International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Legal Challenges of Cyberbullying and Online Harassment: A Comparative Analysis

Shashank Mittal

Amity Law School, Noida

Abstract

Nowadays, when the internet is present in every sector of our lives like in (education, information, shopping, etc), adolescents are fascinated by the opportunities of the new technologies. Youngsters use the internet and mobile phones for easy access to knowledge, for better and wider communication, for social interactions; and all of these can be done at any time or at any place.

However, all these are the benefits of the new technologies but along with this there are some threats for the school and college going students in this virtual world most of the today's generation instead of using internet for some innovative and informative motive they move to wrong directions they try to have access to pornography, doing online bullying , stalking through electronic media etc has increased nowadays.

Young adults can also use the internet and mobile phones for doing wrongful actions which are being prohibited by law which includes sending shameful pictures or messages, threatening someone, spreading rumors about someone , sarcastic comment on physical characteristics of someone with intention to harass him/ her, or using a fake identity or taking revenge.

Such online activities are called cyberbullying which is also defined as "an aggressive act or anti social behavior that is done using electronic means by a group or an individual repeatedly against a victim who cannot easily defend himself/herself".

So therefore it can be said that, cyberbullying is a type of bullying occurring by the use of digital technology . The term cyberbullying can be called by different names such as : cyber bullying, e-bullying, cyber harassment, text bullying, SMS bullying, mobile bullying, digital bullying, internet bullying. In this paper we will use "cyberbullying" to refer to the harassment of the others through new electronic technologies, first of all by the internet and smart phones.

CHAPTER-I
INTRODUCTION

Introduction

Nowadays, when the internet is present in every sector of our lives like in (education, information, shopping, etc), adolescents are fascinated by the opportunities of the new technologies. Youngsters use the internet and mobile phones for easy access to knowledge, for better and wider communication, for social interactions; and all of these can be done at any time or at any place.

However, all these are the benefits of the new technologies but along with this there are some threats for the school and college going students in this virtual world most of the today's generation instead of using internet for some innovative and informative motive they move to wrong directions they try to have

access to pornography, doing online bullying , stalking through electronic media etc has increased nowadays.

Young adults can also use the internet and mobile phones for doing wrongful actions which are being prohibited by law which includes sending shameful pictures or messages, threatening someone, spreading rumors about someone , sarcastic comment on physical characteristics of someone with intention to harass him/ her, or using a fake identity or taking revenge.

Such online activities are called cyberbullying which is also defined as "an aggressive act or anti social behavior that is done using electronic means by a group or an individual repeatedly against a victim who cannot easily defend himself/herself".

So therefore it can be said that, cyberbullying is a type of bullying occurring by the use of digital technology . The term cyberbullying can be called by different names such as : cyber bullying, e-bullying, cyber harassment, text bullying, SMS bullying, mobile bullying, digital bullying, internet bullying. In this paper we will use "cyberbullying" to refer to the harassment of the others through new electronic technologies, first of all by the internet and smart phones.[1]

Meaning Of Bullying

The term Cyber bullying was for the first time coined by Bill Belsey, who was a Canadian educator. Cyber bullying means using both information and communication technology beyond the limit with the intention to harm a person's reputation, state of mind, or to humiliate a person. It is an act by which the person being bullied suffers an adverse effect.[2]

Cyber bullying is bullying that takes place through the medium of digital devices like cell phones, computers, and tablets, I pads laptops etc . Cyber bullying can occur through SMS, Text messages, and on chat rooms , forums, or online games where people can view, participate in, or share contents.

Cyberbullying means sending, posting, or sharing negative thoughts , harmful, false, or mean content about someone else. It can include sharing personal or private information of someone else causing embarrassment or humiliation. Some of the acts of cyber bullying also include unlawful or criminal behavior.

The most common places where cyber bullying occurs are:

- On Social Media platforms such as Facebook, Instagram, Snapchat, and Tik Tok, whatssap , v chat, skype etc.
- On Text messages and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities.[3]

Bullying is unwanted, aggressive and anti social behavior among school aged children who commits cyber bullying with their classmates which involves teasing , embarrassing , making sexually colored remarks to girl child or discloses the private information regarding someone to cause annoyance . This behavior is frequently repeated by the perpetrator.

[1] Romanian Journal Of Experimental Applied Psychology RJEAP Special Issue - PSIWORLD 2016 Proceedings www.rjeap.ro • www.psiworld.ro, Psychological Effects Of Cyberbullying In Adolescence Theoretical Analysis A*Mioara Boca-Zamfir

[2] https://acadpubl.eu/hub/2018-119-17/2/146.pdf

[3] https://www.stopbullying.gov/cyberbullying/what-is-it

One student shared that "all bullying hurts, whether in person or through technology, the ultimate output is that bullying in any form is causing emotional damage to the victim "Some of the most common cyber bullying tactics include:

- Posting rude comments or rumors about someone online that are mean, hurtful, or embarrassing in nature
- Threatening to hurt someone
- Posting a mean or hurtful picture or video.
- Pretending to be someone else online in order to solicit or post personal or false information about someone else.
- Posting mean or hateful names, comments, or content about any race, religion, ethnicity, or other personal characteristics online.
- Creating a mean or hurtful webpage about someone.

A few cyber bullying examples are provided here to help you understand what cyber bullying or anti-bullying is.

