdit-lacces-aux-reseaux-sociaux-aux-moins-de-16-ans-R7EWET7M2FEWTDA5QMULPHWYXU/

Lanteigne, C. (2023, mars). *Élaboration et implantation d'activité de prévention de la cyberintimidation destinées aux parents afin d'accompagner les enfants du premier cycle du primaire à l'utilisation de techniques de contre-manipulation*. Rapport de stage à la maîtrise en psychoéducation, Université du Québec en Abitibi-Témiscamingue (UQAT), Département des sciences du développement humain et social, 130 p.

La Presse Canadienne (2022, 3 septembre). Étude de McAfee. Réseaux sociaux : 57 % des jeunes Québécois ont déjà subi du cyberharcèlement. *Société, En Bauce, Néomédia*. Repéré le 5 juillet 2024 à : https://www.enbeauce.com/actualites/societe/471200/reseaux-sociaux-57-des-jeunes-quebecois-ont-deja-subi-du-cyberharcelement

Légifrance (s.d.). *Projet de loi visant à sécuriser et réguler l'espace numérique*. Repéré le 12 mai 2024 à : https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/?detailType=EXPOSE_MOTIFS&detailId=

Legislation.gov.au. (2024). *Online Safety Amendment (Social Media Minimum Age) Act 2024*. [En ligne]. Consulté le 18 décembre 2024 à https://www.legislation.gov.au/C2024A00127/asmade

Li, H. (2020, 12 octobre). Une brève histoire d'Internet... et un regard vers l'avenir. *Chronique d'Harold Li, Journal du Net*. Consulté le 30 septembre 2024 à : https://www.journaldunet.com/ebusiness/internet-mobile/1494519-une-breve-histoire-d-internet-et-un-regard-vers-son-avenir/

Li, J., Craig, W., & Johnson, M. (2015, novembre). *Young Canadians' Experience with Electronic Bullying*. Kingston, Ontario, Queen's University, Media Smarts, 1–25. Repéré le 28 mars 2023 à : https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/young-canadians-electronic-bullying.pdf

Livingstone, S., & Mason, J. (2015). Sexual rights and sexual risks among youth online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments. *European NGO Alliance for Child Safety Online (ENACSO)*.

Madigan, S., Ly, A., Rash, C. L., Van Ouytsel, J., & Temple, J. R. (2018). Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis. *JAMA Pediatrics, 172*(4), 327–335.

MFA (2021). *S'engager collectivement pour une société sans intimidation : Plan d'action concerté pour prévenir et contrer l'intimidation et la cyberintimidation 2020-2025*. Gouvernement du Québec, Direction adjointe de la Lutte contre l'intimidation et mandats spéciaux, ministère de la Famille (MFA), 49 p. Repéré le 5 juill. 2024 à : https://www.mfa.gouv.qc.ca/fr/publication/Documents/plan-action-intimidation-2020-2025.pdf

Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof, 23*(3), 255–262.

Marciano, L., Schulz, P. J., & Camerini, A.-L. (2020). Cyberbullying perpetration and victimization in youth: A meta-analysis of longitudinal studies. *Journal of Computer-Mediated Communication, 25*(2), 163–181.

McAffee. (2022). *Cyberbullying in plain sight : A McAffee Connected Family Report*. McAfee, 1-26. Repéré le 30 juin 2024 à : https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-cyberbullying-in-plain-sight-2022-global.pdf

MEES (2018). *Plan d'action numérique en éducation et en enseignement supérieur*. Gouvernement du Québec, Ministère de l'Éducation et de l'Enseignement supérieur, 1–86.

MEES (2029, avril). *Cadre de référence de la compétence numérique*. Gouvernement du Québec, Ministère de l'Éducation et de l'Enseignement supérieur, 1–35.

MENESR (2016, nov.). *Guide de prévention des cyberviolences en milieu scolaire*. Ministère de l'Éducation Nationale, de l'Enseignement Supérieur et de la Recherche, Paris, 47 p.

MENJ (2011). *Guide pratique pour lutter contre le cyber-harcèlement entre élèves*. Ministère de l'Éducation Nationale et de la Jeunesse, 15 p.

