**DIGITAL INCLUSION AND SOLIDARITY**

APRIL 2020

# CYBERBULLYING: A REVIEW OF THE LITERATURE

RENAISSANCE numerique

# PREFACE

This note aims to offer an overview of the existing academic research on the subject of cyberbullying - specifically cyberbullying among young people - that could inform the French response to this challenge. This note is organized according to the main themes that occur in the literature, with a specific attention paid to intervention (prevention, detection, response). An index is provided at the end of the note highlighting international best practices and offering further resources. Concrete recommendations are also provided for all of the identified stakeholders. The academic research in this field presents certain weaknesses, partly because of the challenges of data collection and the relatively slow pace of academic production compared to the rapid rate at which the internet and online behavior evolves. This weakness is even more pronounced in the French literature. For that reason, this note mostly relies on anglophone research.

# TABLE OF CONTENTS

# KEY FINDINGS

- Cyberviolence consists of occasional acts of violence whereas cyberbullying consists of repeated acts of violence.
- A power imbalance between the bully and victim may be linked to an imbalanced familiarity with digital tools.
- The reflex for represial can be stronger in cyberbullying, turning the victim into the aggressor.
- Most cases of cyberbullying occur outside of the school environment.
- Cyberbullying effects disproportionately: girls, members of sexual, racial and ethnic minorities and children suffering from mental health or behavioral issues.
- Victims supported or defended by bystanders are less depressed and anxious, have better self esteem and are less rejected by their peers.
- When children understand that cyberbullying isn't the norm, bullying rates decrease.
- School programs to address cyberbullying are less efficient when they are conceived for the short-term rather than the long-term.
- Students often feel that teachers and adults are not sufficiently aware of the problem, and are therefore unable to properly intervene.
- There is a phenomenon of migration of bullying activity between platforms that deserves further investigation.
- Children rarely read and understand the privacy policies of the services they use, and do not fully understand the boundaries between public and private in these spaces, or the diverse security options and recourse mechanisms that are available to them.
- The most effective prevention and detection programs involve children themselves.
- Despite a proliferation of resources availables online on cyberbullying, searching for advice online as a coping mechanism for victims is less efficient than other strategies.

# PART 1
# A BETTER UNDERSTANDING OF THE CONCEPT



## CYBERBULLYING VS. "TRADITIONAL" BULLYING

Cyberbullying is often defined by enlarging the definition of "traditional" bullying, which relies on three main criteria: 1) intentionally aggressive behavior, 2) repeated actions, and 3) an interpersonal relationship characterised by a systemic imbalance in power (Olweus, 1993). Cyberbullying describes a behavior that encapsulates those three criteria and that relies on electronic forms of contact (Kowalski and al., 2012, 2014 ; Patchin and Hinduja, 2012). Blaya reaffirms the importance of the repetitive aspect in cyberbullying and distinguishes it from cyberviolence. For Blaya, **cyberviolence consists of occasional acts of violence, whereas cyberbullying consists of repeated acts of violence, at least once a week over the course of a month** (Blaya, 2018).

There are some theoretical and practical limits to the applicability of these three characteristics to cyberbullying. For example, intent is difficult to determine in an online environment (Hee and al., 2018). The concept of repetition in cyberbullying is not simple either, because digital technologies provide the aggressors with a means to propagate their actions, so that a single act can become repetitive over time (Slonje and al., 2012). **In regards to power imbalance, the relative power dynamic in cyberbullying can be linked to skills with digital tools** (Cross and al., 2009). The question of knowing whether cyberbullying should limit itself to relations between peers, despite the fact that not all forms of cyberbullying occur between peers, is also the subject of debate. (Cross and al., 2009).

Because cyberbullying occurs (at least for the most part), in a virtual environment, the aggressors are not always conscious of the consequences of their actions and of their effects on their victims (Blaya, 2013). The anonymity possible in cyberbullying is often mentioned as a significant difference from traditional bullying. But many other differences have been noted. Cyberbullying has been associated to more serious consequences, including severe psychological suffering in victims (Kim and Song, 2013 ; Song, 2017). The victims often face this intimidation alone, isolated in cyberspace, which can cause a more severe psychological shock (Cho, 2013 ; Seo et Cho, 2013). **The reflex of reprisal can also be stronger in cyberbullying, with the possibility of the victim becoming the aggressor** (Kowalski et Limber, 2007).