- Cyber bullying may take many different forms across a variety of internet platforms:
- Humiliating/embarrassing content posted online about the victim of online bullying,
- Hacking of account
- Posting vulgar messages
- Threatening the victim to commit an act of violence
- Stalking
- Child pornography or threats of child pornography

Doxing, an acronym for "doxing," is a type of online harassment used to exact retribution and to threaten and obliterate people's privacy by making their private information, such as addresses, social security numbers, credit card numbers, phone numbers, links to social media accounts, and other details, public.

Bullying includes actions such as making threats, spreading rumors, attacking someone verbally, and excluding someone from a group for specific purpose.[4]

Causes Of Cyber Bullying

The primary cause of cyberbullying is when a person who commits the offence is completely unknown , in which a person who is bullying can easily target anyone over the internet by hiding his/her original identity.

There are various other factors which are responsible for a person to become a cyberbully such as Personality traits are responsible for cyberbullying behavior or anti social behavior.

Another primary cause is online shyness or hampering , in which a person bullies others with the motives of causing harm, domination, or taking revenge, or just for fun

Other causes are moral disentanglement as the findings imply that, regardless of the contemporaneous victimization status, moral disengagement has an equal impact on bullying perpetration for those who are most engaged.

The next one is egotism which means individuals consider social status and authority dominant over their human relations.

The last is aggression, which refers to overcoming negativities and failures by force, triggering them to do cyber bullying for satisfaction.[5]

[4] https://www.pacer.org/bullying/info/cyberbullying/

Types Of Cyberbullying

Exclusion

Exclusion is the deliberate exclusion of someone. Exclusion is a factor in both online bullying and physical bullying scenarios where a victim is targeted. For instance, your child may be left out of message threads or chats with people they both know while other friends are invited or involved in groups or events.

Harassment

Harassment is a broader term under which includes many types of cyberbullying , but it generally refers to constant pattern of sending hurtful or threatening online messages with the intention of doing harm to someone.

Outing/Doxing

Basically the term doxing, refers to the act of openly revealing sensitive or personal information about someone without their consent with the objective of embarrassing or humiliating them. This can also extend to spreading of personal pictures or documents of public figures to sharing an individual's saved personal messages in an online private group. The key is the lack of consent from the victim.

Trickery

Trickery incorporates the element of deception and is comparable to the idea of doxing. In this type of cyberbullying, the bully would develop cordial relationships with the victim in an effort to give them a false sense of security. Once the bully obtains the target's trust, they take advantage of it by disclosing the victim's secrets and personal information to one or more third parties5. Cyberstalking.

Cyberstalking:

is the recurrent contact and harassment of someone through technology, such as social media, emails, and text messages, making them fear for their safety. Cyberstalking is a type of cyberbullying that is similar to in-person stalking in that it invades the privacy of the target and has the potential to be emotionally damaging.

Fraping

Frapping is when a bully posts offensive stuff using the name of your child on social media. When friends publish amusing things to each other's profiles, it can be innocent but also extremely dangerous. For instance, a bully posting homophobic or racial remarks through another person's profile to harm that person's reputation.

Masquerading

Masquerading occurs when a bully creates a false online identity or profile with the intent to bully someone online. This can entail choosing a new identity and set of images to deceive the victim, as well as creating a false email account and social media presence. In these situations, the bully is frequently someone the victim knows well.

Dissing

Dissing refers to the act of a bully spreading cruel information about their target through public posts or private messages to either ruin their reputation or relationships with other people. In these situations, the bully tends to have a personal relationship with the victim, either as an acquaintance or as a friend.

[5] https://link.springer.com/article/10.1007/s10639-022-11168-4

Trolling

Trolling is when a bully will seek out to intentionally upset others by posting inflammatory comments online. Trolling may not always be a form of cyberbullying, but it can be used as a tool to cyberbully when done with malicious and harmful intent. These bullies tend to be more detached from their victims, and do not have a personal relationship.

Flaming

Flaming or roasting is the act of using abusive language or using profanity to publish insults online. This phrase shouldn't be confused with trolling, which refers to the behaviour of someone who stirs up conflict offline or online. Flaming evolved as a result of how Internet forums' anonymity allows users to act more violently.[6]

Psychological Effects Of Cyber-Bullying In Adolescence

Researchers laid down in their research work that being involved in cyber bullying has psychological, emotional and behavioural consequences both on the victims and upon the perpetrators too:

- Many of the cyber victims feel angry, frustrated, sad and depressive.
- They also feel fear, confusion, guilt, shame, stress, and anxiety.
- Researchers who studied the correlation between involvement of the adolescents in cyber bullying and self-esteem found that both victims and perpetrators have lower self-esteem than the adolescents.
- It creates the feeling of depression, self harm, suicide or sometimes suicidal thoughts also comes into the mind of the victims.
- In most of the cases it creates high level of social anxiety in the minds of cyber victims.
- However, cyber bullying can have social effects on victims such as isolation from friends and colleagues.
- cyber victims faces a higher risk related to school problems for example suspension, copying out at tests, absenteeism, school aggression, lower academic achievement and not feeling safe in school and some other destructive behaviours are developed among such children who becomes the victim of cyber bullying such as alcohol abuse, substance abuse, running away from home.
- Cyberbullying can effect the physical health of a victim such as causing weight loss or gain, headaches, abdominal pain and sleeping problems.[7]

Indian Laws On Cyber Bullying

Information Technology Act 2000[8] The Information Technology Act, 2000 (Amended in 2008), is an Indian legislation passed by the Government of India for dealing with crimes related to the internet or cyberspace, and punishments for these offences are also provided under rthe same act.