MENJ (s.d.). *Non au harcèlement*. Ministère de l'Éducation Nationale et de la Jeunesse (MENJ), France. Repéré le 13 sept. 2024 à : https://www.education.gouv.fr/non-au-harcelement

Meta (s.d.). *LGBT+ : Adoption des comportements bienveillants sur Internet*. Centre de sécurité, Meta, 8 p. Repéré le 10 juill. 2024 à : https://about.meta.com/actions/safety/resource/f/239763489799000/

Milton, A., et *al.* (2019). Sexting, Web-Based Risks, and Safety in Two Representative National Samples of Young Australians: Prevalence, Perspectives, and Predictors. *JMIR Mental Health, 6*(6), e13338.

MSP (2009). *La cyberintimidation et le harcèlement*. Ministère de la Sécurité publique Québec, 12 p. Repéré le 12 sept. 2024 à : https://web.archive.org/web/20150724201248/http://www.securitepublique.gouv.qc.ca/fileadmin/Documents/police/statistiques/criminalite/cyberintimidation/Bulletin_statistique_cyberintimidation_cyberharcelement.pdf

Naffi, N., Davidson, A.-L., Barma, S. et *al.* (2021). Pour une éducation aux hypertrucages malveillants et un développement de l'agentivité dans les contextes numériques. *Éducation et francophonie, 49*(2).

National Campaign to Prevent Teen and Unplanned Pregnancy and CosmoGirl.com. (2008). *Sex and tech: Results from a survey of teens and young adults*. Repéré le 24 sept. 2024 à : https://powertodecide.org/sites/default/files/resources/primary-download/sex-and-tech.pdf

National Crime Prevention Council. (s.d.). *Cyberbullying and Sexting on Social Media*. Repéré le 24 sept. 2024 à : http://archive.ncpc.org/programs/living-safer-being-smarter/surfing-safer/cyberbullying-and-sexting-on-social-media.html#fn2

Cave, D. (2008, 12 avril). Eight teenagers charged in internet beating have their day on the web. New York Times. Repéré le 24 mai 2024 à : http://www.nytimes.com/2008/04/12/us/12florida.html?_r=2

Niang, P. M., & Nagem, R. (2018). Les cyberviolences genrées, sexistes et sexuelles chez les jeunes. Du constat d'une persistance à l'émergence de formes de résilience. *Terminal. Technologie de l'information, culture & société*(123).

OCDE (2020). Protecting children online: An overview of recent developments in legal frameworks and policies. *Documents de travail de l'OCDE sur l'économie numérique, no 295*. Éditions OCDE, Paris.

Ollagnier, A., Cabrio, E. and *al.* (2022, juin). CyberAgressionado-v1: a Dataset of Annotated Online Aggressions in French Collected through a Role-playing Game. In *LREC 13 th Language Resources and Evaluation Conference*, 867–875

Patchin, J. & Hinduja, S. (2020). It is Time to Teach Safe Sexting". *Journal of Adolescent Health*, *66(2)*, 140–143.

Pérez, P.J.C., Valdez, C.J.L., and *al.* (2012). MISAAC: Instant messaging tool for ciberbullying detection. In *Proceedings on the International Conference on Artificial Intelligence (ICAI)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Pierre, Djanikian (2023, 20 janv.). L'Europe avertit TikTok d'une potentielle interdiction dans ses 27 pays. Dans *Charles Tech*. Repéré le 10 sept. 2024 à : https://charlestech.fr/leurope-avertit-tiktok-dune-potentielle-interdiction-dans-ses-27-pays/.

Polanin, J. R., Espelage, D. L. and *al.* (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science*, *23*(3), 439-454.

PPC (2022, 23 février). Conseils pour les parents aux prises avec l'intimidation et la cyberintimidation. *Plan de protection du Canada (PPC)*. Repéré le 8 décembre 2024 à : https://www.cpp.ca/fr/blogue/conseils-pour-les-parents-aux-prises-avec-lintimidation-et-la-cyberintimidation/.

RAINN (2020, 10 juillet). *Grooming: Know the warning signs*. [En ligne]. Consulté le 18 décembre 2024 à https://rainn.org/news/grooming-know-warning-signs

Respect Zone. *L'association : Notre projet*. Repéré le 30 novembre 2024 à : https://www.respectzone.org/lassociation/.

Rethink. (s. d.). *Rethink Summit School Program. Welcome to ReThink Summit School Program: A Program Designed to Stop Cyberbullying and Promote Positivity at Your School*. Repéré le 7 décembre 2024 à : https://www.rethinkwords.com/rethinksummit.