According to Slonje, despite a significant overlap between "traditional" bullying and cyberbullying (Salmivalli et Pöyhönen, 2012), **most cases of cyberbullying happen outside of school** (Slonje and al., 2012). In France, a study conducted in 2014 by Kubiszewski and al. on the overlap of cyberbullying and bullying at school among French teenagers showed that "cyberbullying is not part of school bullying, but rather offers to other students new possibilities to bully" (Kubiszewski and al., 2014). **It was frequently noted that the locations of cyberbullying reflect the most commonly used technologies of the time** (Whittaker et Kowalski, 2014) **and are thus directly linked to the context and are constantly changing.** According to the NGO *Ditch The Label*, which conducts a yearly survey on bullying among high school and college students, cyberbullying is most common on Instagram (42%), followed by Facebook (37%) and Snapchat (31%) (Ditch the Label, 2017). **There is also a significant trans-platform aspect to cyberbullying: bullies can begin bullying on one platform and move to another one; bullies can reach their victim through other platforms than the one on which the bullying started on.** Further research is necessary to fully understand this migration phenomenon.

# TYPOLOGIES OF BULLYING

## THE DIFFERENT ROLES

Many responses to bullying, especially regarding the use of artificial intelligence technologies and the detection of cyberbullying, focus on the binary relationship bully/bullied. **However, a fair amount of the research on cyberbullying deals with the identification of the different roles of the participants and witnesses, as well as on the exploration of the range of participation in cyberbullying between bullies and victims**.

Hee and al. focus on four different roles: victim, bully, defender of the victim and assistant to the bully. Vanderbosch and al. identify three types of witnesses: those who take part in the bullying, those who help the victim and those who do nothing (Salmivalli and al., 1996 ; Vandebosch and al., 2018 ; Hee and al., 2018). Research on traditional bullying has identified up to eight different type of reactions among witnesses (Olweus, 2001). **It is important to point out that victims that are supported or defended by witnesses are less depressed and anxious, have better self esteem and are in the end less rejected by their peers than those who are not supported by bystanders** (Sainio, Veenstra, Huitsing, et Salmivalli, 2011).

## CYBERBULLYING TACTICS

The following list includes actions that are generally considered as cyberbullying "tactics". The behaviours can be more specific depending on the digital platform used. This thematically organized list is a synthesis of resources by *StopBullying.gov*, a website of the American federal government managed by the Department of Health and Social Services, the American *Anti-Defamation League* and *CyberMentors*, a program launched in the United Kingdom by the Prime Minister and professor Tanya Byron in 2009.

There is a spectrum of online bullying that ranges from "non-technical" to practices that approach forms of hacking and cybercrime. This reinforces the aforementioned notion of a power imbalance between those who have technical skills of an advanced level and those who do not.

| Themes | Cyberbullying "tactics" |
|---|---|
| Exclusion | • Deliberately excluding a person from online games or groups |
| Threats, intimidation, provocation, incentives to self-harm | • Sending someone threatening or disturbing messages, threatening to hurt someone, telling someone to kill themself<br>• Creating hateful websites or online groups against one person<br>• Stealing someone's password and blocking access to their account<br>• "Trolling" : provoking someone through triggering behaviours<br>• "Flaming" : denigrating someone in an online public environnement using profane or vulgar language to assert power or establish a dominant position<br>• "Happy Slapping" : Physically assaulting or embarrassing a victim while filming/photographing the act and publishing the material online publicly<br>• "Cyberstalking" : Calling or messaging someone in a concerning, persistent, or pervasive manner to worry or frighten them<br>• Indirectly causing damages to someone's digital device (for example: infecting someone's computer with malware) |
| Privacy abuse or exposure | • Displaying of diffusing communication or images<br>• Diffusion of webcam images in a threatening or manipulative manner<br>• "Doxing" (abbreviated form of "document") : publishing someone's personal information (address, phone number, social media account information, and other private details) |
| Reputation damage, denigration | • Posting comments or rumors about someone online<br>• Publishing a denigrating photo or video<br>• Taking and sharing denigrating pictures or video (this can be considered a criminal act in the case of pornographic images or images of minors)<br>• Creating or voting for someone in an insulting online survey (polling/survey features are offered by many websites) |
| Severe defamation involving the authorities | • Making false allegations involving sensitive or inappropriate information to internet service providers about the victim<br>• Encouraging the victim to engage in online hacking<br>• Sharing false information claiming the victim is planning an attack |