This act describes the cyber offences and punishment for each offence, Cyberbullying is one such offence which causes mental agony in the mind of the victim for life time, they cannot get over it easily, sometimes the effects of such cyber crimes are so much extreme that the victim may commit suicide also.

It is hard to believe that there is no specific law to deal with cyberbullying in India, but it is true. In the Amendment made in 2013 in the act, the offence of cyberstalking was introduced as a criminal offence but cyberbullying has not been yet introduced . Nevertheless, there are certain sections under Chapter XI of the act which may provide remedy for the actions of cyberbullying to some extent:

[6] https://blog.securly.com/10/04/2018/the-10-types-of-cyberbullying/
[7] Psychologicaleffectsofcyberbullyinginadolescencetheoreticalanalysis.pdf
[8] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)

Section 66 (A):

This section deals with the punishment for the offence of sending objectionable, derogatory, abusive, hurtful messages or material online through the internet on any social media or any other web chat room or platform.

Section 66 (D):

"Punishment for cheating by personation by using computer resource" 10 If a person deceives, cheats someone through the internet on a social media or any other online platform, that person should be punished for up to 3 years of imprisonment and fine of up to 1 lakh rupees.

Section 66 (E):

This section deals with the punishment for infringement of privacy, if a person violates someone's privacy digitally, using their pictures, sharing information, he is guilty for cyberbullying in a way and that person must be charged with a fine up to 3 lakh rupees or imprisonment for up to 3 years under this section.

Section 67:

This section of the act deals with the punishment for uploading, transferring, circulating offensive, vulgar, indecorous material on the internet / cyberspace, with a fine up to 10 lakh rupees or imprisonment for up to 5 year.

Cyberbullying & Covid-19

- Youth are spending more time online for school, connecting with peers, and socially interacting with friends
- Kids are still adjusting to learning and interacting with their peers virtually
- Many young people may be feeling new and uncertain emotions due to the pandemic, such as anxiety, anger, fear, isolation, or stress
- This unprecedented period, as well as more time spent online, have the potential to cause an increase in cyber bullying behaviour.[9]

Cyberbullying Laws In Different Countries:

Canada:

Canada is the only country in the world which is having strictest laws to deal with Cyber bullying . They have a legislation called the "Education Act" which deals with cyber bullying , under which if a person is found guilty of cyberbullying, he/she may be charged a fine of $500 or 6 months of imprisonment or more.

European Countries:

To deal with cyber bullying, online harassment, Masquerading or any other Cybercrime, all European countries have the European Data Protection Legislation.

United Kingdom

For dealing with Cyber bullying cases, the United Kingdom has the Malicious Communications Act legislation under which, if found a person is involved in cyber bullying, it could lead to burly fine or imprisonment for six months or more. There are other laws like Computer Misuse Act, 1990 and various other legislations for dealing with it.

In USA, the Central Legislation for Cyberbullying crimes is the Magna carta Cyber bullying Prevent Act , though there are different legislations in different states, Hawaii: As per the Law, if a student gets

[9] https://www.pacer.org/bullying/classroom/pdf/covid-infographic-parents.pdf

involved in the act of cyber bullying, A sampling of cyber bullying laws around the world he/she may be charged with $100 fine.

Louisiana:

As per the H.B. 1259 Act, 989, if a student is found blameable of cyber bullying he may be charged with a $500- or six-months imprisonment.

Maryland:

According to the Grace's Law, the cyber bullies must be charged with a $500 fine, Wrongdoing and one year imprisonment.

North Carolina:

As per the 14-458.1, the cyber bullies are charged with misdemeanour for one year in a major and class two misdemeanour if a minor.[10]

Objective of the study

- To examine the existing legal frameworks and legislation addressing cyberbullying and online harassment across different jurisdictions, aiming to identify similarities, differences, and gaps in legal approaches.
- To analyze the effectiveness of legal measures and enforcement mechanisms in combating cyberbullying and online harassment, considering factors such as jurisdictional issues, technological advancements, and victim support systems.
- To explore the challenges and limitations associated with prosecuting cyberbullying and online harassment cases, including issues related to evidence collection, perpetrator anonymity, and cross-border jurisdictional complexities.
- To provide recommendations for strengthening legal responses to cyberbullying and online harassment, based on the comparative analysis of legal frameworks and the identification of best practices, aiming to contribute to the development of more effective policies and interventions to address these issues globally.

Scope of the Study

The scope of this study encompasses a comparative analysis of the legal challenges surrounding cyberbullying and online harassment across different jurisdictions. It will delve into the existing legal frameworks and legislation aimed at addressing these issues globally, examining variations in definitions, enforcement mechanisms, and penalties. By exploring case studies and victim perspectives, the study aims to identify challenges and limitations in prosecuting cyberbullying and online harassment cases. Additionally, it will evaluate the effectiveness of support systems and technological interventions while providing recommendations for strengthening legal responses to mitigate these challenges. Through this comparative analysis, the study seeks to contribute to a deeper understanding of the complexities involved in combating cyberbullying and online harassment and to propose strategies for fostering safer online environments.