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*, *36*(1), 1-17.

Salawu, S., He, Y. & Lumsden, J. (2017). Approaches to automated detection of cyberbullying: A survey. *IEEE Transactions on Affective Computing*, *11*(1), 3-24.

Schimmele, C., Fonberg, J., & Schellenberg, G. (2021). Évaluations que font les Canadiens des médias sociaux dans leur vie". *Rapports économiques et sociaux*, Statistique Canada, vol. 1 no 3, produit no 36-28-0001. Repéré le 2 décembre 2024 à : https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-fra.htm.

SCF (2016). *Relations NETtes. Guide d'animation*. Secrétariat à la condition féminine du Québec (SCF), Y des femmes de Montréal, 1-40. Repéré le 2 décembre 2024 à : https://www.ydesfemmesmtl.org/services-jeunesse/outils/relations-nettes/

Schultze-Krumbholz, A. et al. (2016). Feeling cybervictims' pain—The effect of empathy training on cyberbullying. *Aggressive behavior*, *42*(2), 147-156.

Sécurité publique Canada (s. d.). *Fiche de renseignement : Cyberintimidation*. Repéré le 17 avril 2023 à https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2015-r038/2015-r038-fra.pdf.

Serra, S.M. & Venter, H.S. (2011). Mobile Cyber-Bullying: A Proposal for a Pre-Emptive Approach to Risk Mitigation by Employing Digital Forensic Readiness. In *2011 Information Security South Africa (ISSA)*, IEEE, 1–5.

SPVM (s.d.). *Cyberintimidation*. Repéré le 18 novembre 2024 à : https://spvm.qc.ca/fr/Fiches/Details/Cyberintimidation.

Stassin, B. (2022). La prévention du harcèlement et du cyberharcèlement à l'école. Dans *Acte du colloque : Éducation, numérique, cohésion sociale et politiques publiques*, 73–88.

Statistique Canada (2009). *Enquête sociale générale de 2009*, fichier de microdonnées à grande diffusion, adapté par l'Institut de la statistique du Québec. Repéré le 3 décembre 2024 à https://www150.statcan.gc.ca/n1/pub/45-25-0001/index-fra.htm

Statistique Canada (2023, 21 février). *La cyberintimidation chez les jeunes au Canada* [Infographie]. Repéré le 20 novembre 2024 à : https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2023017-fra.htm.

StopBullying (2021). *California Anti-Bullying Laws & Policies*. Repéré le 24 novembre 2024 à : https://www.stopbullying.gov/resources/laws/california.

Strohmeier, D., Hoffmann, C., Schiller, E. M., Stefanek, E., & Spiel, C. (2012). ViSC social competence program. *New directions for youth development*, *2012*(133), 71-84.

Stupp, C. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. *The Wall Street Journal*, *30*(08).

Tison, F. (2019, 12 décembre). *Retour sur nos entrevues marquantes de 2019 : les gameuses systématiquement harcelées.* Espresso Jobs.com. Repéré le 5 décembre 2024 à https://www.espresso-jobs.com/article/9215/les-gameuses-du-quebec-systematiquement-harcelees-en-ligne.

Van Ouytsel, J. et al. (2019). Longitudinal associations between sexting, cyberbullying, and bullying among adolescents: Cross-lagged panel analysis. *Journal of adolescence*, *73*, 36-41.

Vann, V. (2020, 21 janvier). *What is an Internet Troll? (and How to Handle Trolls)*. *How-to Geek*. Repéré le 2 décembre 2024 à : https://www.howtogeek.com/465416/what-is-an-internet-troll-and-how-to-handle-trolls/.

Vie publique (2023, 10 mai). *Conseil des ministres du 10 mai 2023 : Sécurisation et régulation de l'espace numérique*. Repéré le 12 novembre 2024 à : https://www.vie-publique.fr/discours/289346-conseil-ministres-10052023-securisation-regulation-de-l-espace-numerique.

We are Social (2023). *Notre April Statshot report avec les toutes dernières tendances du web et du social media est sorti !* Repéré le 13 novembre 2024 à : https://wearesocial.com/fr/blog/2023/04/les-derniers-chiffres-du-numerique-avril-2023/.

Web Foundation (2022a, 21 sept.). *Strengthening Accountability for Online Gender-Based Violence – one year later*. Repéré le 2 décembre 2024 à : https://webfoundation.org/research/strengthening-accountability-for-online-gender-based-violence-one-year-later/.