| | |
|---|---|
| Identity theft | • Stealing an identity online<br>• Pretending to be someone else online in order to request personal information or share false information<br>• Usurping someone's identity to post comments that cause them harm<br>• "Mirroring": use a username resembling the victim's<br>• Subscribing someone to several pornographic marketing lists<br>• "Phishing": tricking, persuading or manipulating someone into revealing personal or financial information |
| Sexual bullying over digital media | • Recording images or video of the victim that could be interpreted as being of a sexual nature, usually without the victim's consent, and sharing this content publicly (this activity mostly targets girls)<br>• "Sextortion": exploiting someone for sexual favors by threatening to reveal information about them (often, by threatening to expose evidence of their sexual activities) |



# DEGREES OF VULNERABILITY ONLINE

Cyberbullying poses serious risks, and some children are more exposed or more vulnerable to it than others. Factors like sexual activity, identity or ethnicity can imply a more acute exposure to cyberbullying. **It was found that cyberbullying disproportionately affects girls, members of sexual, racial or ethnic minorities, and children suffering from mental health or behavioural issues** (Rice and al., 2015). **Cyberbullying often implies sexual harassment and sexual shaming linked to sexual activity or orientation** (Shariff, 2008). In the United Kingdom for example, girls are two times more likely than boys to be victims of cyberbullying, as well as non-British children and children from ethnic minorities. Blaya also notes in her research a **rise in "fat-phobia"** or cyber violence against overweight children.

Beyond characteristics linked to identity, **the balance of power observed in cyberbullying interactions can be linked to gaps in terms of digital skills**. The British program *Cybermentors* rejects the idea that young people are intrinsically vulnerable online and that staying off-line will keep them safe. They maintain that the **young people with limited digital access and experience are particularly vulnerable because of their lack of knowledge of digital tools** (Cross and al. 2009).

# PART 2
# RESPONSES AND MECHANISMS OF THE DIFFERENT ACTORS



## STRATEGIES OF THE PLATFORMS: PATHWAYS FOR IMPROVEMENT

Online platforms are often criticized for their lack of regulation of cyberviolence and inadequate moderation policies. Beyond this, it was noted that privacy protection policies and recourse mechanisms are insufficient or not sufficiently accessible. Livingstone and Haddon note that **children rarely read or understand confidentiality policies of the services that they use and they do not understand the limits between public and private in these spaces, nor the diverse security and recourse options that are offered to them.** According to Livingstone and Haddon, "part of this problem can be fixed with media education, [but] generally, a better regulation and better interface design are necessary." (Livingstone and Haddon, 2009)

In his investigation about platform responses to the phenomenon of cyberbullying, Milosevic notes that certain companies also create "safety corners" that redirect users to associations and services in order to find help or information. These "safety corners" share videos and pedagogic texts developed by companies in collaboration with associations (Milosevic, 2016). But the efficiency of these security centers has not been properly evaluated.

**Even with limited functionalities, platforms can still be misused** (Hinduja, 2016). For example, Snapchat has rules that are supposed to prevent cyberbullying, however it is still possible to take a screenshot of an image and to share them through other mobile app, including an app called *Snap Save*, which allows the user to take screenshots and anonymous recordings. Further investigation is needed on this topic.