Research Methodology

The research methodology for this comparative analysis on the legal challenges of cyberbullying and online harassment involves a multi-faceted approach. Firstly, a comprehensive review of existing literature, including academic studies, legal documents, and case law, will be conducted to establish a foundational understanding of the subject matter and identify relevant legal frameworks and case studies

[10] https://resources.uknowkids.com/blog/cyberbullying-laws-around-the-globe-where-is-legislation-strongest

for comparison. Additionally, qualitative methods such as interviews or surveys may be employed to gather insights from legal experts, policymakers, and stakeholders involved in addressing cyberbullying and online harassment. Furthermore, a comparative analysis will be conducted to examine the similarities and differences in legal approaches across different jurisdictions, focusing on aspects such as definitions, enforcement mechanisms, penalties, and victim support systems. This research methodology aims to provide a holistic understanding of the legal challenges associated with cyberbullying and online harassment and to generate insights that can inform policy-making and legal reform efforts.

Limitation of Study

The legal challenges of cyberbullying and online harassment lies in the inherent complexity and dynamic nature of the digital landscape. Given the rapid evolution of technology and online platforms, the legal frameworks and responses analyzed may quickly become outdated or insufficient to address emerging forms of cyberbullying and online harassment. Additionally, the effectiveness of legal measures may vary depending on factors such as cultural norms, societal attitudes, and the enforcement capacity of respective jurisdictions, which could limit the generalizability of findings across different contexts. Furthermore, the study's scope may be constrained by the availability and accessibility of relevant legal documents, case studies, and expert perspectives, potentially limiting the comprehensiveness of the comparative analysis.

CHAPTER-II
OVERVIEW OF CYBERBULLYING AND ONLINE HARASSMENT LAWS

Technology has changed the life of an individual. Although it helps him to live his life with ease, there are certain problems that exist side by side also. Cyberbullying is one aspect of technology. In this article, we will be discussing cyberbullying, its meaning, types, Indian laws related to it, effects and how it can be stopped.

What do you mean by cyberbullying

Cyberbullying means harassing or insulting any person through various digital platforms or communication sources such as e-mails, direct messages and other social media apps. Simply put, there is use of technology to insult or harass someone. When something abusive is shared about anyone on online platforms which humiliates, embarrasses or degrades the reputation of the person is called cyberbullying.

The National Crime Prevention Council defines cyberbullying as *"the process of using the internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person."* This also happens through gaming apps. It includes posting offensive comments, and remarks that may lead to racial, religious, ethnic and political hatred. The term "cyberbullying" was first defined by a Canadian named Bill Belsey.

What are the types of cyberbullying

The different types of cyberbullying have been discussed hereunder, for providing an idea to the readers about the same.

Flaming

Flaming signifies a type of cyberbullying that involves sending of offensive or hurtful texts, messages or emails, directly to the victim. Vulgar and abusive words are sent which are aggressive in nature. Flaming usually contains insults, words full of anger, etc. A few traits of flaming that readers should know about are:

1. It is necessary to note that bullies who engage themselves in flaming generally use capital letters, images and symbols, so that they can add emotion to their argument.
2. It is not a surprise if the flammer puts down someone's race, sexual involvement, gender, economic status, etc. This aggravates the insult that is intended to be done.
3. It is always advisable that the incident of flaming must be reported to those you trust such as your parents, teachers, friends, etc, so as to keep confidentiality intact.
4. Flaming in itself is a dangerous type of behaviour that can lead to serious consequences.
5. It is necessary to note that flamers carry on their activity so as to seek attention. The longevity and trait of the attention period does not matter as both positive and negative attention is welcomed by these flamers.

Harassment

In this type of online bullying, a person receives threatening or hateful messages. These messages usually follow a constant pattern with the intent to hurt. The three prime traits of harassment as a form of cyberbullying have been provided hereunder:

1. **Severe:** Online harassment is considered to be severe for the consequences it wears along with itself. Be it abuse or death threats, the resultant effect on the aggrieved party is hard to estimate.
2. **Pervasive:** Online harassment is considered to be pervasive because at times it appears to be extremely minor in proportion but similarly its detrimental consequences on the targeted individual can be said to be another side of the coin.
3. **Online:** The harassment we are talking about is inclusive of email, social media platforms (such as Twitter to that of Facebook, Instagram, and TikTok), blogging platforms (such as Medium, Tumblr, etc), and the comments sections as well such as those on digital media or any personal blogs.

Trolling

When inflammatory comments are posted about a person intentionally to disturb him or her mentally, the same is termed as trolling. Usually, celebrities are trolled for their actions online for they are considered to be soft targets due to their public presence.

Cyberstalking

Cyberstalking is a serious offence where the victim receives threatening messages. It also includes physical threats. Here the victim is monitored and followed online. It can be called the extension of physical stalking. It is considered a criminal offence according to Section 354D of the Indian Penal Code, 1860.

Frapping

When an individual uses your social networking accounts to post some inappropriate content under your name, the same is considered to be frapping. This is usually done to ruin your reputation and can be considered as one of the forms of online defamation.

Exclusion

In this type of cyberbullying an individual is excluded deliberately from a group. He is also bullied online through messages.

Impersonation

Impersonation is when a person makes fake profiles and accounts to destroy one's reputation in society. Sensitive information about the victim is also shared online.