Web Foundation (2021, 1er juill.). *Facebook, Google, TikTok and Twitter make unprecedented commitments to tackle the abuse of women on their platforms*. Repéré le 2 décembre 2024 à : https://webfoundation.org/2021/07/generation-equality-commitments/.

Web Foundation (2022b, 21 sept.). *Building Blocks for OGBV Accountability*. Repéré le 2 décembre 2024 à : https://webfoundation.org/2022/09/building-blocks-for-ogbv-accountability/.

Wikipédia (s.d.). *Doxing.* Repéré le 7 décembre 2024 à : https://en.wikipedia.org/wiki/Doxing.

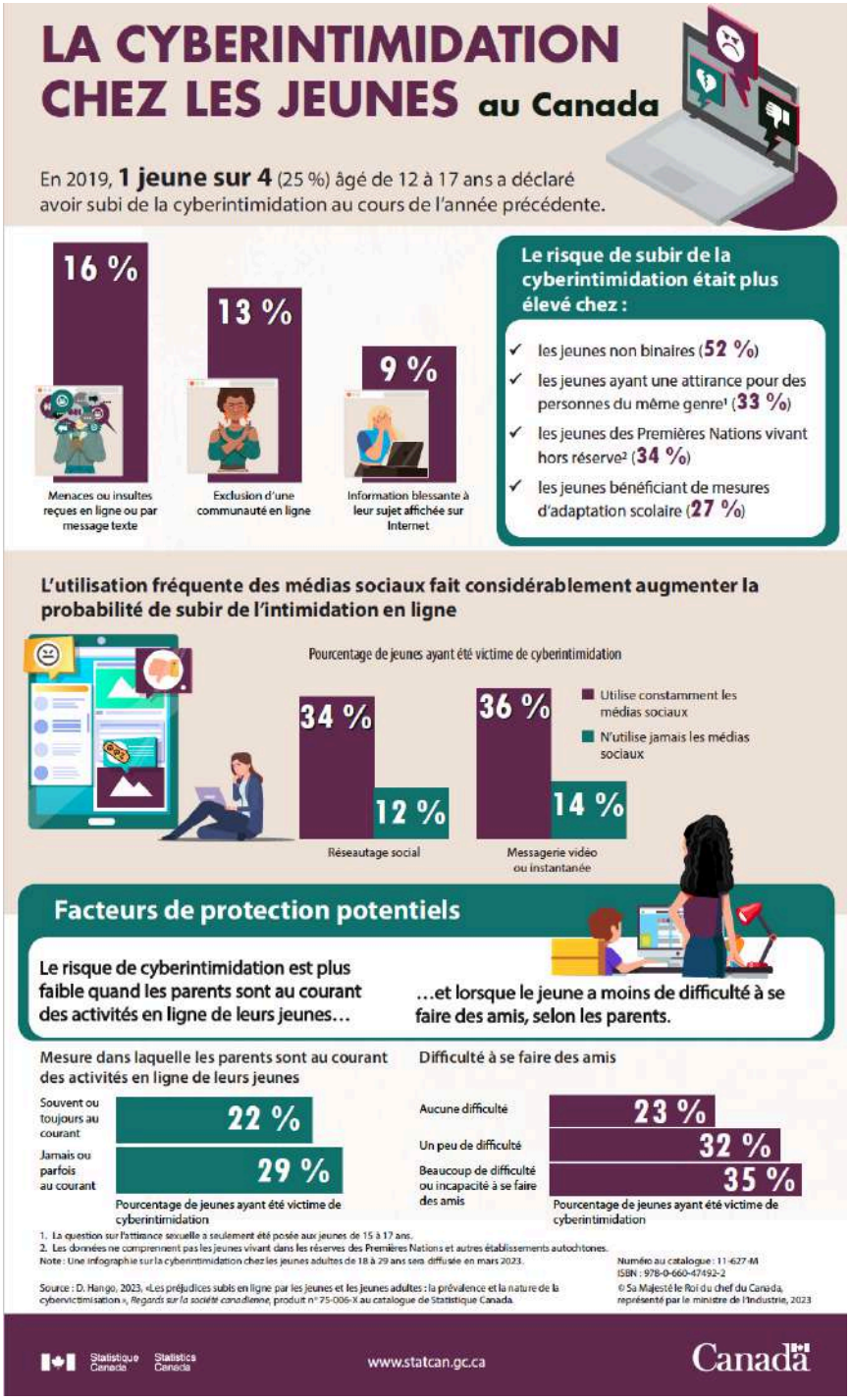
Wikipedia (2022). *Revenge Porn.* Repéré le 24 novembre 2024 à : https://en.wikipedia.org/wiki/Revenge_porn.