## PROACTIVE CONTENT MODERATION

Many platforms use proactive content moderation strategies that rely on technology. The automatic surveillance of content and interactions, which enables the detection of cases of cyberbullying as soon as they appear, is one such practices (Dinakar, Jones, Havasi, Lieberman, et Picard, 2012 ; Xu, Jun, Zhu, et Bellmore, 2012). Some platforms also use "pre-filtering" or "sentiment analysis" : when a person publishes a "deviant" word, the system compares the message to a database of "bad words". The platform can then send a message to the user along the lines of "Are you sure you want to post this ?", in order to deter the author from publishing a message that transgresses the community guidelines. In addition, the system can verify the level of seriousness of the message and submit the reported content to a human moderator for more thorough examination (Milosevic, 2016). Automated prevention and detection of cyberbullying constitutes a major trend among platforms and within scientific research. Technologies of artificial intelligence - including machine learning and deep learning - allow the identification of potentially dangerous messages with growing precision (Hee and al., 2018 ; Agrawal et Aweka, 2018 ; Al-Garadi and al., 2018). **However these technologies can still yield false positives, deleting valid content by mistake, which could undermine users rights to freedom of expression** (Milosevic, 2016). Generally speaking, IA are forced to make binary classification (bullying vs. non-bullying) and are unable to grasp the subtlety in discourse; indeed, human discourse evolves constantly. Moreover, **artificial intelligence cannot provide the same emotional support and advice as human engagement, and it does not involve peers and bystanders in a constructive way.**



# PREVENTION THROUGH PEDAGOGY

A growing attention is granted to media literacy practices (MLA). MLA aims at addressing cyberbullying by teaching children to think before communicating online, to use technology in a ethical and responsible manner, to discern the nature and quality of online content, etc. **When children understand that cyberbullying is not the societal norm, intimidation rates decrease** (Barbara, 2010). Rather than considering that cyberbullying is a common and inevitable phenomenon, children should understand the real prevalence of cyberbullying. The Canadian NGO MediaSmarts considers that children must understand the emotional effects of cyberbullying to counterbalance a digital culture that is influenced by feelings of apathy and mechanisms of separation: "What can seem like a joke can have a powerful effect on another person".

School programs to address cyberbullying are becoming more and more widespread, but they tend to be inefficient if they fall into clichés and stereotypes, or if they present unrealistic scenarios. Such programs are also less efficient if they are conceived for a limited period of time or ad-hoc, rather than integrated into the curriculum throughout the year. According to the study "Young Canadians in a Wired World" by MediaSmarts, young people consider that anti-cyberbullying programs that are administered only once (during school assemblies for example) have the effect of trivializing the problem. According to the same study, "zero tolerance" policies in schools have made children reluctant to report cases of cyberbullying, in fear of the effects on their peers (Valerie, 2012).

Teacher training is a major axis of prevention strategy at school, particularly important when teachers do not have the same comprehension of digital tools and cyberbullying trends as children. **Students often feel that teachers and adults are not sufficiently aware of the problem or are unable to properly help them, which discourages them from reaching out for help.** (Slonje and Smith, 2008 ; Slonje 2012). Byrne shows that school nurses may be particularly well positioned to help victims of cyberbullying and that they should be trained to do so (Byrne, 2018).

The work of Slonje and al. echos the conclusion of the MediaSmarts study, and recommends that cyberbullying programs to be integrated into holistic and continuous school policies.

## CHILDREN'S COPING MECHANISMS

The children that are victims of cyberbullying develop different strategies to protect themselves with regard to the digital aspects: blocking online contacts, changing usernames and electronic addresses, deleting messages without reading them (Aricak and al., 2008 ; Smith and al. 2008). Currently, **blocking messages and users seems to be children's preferred option**, although some children opt for more conflictual reactions, by directly answering bullies (Aricak and al., 2008 ; Smith and al., 2008). **The desire to react can be stronger in cyberbullying than in offline bullying, by inciting the victim to become the bully** (Kowalski and Limber, 2007). It can be particularly important for bullies to understand the results of their actions in order to prevent cyclic behaviour, given that the reflex of represail is stronger in cyberbullying (Kowalski and Limber, 2007 ; Slonje and al., 2012).

Knowing how victims face cyberbullying and assessing the efficiency of their strategies raises many methodological challenges. In a study conducted in 2013 on Czech children, Machakova and al. examined the experiences and reactions of children facing cyberbullying. To make a more precise assessment of the efficiency of their strategies, they distinguish between coping mechanisms of victims of severe cyberbullying and the reactions of children suffering from less serious forms of cyberbullying.

The researchers came to the conclusion that the most useful strategies are:

- technological solutions that block contact, by changing profiles or phone numbers, etc.
- avoiding the website
- seeking support



The less useful strategies are:

- reprisals
- confrontation
- searching for advice online

In the study, more than half of the victims chose the delete the cyberbully from their contact list and changed their settings to block them. But they avoided more radical strategies, like changing their own usernames or phone numbers, or deleting their profile (Machackova and al., 2013). It is also interesting to note that while technological solutions have proven themselves to be among the more efficient methods, **online searches for advice appeared to be less efficient.** The researchers believe that this might be linked to be the quality and the accessibility of online advice and recommendations. Despite the wide variety of online resources, the act of search for quality online content can be challenging.