Cyberbullying in India

Although the rate of cyberbullying is increasing day by day in India, there lies no direct provisions

dealing with the same. There are some sections of the Information Technology Act, 2000 and IPC which deal with the punishment related to cyberbullying, as have been discussed hereunder.

Section 66 A of the Information Technology Act, 2000

This section deals with the punishment for sending messages or emails which are harmful or abusive in nature through the internet or any other platform. These messages are sent to cause annoyance, injury, and inconvenience to the victim. It is also punishable under the provision when someone shares information that he believes to be false.

Punishment under this section is 3 years of imprisonment, if the message sent was found grossly offensive. However, this provision was struck down by the Apex Court as it was declared unconstitutional in 2015 in the Shreya Singhal case, for the purpose of violating the freedom of speech.

Section 66 C of the Information Technology Act, 2000

This provision deals with the punishment for using electronic signature, password or any other identification feature of any other person dishonestly or fraudulently. A person is punishable under this provision up to 3 years of imprisonment or a fine up to one lakh rupees for identity theft.

Sec 66 D of the Information Technology Act, 2000

An individual who cheats by personation using any social media or communication device is punished under this provision. It means a person is typically punished for fraudulently pretending to be some other person.

Sec 66 E of the Information Technology Act, 2000

This provision was added in the Information Technology (Amendment) Act, 2008. It reduces the gender bias which was made in Section 354 C of the Indian Penal Code, 1860. This provision provides protection to both men and women. This provision specifically deals with privacy with respect to one's body parts. It is punishable to capture (any video, image, film or record through any means) publish,(that is available to the public) or to transmit an image film or video recorded that has been sent in such a way that it can be viewed by person or persons without the consent of the person, violating his or her privacy. This section covers two circumstances that would amount to a violation of the privacy of that person.

Section 67 of the Information Technology Act, 2000

Under this provision, publishing or transmitting any material which is obscene in nature and if such material tends corrupt people to read, hear or see the material, it would be considered as an offence. It means such material raises lustful thoughts in the person. The person committing offence under section 67 will be punished with imprisonment which may extend up to 3 years and fine up to 5 lakh rupees and on subsequent conviction the imprisonment may extend up to 5 years and of fine 10 lakh rupees.

Section 67 A of the Information Technology Act, 2000

Section 67 A deals with penalising the publishing or transmission of any material which contains sexually explicit content or act. The publication or transmission of such material should be in electronic form. Punishment under Section 67 A on 1st conviction is imprisonment which may extend up to 5 years also with a fine up to 10 lakh however on the second conviction, imprisonment may extend to 7 years and with a fine up to 10 lakh rupees.

Exception to Section 67 and Section 67 A

1. These sections do not extent to any book, paper, painting or figure in electronic form
2. When a publication is for the public good and in the interest of science, literature, art, etc, then it does not come within the purview of these sections.
3. When a publication is related to bonafide heritage or religious purposes, the act won't be categorised

4. as those mentioned in these sections.

Sec 67 B of the Information Technology Act, 2000

This section deals with the transmission of material that depicts children involved in sexually explicit conduct or act. Any person who creates text, advertisements or images or records anything which depicts children in a vulgar or obscene manner, is punishable under Section 67 B.

Section 292 A of the Indian Penal Code, 1860

This section deals with the printing of any matter in grossly indecent manner or matter intended for blackmail; it includes printing, selling or conveying any printed or written document which is indecent or intended for blackmail. Taking part in or receiving any profit from such business which includes sale, import, export or printing etc, of such materials or advertising the same which would be injurious to morality, is punishable under this provision.

Section 354 C of the Indian Penal Code, 1860

This section deals with voyeurism. Under this provision, if any man who captures the image or watches any woman engaged in some private act in such circumstances where she presumes privacy or spreads such images to a third party, would be considered as an offence. This provision is gender specific, i.e.it only covers males. Females are not punished under this provision. On first conviction, he shall be punished with imprisonment which should not be less than 1 year and this may extend to 3 years with a fine. This imprisonment increases on a second conviction of at least 3 years which may extend to 7 years with a fine.

Section 354 D of the Indian Penal Code, 1860

Section 354 D defines stalking as :

1. When a man follows a woman and contacts her, or tries to contact her to stimulate personal interaction frequently even when she shows a clear intention of disinterest.
2. Monitors the activity of the woman online through various communication methods like email, messaging apps.

This section only covers women. Any stalking of males is not covered under Section 354 D. In the case of the ***State of West Bengal v. Animesh Boxi (2018)[11],*** *the accused hacked the victim's phone and took control of some of her private pictures. He blackmailed her by threatening to post those pictures on a pornography website. Here the court held that the* victim has suffered from virtual rape. Thus the accused will be convicted under Section 354 D of IPC.

Section 499 of the Indian Penal Code, 1860

This section deals with defamation. As discussed in this section, the scope of defamation is quite broad. Along with offline defamation in written or oral form, it also includes any speech or document in online format which are posted on online platforms by any person which tends to harm the reputation of any other person. Such a person will be considered as doing online defamation and he will be penalised under Section 500 of IPC which deals with the punishment of the same. The punishment is simple imprisonment which may extend to 2 years or a fine or both.

Section 507 of the Indian Penal Code, 1860

This section specifically addresses criminal intimidation through the use of anonymous communication. It means that when any person through a fake identity (which is not known), or through an unknown

[11] section 439(2)

telecommunication source; it may be any social media platform, threatens another person shall be punished with imprisonment of maximum of 2 years.