Yagoubi, A. (2020). Cultures et inégalités numériques : usages numériques des jeunes au Québec. *Printemps numérique*, *Jeunesse QC 2030*, 236 pages.

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. In *Frontiers in Public Health*, vol. 9, p. 634909.

ANNEXES

Annexe 1. La cyberintimidation chez les jeunes au Canada



Annexe 2. Les situations de cyberviolence

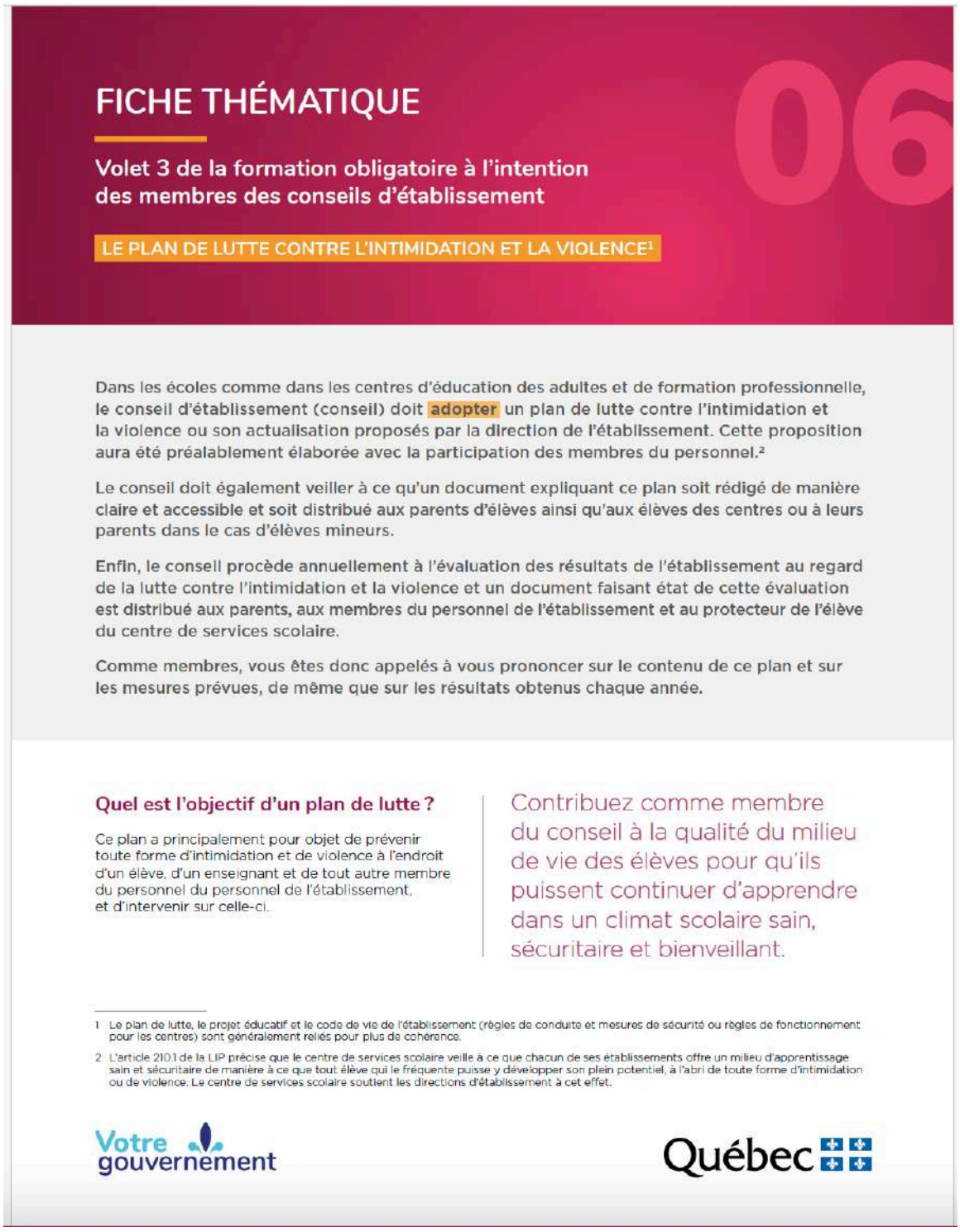
Les questions et exemples ci-dessous sont extraits de Hango (2016), elles permettent d'identifier des situations de cyberviolences.