## RESPONSES TO CYBERBULLYING

*The following list is drawn from HelpGuide.org, a non-profit organisation based in the United States, and from Ditch the Label, a charitable organisation based in the UK. It consists of generic advice, non-specific to the French context.*



- In general, do not answer. Avoid reprisal or further aggravating the situation.
- If you can, take a screenshot and keep a recording on your computer.
- Block the user-bully.
- Report the user-bully. You can report their actions to your ISP (internet service provider), or to the social network or website that they use to bully you. Cyberbullying can be a violation of the terms of use of the social network or website, and according to the applicable laws in your area, may even justify criminal accusation.
- Depending on the service, you can increase your privacy settings.
- If the intimidation persists, you can change your phone number or delete your account.
- If the bullying involves a classmate, report the bully to a teacher or to a member of the school staff.
- Speak to someone about the incident for support, as well as to document the event.
- If somebody is threatening you, sharing your personal information or making you fear for your safety, talk to an adult as soon as possible.



# INVOLVING CHILDREN IN AN EFFICIENT RESPONSE

**Most successful prevention and intervention programs involve children themselves,** attesting to the importance of peer-programs, bystander intervention and children's responsibility in general. The program *Cybermentors* received a very positive evaluation from researchers in this regard (Banerjee, Robinson, et Smalley, 2010 ; Thompson et Smith, 2011). In the *Cybermentors* program, youth between the age of 11 to 25 were trained online via an a peer-support web training. **It has been demonstrated that the peer-to-peer system made the children feel safe, while the website feature of the resource allowed them to keep a reassuring and familiar distance.** In addition, security measures were integrated into the process to help report dangerous behaviour, and qualified counsellors were available if needed (Cross and al., 2009).

**The role or peers as bystanders is also crucial** (Hawkins, Pepler, et Craig, 2001 ; Oh et Hazler, 2009 ; Song, 2017). **Witnesses that intervene in a positive way in cyberbullying, or traditional bullying are often referred to as "upstanders"** : active witnesses, that react in defense or support of the victim, or that report the intimidation (*StopBullying.gov, OnlineSense.org*). There are many initiatives and campaigns that encourage peers to be "upstanders" and to provide forms of support. Despite a general consensus in the research that the positive intervention by witnesses lessens the problem of cyberbullying, witnesses do not necessarily act when they notice this type of situation (Whittaker et Kowalski, 2015). Additional research is needed about how to encourage witnesses to intervene in a positive manner.

**Hinduja and Patchin (2017) highlight the importance of resilience among young people, despite this being often neglected in the debate on cyberbullying.** Studying a sample of young Americans, researchers have found that the young people able to react are less likely to be hurt. Resilience is un-

derstood as “the capacity to bounce back, to successfully adapt when faced with adversity, and to develop social and academic skills despite severe exposure to stress, or simply the stress of today’s world” (Henderson and Milstein, 2003) and is a product of diverse internal and external factors (Hinduja and Patchin, 2017). Building resilience among young people is related to both empowering them in their digital environments and taking a holistic approach to the problem, raising awareness about the technical and social dimensions.



# RECOMMENDATIONS BY STAKEHOLDER

## SCHOOLS

- Schools should establish policies and procedures that are clear, transparent, easy to understand, and well communicated. These policies must specify the responses that the schools take to cyberbullying incidents, including the timeframe, designated contacts, and support mechanisms available to the victims and to bullies. Schools should have a clear protocol and mapping of the response system.

- Schools must prioritize the implementation of holistic and integrated programs of awareness raising and prevention, rather than occasional or ad hoc interventions.

- Schools should provide necessary support and training to teachers and other staff members.

- Schools should implement policies and mechanisms to encourage children to report cyberbullying.

- Schools should aim to implement to peer-to-peer programs as much as possible.

- Programs should combine elements of online and offline support.

- Training on cyberbullying should be included in relation to empathy and diversity trainings.