Section 509 of the Indian Penal Code, 1860

If a person does any act or utters any word or makes such gestures or sounds with the intention to intrude on the privacy and to offend the modesty of women, he shall be punished with simple imprisonment which may extend to three years with a fine. The intention is the most important essential of the section. If any person tries to harass a woman through electronic mode or by using any telecommunication device shall be punished with fine and rigorous imprisonment which shall not be less than two months however this rigorous imprisonment may extend to 2 years also.

Initiatives taken by the Indian government

Cybercrime prevention against women and children scheme (CCPWC Scheme)

Under this scheme, various units are established to analyse cybercrime reports and investigations related to cybercrimes. These units are also responsible for reporting cyberbullying with the aim to prevent cybercrime. Under this financial assistance has been provided to all states and UTs for implementing the schemes. The portal cybercrime.gov.in will receive complaints from the citizens on objectionable online content related to child pornography, child sexual abuse material, and sexually explicit material like rape and gang rape. CCPWC portal will facilitate victims/complainants to report cybercrime complaints online in either anonymous mode or 'report & track' mode.

Indian cyber crime coordination centre scheme

This scheme focuses especially on women and children victims and issues faced on online media. It also creates awareness among youth about cybercrime. It deals with all kinds of cybercrimes in a comprehensive manner. It has various components, namely, National Cybercrime Reporting Portal, National Cybercrime Threat Analytics Unit, Joint Cybercrime Investigative Team Group, National Cybercrime Forensic Laboratory Ecosystem, National Cybercrime Training Centre, Management Unit of Cybercrime Ecosystem, National Cyber Research and Innovation Centre.

Helpline numbers

Various helpline numbers are also set up for tackling the problem of cyberbullying. Complaints on numbers like **1800-180-5522** are promptly forwarded to the authorities.

The Nirbhaya Fund Scheme

This fund has been set up by the Indian Government for the safety and security of women and children. The Ministry of Home Affairs has also generated a single number to cope up with the emergency. This is under the Emergency response support system (ERSS).

National Database on Sexual Offenders (NDSO)

It was launched to provide assistance in monitoring & investigation of sexual crimes. NDSO portal will only be accessed by law enforcement agencies to effectively track and investigate cases of sexual offences.

Effects of cyberbullying

Cyberbullying may affect an individual's life in various ways. It may harm him emotionally, mentally.A 2019 Swedish study indicates that youths involved in cyberbullying, either as the target or the perpetrator, had a higher risk of symptoms of depression and anxiety. They also had lower levels of general well-being.

A person starts eluding from reality, from social media or other online platforms. He may feel it difficult to engage in social activities and have a social life. He may have a low opinion of himself. Cyberbullying usually increases fear and anxiety in the mind of a person. Destructive thoughts, mood swings, not showing emotions, not trusting anyone, aggressiveness and short-tempered nature are some of the symptoms of a victim. He sees no hope in the near future. There are many chances that a victim may commit suicide. There is a lot of mental agony and pain. He remains mentally disturbed and many of times, starts hiding things. Fear of losing reputation and respect changes his behaviour towards his family members are the common symptoms.

How it can be prevented

It is the responsibility of parents to check their child's online activities so that the problem of cyberbullying can be prevented from the root. Parents should be aware of apps their child is using. They should encourage their child to engage in offline activities. They must notice changes in a child's behaviour such as less involvement with others , deactivation of social media accounts, hiding things, avoiding discussions, showing symptoms of depression etc. They must note these changes and investigate whether these occur during the child' s involvement in online activities.

If by any chance these symptoms are there in a child' s behaviour, Parents must take quick and effective action.They should start a conversation with the victim and assure him that there would be no harm to him. Ask him how it happened, who are involved etc

A proper record should be maintained of the bullying. Enough proof should be taken either through screenshots or through any other methods. Bullies should be reported immediately. Also, social media platforms can be requested to remove the offensive post. These platforms have guidelines regarding cyberbullying. Parents can send a complaint to the complaint-mwcd@gov.in and can register a complaint with the nearest police station in case the victim receives threats.Victims should be supported morally.

Bullying

Bullying may be characterised as an intentional act by a perpetrator which, though may not amount to a criminal offence, causes pain or anguish or suffering to the victim, either physically or emotionally. The victim is usually at the mercy of the perpetrator and the bully uses tactics such as name-calling or intimidation or social ostracization to achieve his or her goal. Bullying may take place in both public and private spaces. It traumatises the victim and may result in permanent emotional damage.

Traditional Approach to Bullying

The traditional approach to bullying in educational institutions and workplaces has been to brush it aside, with excuses such as 'boys will be boys' or 'tough men don't complain', though it is possible that bullying which involves intimidation or the threat of violence could trigger the offence of assault[12] or battery.[13]

Examples of bullying which do not tantamount to a traditional criminal offence are, classmates calling a school boy 'fat' or 'stupid' or an employee being shouted at by a senior or superior officer. When

[12] S. 351, Indian Penal Code, 1860 defines assault as: Whoever makes any gesture, or any preparation intending or knowing it to be likely that such gesture or preparation will cause any person present to apprehend that he who makes that gesture or preparation is about to use criminal force to that person, is said to commit an assault.