Questions pour identifier des situations de cyberviolence	
Exemples de questions pour détecter si une personne est victime de cyberintimidation	
Variable 1	« Cyberintimidation : Avez-vous reçu des courriels ou des messages instantanés menaçants ou agressifs dont vous étiez le seul destinataire ? » (Hango, 2016 :12)
Variable 2	« Cyberintimidation : Avez-vous été la cible de commentaires menaçants ou agressifs diffusés dans des courriels ou des messages instantanés de groupe ou publiés sur des sites Internet ? » (Hango, 2016 :12)
Variable 3	« Cyberintimidation : Une personne a-t-elle déjà envoyé ou publié des photos qui vous ont embarrassé ou que vous avez ressenties comme une menace ? » (Hango, 2016 :12)
Variable 4	« Cyberintimidation : Une personne a-t-elle déjà utilisé votre identité pour envoyer ou publier des renseignements embarrassants ou menaçants? » (Hango, 2016 :12)
Variable 5	« Cyberintimidation : Avez-vous déjà été la cible de tout autre type de cyberharcèlement ou cyberintimidation (c'est-à-dire l'utilisation d'Internet pour embarrasser, intimider ou menacer une personne) n'ayant pas été mentionné ? » (Hango, 2016 :12)
Autres questions renseignant une situation de cyberintimidation	
As-tu déjà subi de la cyberintimidation et à quelle fréquence ?	
	- Quelqu'un a affiché de l'information blessante à ton sujet sur Internet - Quelqu'un t'a menacé ou insulté par courriel, par messagerie instantanée, par message texte ou dans un jeu en ligne - Quelqu'un t'a par exprès exclu d'une communauté en ligne - Quelqu'un a-t-il utiliser de manière abusive de photos, de vidéos ou d'autre contenu personnel (Hango, 2023 : 18)

Questions pour détecter si une personne est victime de cyberharcèlement	
Variable 6	« Harcèlement (communication) : Une personne vous a-t-elle déjà envoyé des messages non souhaités par courriels, messages texte, Facebook ou tout autre réseau social ? » (Hango, 2016 :13)
Variable 7	« Harcèlement (menace) : Une personne a-t-elle déjà publié des informations ou photos inappropriées, indésirables ou personnelles sur vous sur un site de réseau social ? » (Hango, 2016 :13)
Autres questions renseignant une situation de cyberharcèlement	
As-tu subi de la discrimination, du harcèlement, de l'intimidation sur Internet ? Sous quelle forme ? (Hango, 2023 : 18)	
Questions renseignant une mauvaise expérience sur Internet	
As-tu vécu de mauvaises expériences sur Internet ? Sur quelle plateforme ? Avec quelle intensité (durée, fréquence) ? (Hango, 2023 : 18)	
	- Tu as reçu des courriels ou des messages instantanés au contenu menaçant ou agressif dont tu étais le ou la seul.e destinataire - Tu as été la cible de commentaires au contenu menaçant ou agressif envoyés dans des courriels de groupe, par messages textes de groupe ou de publications dans les médias sociaux ou tout autre site Internet - Quelqu'un a envoyé ou affiché des photos qui t'ont embarrassé ou qui t'ont fait sentir menacé(e) - Quelqu'un a publié ou distribué, ou menacé de publier ou de distribuer, des vidéos ou des images intimes ou sexuellement explicites de toi, sans ton consentement - Quelqu'un t'a pressé d'envoyer, de partager ou de publier des images ou des messages sexuellement suggestifs ou explicites - Quelqu'un t'a envoyé des images ou des messages sexuellement suggestifs ou explicites, alors que tu ne voulais pas les recevoir - Quelqu'un a utilisé ton identité pour envoyer ou afficher des renseignements gênants ou menaçants te concernant - Tout autre type de mauvaises expériences

Annexe 3. Plan de lutte contre l'intimidation et la violence

Ce Plan permet à tous les établissements de contrer toutes formes de violence et intimidation. La cyberviolence et autres formes de cyberviolence sont prises en compte par les établissements (CSS, s.d).