- Digital literacy should not be limited to MLA (media literacy education) and should include an understanding of the Internet and the Web as a whole, the workings of social network mechanisms (such as algorithms, virality, privacy settings) and should encourage online citizenship.



## PLATFORMS

- Many platforms experiment with new functionalities that aim to limit cyberbullying and to ensure victims' security, for example with the tool "Restrict" on Instagram : with this feature, comments on accounts that you choose to "restrict" will not be publicly displayed in your comment section (unless you accept them), and restricted users will not be able to see when you are online or if you have read their direct messages. This type of additional feature is useful for those who are hesitant about blocking their bullies. Platforms are also experimenting with pulling back features that encourage virality (the "like" button, number of "followers" displayed, etc.). Deleting these mechanisms can change the design of the platforms that enable online intimidation. There is work to do in terms of "civic by design" approach (inspired by the logic of "privacy by design"), in order to develop new features and options for protection to users. Companies should reinforce their reporting procedures and improve user experience to move from reactivity and receptivity.

- Platforms should make sure that their services are compliant with laws on bullying, privacy and security.

- Data privacy is especially important given the sensitive nature of children's' personal data. Platforms should commit to the protection of children's data. Beyond strict compliance with the European General Data Protection Regulator, this requires platforms to explain data and privacy policies in a way that the children can comprehend. This also implies not sharing children's data with third parties.

- Online interactions - anonymised to protect privacy - could be useful for researchers working on the subject. For example, much the current research on social media behavior is conducted about Twitter in part because it is easier to scrape data there, but this implies less visibility into dynamics on other platforms.

- Even though official platform policies tend to appear on websites, those policies do not always explain how anti-cyberbullying mechanisms work. Platforms should make their algorithms transparent and explainable in order to allow researchers to inspect them and suggest improvement, but also to allow the public to understand the mediation of their online interactions. Of course, transparency in not an end in itself, rather a necessary step to understand which solutions are efficient regarding young users.

## FAMILIES

- Families have an essential role to play in an efficient anti-cyberbullying strategy. It was found in the research that their involvement reduces bullying and victimisation.

- Families should understand the modalities and parameters of confidentiality on profiles and accounts. They should be familiar with the different ways in which they can reduce the number of people that can contact their child, as well as the amount of information that is publicly available about them online.

- Families should know what to do when confronted with cyberbullying: how to report it and what measures to take. They can report cyberbullying to schools, local authorities, and social network or to internet provider services.

- Families should talk with their children about the type of content that would be appropriate and inappropriate for them to share online. Even though children believe in their right to privacy online, families have the responsibility to accompany them, without being intrusive.

- Families and children should discuss what parents should know of their children's online interactions.

- Families should pay attention to symptoms of cyberbullying - as described for example by the Cyberbullying Research Center, Cyberbullying.org

- Families should take a critical look at the resources and advice available online, given that such material is not always accurate or helpful, and may sometimes be serving commercial purposes.



## PUBLIC AUTHORITIES

- Support to families should be a top priority. Public authorities should make sure that the training that is available to families is accessible, and they should provide resources for families with vulnerable children or children with special needs.

- Public authorities should involve children in the elaboration of policies and practices. This can be done in part through the allocation of grants to youth programs that allow young people to develop and undertake their own initiatives to fight cyberbullying.

- Public authorities should finance research to measure the prevalence and the impact of cyberbullying on a national scale and an annual basis. This initiative could be conducted collaboratively between platforms and civil society.

- Public authorities should educate the public about the legal framework that exists already in relation to bullying and cyberbullying.

## CIVIL SOCIETY, ACADEMIA

- Neutral and thorough research is needed on the effects and modalities of cyberbullying, as well as on the efficiency of prevention and intervention strategies.

- **Researchers should not limit their focus to a few platforms, but rather consider the online ecosystem in its entirety and pay attention to the phenomenon of migration between platforms.**

- **Further research should be conducted on the phenomenon of the "active bystander" in order to better understand their motivations, the efficiency of their actions and the means to support this type of behaviour.**

- The majority of studies remain focused on school settings, but because cyberbullying does not limit itself to the school day, further research is needed into different settings.

- Civil society should look beyond the solution of media literacy education (MLA) as a "catch-all" response to online problems.