[13] S. 350, Indian Penal Code, 1860 defines battery or criminal force as : Whoever intentionally uses force to any person, without that person's consent, in order to the committing of any offence, or intending by the use of such force to cause, or knowing it to be likely that by the use of such force he will cause injury, fear or annoyance to the person to whom the force is used, is said to use criminal force to that other.

classmates threaten or rough up another in the school yard or when a subordinate is threatened with the imminent application of force or is slapped, an offence is committed, though such actions usually go unpunished.

As more and more women enter workplaces, women too become targets for bullying in such workplaces. At times, bullying takes the form of sexual harassment.

Cyber Bullying

Cyber bullying refers to bullying or harassment of any kind inflicted through electronic or communication devices such as computers, mobile phones, laptops, and usually involve text messages, phone calls, e-mails, instant messengers, social media platforms, or chat rooms. It ranges from the posting of hurtful words, derogatory comments, fake information on public forums or blogs to threats to rape or kill.

The most frequently used definition of cyber bullying is 'an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and overtime against a victim who cannot easily defend him or herself.'[14]

The Anonymous Bully

Bullying traditionally involved a stronger person asserting his or her superiority over a weaker person to his or her advantage. With the advent of the internet, it has become possible for a person with neither superior physical strength nor financial clout to bully another. In many cases, the bully uses a fake identity and the anonymity offered by the internet to stay away from the clutches of the victim and the law.

Laws against Cyber Bullying

The Indian Penal Code, 1860 ("**IPC**"), neither defines bullying nor punishes it as an offence. However, various provisions of the IPC and the Information Technology Act, 2000 ("**IT Act**") can be used to fight cyber bullies.

Cyber Stalking of Women

The National Commission for Women ("**NCW**") in its legal module on 'Gender Sensitization and Legal Awareness Programme'[15] defines cyber stalking as following:

'Stalkers are strengthened by the anonymity the internet offers. He may be on the other side of the earth, or a next-door neighbour or a near relative!' It involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chatrooms frequented by the victim, constantly bombarding the victim with emails, etc. In general, the stalker intends to cause emotional distress and has no legitimate purpose to his communications'

Cyber Stalking is an extension of the physical form of stalking, committed over the internet, through e-mail or other electronic communication devices and can take different forms including slander, defamation and threats.

Cyber stalking includes, inter alia, the following:

- Sending threatening or obscene messages, posts or emails;

[14] Smith, P. K., del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross, & J. Walker (Eds.), Routledge monographs in mental health. Principles of cyberbullying research: Definitions, measures, and methodology (p. 26–40). Routledge/Taylor & Francis Group.

[15] Ministry of Women and Child development. National Commission for Women. 2019. Legal module on 'Gender Sensitization and Legal Awareness Programme'. http://ncw.nic.in/notice/legal-module-gender-sensitization-and-legal-awareness-programme-collaboration-kendriya.

- Stealing a person's identity online and circulating false information with the intent to humiliate or harass;
- Tracing the location of a person through illegal means;
- Uploading obscene pictures;
- Posting derogatory remarks online with the intent to harass.

The Press release on 'Digital Exploitation of Children', by the Ministry of Women and Child Development states that the sections 354A and 354D of the IPC provides punishment for cyber bullying and cyber stalking against women.

Cyber-stalking of women was recognised as an offence, subsequent to the insertion of section 354D in the IPC through the Criminal Law (Amendment) Act, 2013.

Section 354D of IPC defines stalking as following:

'Any man who

1) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

2) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking: (emphasis supplied)

Provided that such conduct shall not amount to stalking if the man who pursued it proves that

1. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state
2. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law
3. *in particular circumstances such conduct was reasonable and justified.'*

The language of Section 354D of IPC makes it clear that the section penalises both the offence of offline and online stalking, without discriminating on the basis of presence or absence of the 'cyber' component. However, sub-section (2) fails to clarify the manner in which the victim can be said to be 'monitored' or 'watched' or what constitutes such acts.

In the case of ***State of West Bengal v. Animesh Boxi***[16] , the accused took possession of some private and obscene photographs of the victim by hacking into her phone, blackmailed her by threatening to upload the stolen pictures and videos on the internet and subsequently uploaded her private pictures and intimate videos onto an obscene website.

The District Court of West Bengal convicted the accused under sections 354A, 354C, 354D, 509 of IPC and sections 66C and 66E of the IT Act. The court held that the offence u/s 354D of the IPC is proved as the victim was not only stalked online but also suffered from 'virtual rape' every time a user of the openly accessible global website viewed the video. The court commented that deterrence was one of the prime considerations for convicting the accused and an inadequate sentence would do more harm than justice, as it would undermine public confidence in the seriousness of the issue.

Cyber Stalking of Men

At present, if a man is a victim of cyber stalking, Section 354D will not apply. However, it is possible that other provisions of the IPC or the IT Act may apply. For example, let's assume that Mr. ABC, the manager of a reputed venture capital fund, is being stalked online by XYZ, who may be a male or a female. XYZ had initially sent a polite email to ABC's work email address, seeking an appointment, so

[16] State of West Bengal v. Animesh Boxi , GR No. 1587 of 2017.

that he could make a pitch for an investment by ABC's venture capital fund into his struggling start-up. A PDF document attached to the email gave relevant details of XYZ's start-up. ABC replied to politely decline the meeting and the investment opportunity, which he felt wasn't worth pursuing. Subsequently, XYZ's emails started to get angrier and nastier. XYZ has now started posting some derogatory remarks regarding ABC on various online venture capital forums. He has also sent a few emails to ABC in which he explicitly threatened to harm ABC.