FICHE THÉMATIQUE

06

Volet 3 de la formation obligatoire à l'intention des membres des conseils d'établissement

LE PLAN DE LUTTE CONTRE L'INTIMIDATION ET LA VIOLENCE[1]

Dans les écoles comme dans les centres d'éducation des adultes et de formation professionnelle, le conseil d'établissement (conseil) doit adopter un plan de lutte contre l'intimidation et la violence ou son actualisation proposés par la direction de l'établissement. Cette proposition aura été préalablement élaborée avec la participation des membres du personnel.[2]

Le conseil doit également veiller à ce qu'un document expliquant ce plan soit rédigé de manière claire et accessible et soit distribué aux parents d'élèves ainsi qu'aux élèves des centres ou à leurs parents dans le cas d'élèves mineurs.

Enfin, le conseil procède annuellement à l'évaluation des résultats de l'établissement au regard de la lutte contre l'intimidation et la violence et un document faisant état de cette évaluation est distribué aux parents, aux membres du personnel de l'établissement et au protecteur de l'élève du centre de services scolaire.

Comme membres, vous êtes donc appelés à vous prononcer sur le contenu de ce plan et sur les mesures prévues, de même que sur les résultats obtenus chaque année.

Quel est l'objectif d'un plan de lutte ?

Ce plan a principalement pour objet de prévenir toute forme d'intimidation et de violence à l'endroit d'un élève, d'un enseignant et de tout autre membre du personnel du personnel de l'établissement, et d'intervenir sur celle-ci.

Contribuez comme membre du conseil à la qualité du milieu de vie des élèves pour qu'ils puissent continuer d'apprendre dans un climat scolaire sain, sécuritaire et bienveillant.

1 Le plan de lutte, le projet éducatif et le code de vie de l'établissement (règles de conduite et mesures de sécurité ou règles de fonctionnement pour les centres) sont généralement reliés pour plus de cohérence.

2 L'article 2101 de la LIP précise que le centre de services scolaire veille à ce que chacun de ses établissements offre un milieu d'apprentissage sain et sécuritaire de manière à ce que tout élève qui le fréquente puisse y développer son plein potentiel, à l'abri de toute forme d'intimidation ou de violence. Le centre de services scolaire soutient les directions d'établissement à cet effet.

Votre gouvernement

Québec

Que contient ce plan ?

Ce plan doit notamment prévoir :

- une analyse de la situation de l'école ou du centre au regard des actes d'intimidation et de violence ;
- des mesures de prévention visant à contrer toute forme d'intimidation ou de violence ;
- des mesures visant à favoriser la collaboration des parents, ainsi que des parents des élèves mineurs et des élèves dans le cas des centres ;
- des modalités pour effectuer un signalement ou pour formuler une plainte ainsi que des mesures visant à assurer la confidentialité ;
- des actions qui doivent être prises lorsqu'un acte d'intimidation ou de violence est constaté ;
- des mesures de soutien ou d'encadrement offertes à un élève victime, à un témoin ou à l'auteur d'un tel acte ;
- des sanctions disciplinaires applicables selon la gravité ou le caractère répétitif de ces actes et du suivi qui doit être donné à tout signalement et à toute plainte.

Que se passe-t-il lors de l'adoption ?

Avant même de délibérer au conseil pour adopter le plan de lutte, vous devriez déjà avoir une idée des forces et défis de l'établissement (ex. : enjeux particuliers dans la cour d'école et les vestiaires), ce que doit contenir un plan de lutte et le format utilisé par l'établissement (ex. : des modèles récents ou un exemple de l'année dernière).

Lors de la séance de votre conseil, il est possible d'apporter, au besoin, des précisions ou des bonifications au plan, ou de retirer des éléments, toujours dans l'intérêt des élèves et en fonction des constats issus du portrait de situation réalisé par l'équipe-école ou l'équipe-centre.

Qui en assure la coordination ?

La direction assiste le conseil en coordonnant, avec le personnel de l'école, l'élaboration, la révision et, le cas échéant, l'actualisation du plan de lutte contre l'intimidation et la violence.

Comment le plan peut-il être diffusé, de même que ses résultats ?