## CHILDREN

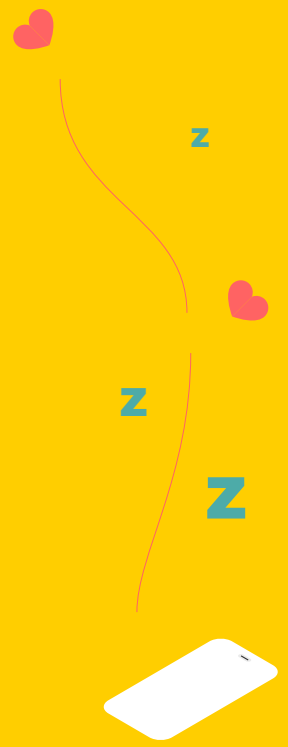
- As peers and classmates, children are particularly well positioned to be active bystanders in class and online. Children should report cases of cyberbullying in an appropriate manner when they are victims or witnesses. Programs and training mechanisms are essentials in that regard.

- Children should develop safe online habits, what is sometimes referred to as “digital hygiene”: using privacy settings, avoiding sharing sensitive information, etc.

- **The idea that going online necessarily jeopardizes children’s privacy and safety should not be banalized and accepted as the norm. It must be questioned how common these practices truly are.**



# APPENDICES



# BEST PRACTICES

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

- StopBullying.gov provides information by different governmental organisations about what constitutes bullying and cyberbullying, who is at risk and how to prevent and react to cyberbullying. The content is provided by the partners of the drafting committee, which works closely with the Secretary of Education, Health and Social Services.

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

- The Anti-Defamation League (ADL) is an NGO traditionally focused on antisemitism. It offers trainings and resources to fight prejudices and offers programs on bullying and cyberbullying in schools. ADL offers a range of interactive workshops for primary, middle and high schools.

Cyberbullying Research Center (USA) :
https://cyberbullying.org/

- The Cyberbullying Research Center is directed by Dr Sameer Hinduja (Florida Antlantic University) and Dr Justin W. Patchin (University of Wisconsin-Eau Claire). It serves as a center of information exchange about the way teengagers use and abuse technology. It offers studies, testimonies and other resources for parents, teachers, psychologists, police officers and young people themselves.

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

- The Queensland Anti-Cyberbullying Taskforce was created in february 2018 in order to elaborate a frame to fight cyberbullying for children and young people in Queensland, and recommends community measures to governments, parents, educators, children, schools, social media companies, community organisations and universities.

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

- The KiVa program, developed in Finland, is a universal school program which tackles the issue of cyberbullying in school by working with teachers, families, community leaders and students. It includes teacher training, classes and digital classrooms. Teachers use a handbook for in-class teaching, which is supplemented by an anti-bullying computer game for primary school children and an internet forum for high school children. Though it is not specifically focused on cyberbullying, the program has proven to be equally effective at reducing cyberbullying as traditional bullying (Salmivalli, Kärna, and Poskiparta, 2011).

# FURTHER READING


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

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

- M. A. Al-Garadi et al., (2019). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. IEEE Access, vol. 7, pp. 70701-70718, 2019
doi: 10.1109/ACCESS.2019.2918354

- Patchin, J.W. & Hinduja, S.,(2019). The Nature and Extent of Sexting Among a National Sample of Middle and High School Students in the U.S. Archives of Sexual

Behavior 48: 2333. https://doi.org/10.1007/s10508-019-1449-y

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

- Machackova, H., Cerna, A., Sevcikova, A., Dedkova, L., & Daneback, K., (2013).

Effectiveness of coping strategies for victims of cyberbullying. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7(3), article 5. http://dx.doi.org/10.5817/CP2013-3-5

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

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

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

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

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

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

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

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

## DIRECTOR OF THE PUBLICATION

**Jennyfer Chrétien,** Executive Director, Renaissance Numérique

## RAPPORTEUR

**Claire Pershan**, Project Manager, Renaissance Numérique

RENAISSANCE
numerique

## ABOUT RENAISSANCE NUMÉRIQUE

Renaissance Numérique is France's main independent think tank focusing on the challenges of digital transformation in society. Bringing together universities, associations, corporations, start-ups and schools, it aims to develop workable proposals to help public stakeholders, citizens and businesses promote an inclusive e-society

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

April 2020