Une fois le plan adopté, le conseil **s'assure qu'un document clair et accessible** est distribué aux parents d'élèves, aux élèves dans le cas des centres, ou à leurs parents dans le cas d'élèves mineurs.

En ce qui a trait à l'évaluation des résultats de l'établissement au regard de la lutte contre l'intimidation et la violence et du document devant faire état de cette évaluation aux parents, aux membres du personnel de l'établissement et au protecteur de l'élève du centre de services scolaire, cette responsabilité appartient effectivement au conseil, avec le soutien de la direction.

Cette évaluation et ce document peuvent prendre différentes formes selon les milieux (résultats mentionnés dans le rapport annuel du conseil, plan et évaluation présentés lors de l'assemblée générale annuelle, etc.). Les forces et défis de l'établissement peuvent y être mentionnés : meilleur climat scolaire en général, sentiment de sécurité accru selon un sondage réalisé auprès des élèves, problématiques réglées dans certaines zones, mesures ayant donné de bons résultats, formations à planifier pour l'an prochain compte tenu de certains résultats liés aux habiletés sociales des élèves, etc.

Suggestion de questions pour les membres

- Quel est le portrait de situation actuelle de notre établissement au regard des actes d'intimidation et de violence ?
- À quel moment cette analyse de situation a-t-elle été réalisée la dernière fois ? Qui a été consulté ? Par quels moyens ?
- Quels constats se dégagent ?
- Quelles mesures ou stratégies sont prévues au plan et pourrions-nous les préciser davantage au besoin ?
- Au cours de l'année dernière, quelles ont été les principales mesures de prévention et d'intervention mises en œuvre dans notre milieu ?
- Quels changements sont apportés au plan de lutte comparativement à l'année dernière ? Qu'est-ce qui justifie ces changements ?
- Quelles informations permettront aux parents, et aux élèves dans le cas des centres, de bien comprendre le plan de lutte et quels moyens de diffusion doit-on privilégier pour les rejoindre ?

Mise en garde

La présente fiche constitue un outil de vulgarisation juridique. Elle ne remplace aucunement les textes de loi en vigueur, lesquels prévalent. Les lecteurs doivent se référer directement aux lois et règlements sous la responsabilité du ministre de l'Éducation, notamment la *Loi sur l'instruction publique*, afin de connaître toutes les dispositions applicables au conseil d'établissement, plusieurs d'entre elles n'étant pas présentées dans ce document.

PRINCIPAUX ARTICLES DE LOI

- **Articles 75.1 à 75.3, 77, 83.1 et 96.13 de la *Loi sur l'instruction publique* (LIP) (école) ;**
- **Articles 110.4 et 110.13 de la LIP (centre d'éducation des adultes et centre de formation professionnelle) (centre)**

Éducation Québec

CONSEILS + BONNES PRATIQUES

- **Connaître les définitions de ce que sont globalement l'intimidation et la violence (voir l'article 13 de la LIP).**
- **Sonder les personnes que vous représentez et proposer des idées inspirées des commentaires obtenus pour bonifier le plan de lutte.**
- **Engager une discussion pour mieux connaître les différents aspects qui favorisent un climat scolaire sain, sécuritaire et bienveillant et ainsi dégager une vision commune et partagée au sein du conseil, et liée à celle que préconise l'équipe-école ou l'équipe-centre.**
- **Ajouter un point statutaire à l'ordre du jour des séances du conseil concernant le plan de lutte (information, suivi ou résultats sur un sujet en particulier).**
- **Réserver une section sur le site Web de l'établissement pour les informations que le conseil doit diffuser dans le cadre de son mandat (dépliant résumant le plan de lutte, résultats obtenus au terme d'une année, etc.).**

20-115-089-06-4

Annexe 4. Stopcybersexisme

Rapport réalisé dans le cadre du Programme de soutien financier *Ensemble contre l'intimidation* du ministère de la Famille du Québec (MFA)

- Responsable de la recherche et de la rédaction : Dre Amina Yagoubi, Sociologue Ph.D, AKY-Conseils.
- Production et édition : Printemps numérique.

Le présent rapport complète le projet du « Référentiel de compétences de prévention de la cyberintimidation chez les jeunes » (2022-2025).

Citer le document : Yagoubi, A. (2025) *Cyberviolence chez les jeunes : Les défis de la Cyberintimidation* - Printemps numérique, p. 1-128

PRINTEMPS
NUMÉRIQUE