The posting of derogatory remarks regarding ABC on various online venture capital forums would tantamount to defamation, as defined under Section 499 of the IPC. Section 500 of the IPC provides that whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

XYZ is also likely to be found guilty of criminal intimidation under Section 503 of the IPC on account of having made threats to ABC through emails. Section 506 of the IPC provides that whoever commits, the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both. If the threat was to, inter alia, cause death or grievous hurt, it shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both. If the emails sent by XYZ to ABC were anonymous, section 507 of the IPC provides that XYZ shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment prescribed under section 506 of the IPC.

Online Sexual Harassment

In India, it used to be common for sexual harassment to be called ‘eve-teasing', which downplayed the severity of the offence. However, the concerted efforts of Indian courts, the legislature, the Law Commission of India, non-governmental organisations and women's activists have led to a radical change in the treatment of sexual harassment of women. The enactment of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act 2013 ("**POSH Act**") has conveyed a stern message that any form of sexual harassment of women in the workplace shall not be tolerated. Further, there have been a number of milestone amendments to the Criminal Procedure Code 1973 (“**CrPC**”), IPC and the Indian Evidence Act which facilitate the prosecution of sexual harassment.

With effect from February 3, 2013, Section 354A was inserted in the IPC to penalise the offence of sexual harassment. Section 354A states that the act of making physical contact and advances involving unwelcome and explicit sexual overtures, or demanding/requesting for sexual favours, or showing pornography, or making sexually coloured remarks amounts to the offence of sexual harassment, shall be punishable with 3 (three) years of rigorous imprisonment and/or a fine.

Online sexual harassment includes, *inter alia*, using an electronic medium to make calls repeatedly, send vulgar SMSes, emails or make vulgar conversation or pressure a woman to engage in friendship or to establish sexual relations. However, Section 354A of the IPC requires physical contact or physical advances and hence harassment through an electronic medium will fall outside of the purview of Section 354A of the IPC.

Overlap between Cyber Stalking and Online Sexual Harassment

Cyber stalking could amount to online sexual harassment if it has sexual overtones. However, a stalker is usually an anonymous person unlike a sexual harasser who is unlikely to hide his or her identity.

Fake Facebook Profiles

Creation of a Facebook profile in someone else's name is relatively easy and such a profile makes it possible to show the victim in a false light. There have been instances where vulgar or obscene photos of

a victim have been linked to such fake Facebook profile, causing the victim extreme mental anguish.
When the creation of a fake Facebook profile is accompanied by the uploading of vulgar or obscene photos of the victim on to such profile, Section 354A (*Sexual harassment and punishment for sexual harassment*), Section 354D (*Stalking*), Section 499 read with Section 500 (*Defamation and Punishment for defamation*), Section 507 (*Criminal intimidation by an anonymous communication*) and Section 509 (*Word, gesture or act intended to insult the modesty of a woman*) of IPC may apply.
In the case of ***Sazzadur Rahman v. The State of Assam and Ors***.[17], the accused created a fake Facebook profile of a 15-year-old victim. In the fake profile, the accused mentioned the victim's name, uploaded obscene pictures, and posted some derogatory remarks against her, which caused her to be mentally unstable and hampered her academic growth. The trial court rejected the application made by the accused under Section 311 of CrPC. Thereafter, a petition under section 482 read with sections 401/397 of CrPC was filed before the Gauhati High court for quashing the order of the trial court. The Gauhati High Court, while dismissing the application, held that discretion of the trial Court, which, ex facie, has been exercised judiciously on the basis of relevant materials, cannot be interfered with either in revisional jurisdiction or under Section 482 CrPC.
In the case of ***Shubham Bansal v. The State (Govt of NCT Delhi)***[18], the accused created a false Facebook account in the name of Nidhi Taneja and included the telephone number of the victim, which caused her annoyance, insult, and harassment and, therefore an FIR was registered against the accused. The victim further moved another application under Section 173 (8) of CrPC requesting further investigation by the investigating officer on account of which the matter was remanded to the Metropolitan Magistrate for consideration. Thereafter, an application was made by the accused for dropping the proceedings against him under Section 66A of the IT Act and Section 509 of IPC.
The Delhi High court while refusing to entertain the application of the accused, ordered that the investigating officer refrain from submitting his final report till the Magistrate issued directions on the pending application filed by the victim. The honourable court noted that the alternative course available to the investigating officer was to file a report based on the investigation carried out until then, reserving the right to file a supplementary challan/report in response to the pending application made by the victim under Section 173 (8) of CrPC seeking further investigation.
In the case of ***Jitender Singh Grewal v. The State of West Bengal***[19], the accused created a fake Facebook account of the victim and uploaded her obscene pictures to such fake Facebook account. After the authorities charge sheeted the accused under Sections 354A/354D/500/509/507 of IPC and Section 67A of the IT Act, he filed a bail application. The trial court rejected the bail application of the accused and the Calcutta High court upheld the trial court's decision.
In the case of ***Prakhar Sharma v. The State of Madhya Pradesh***[20], the accused created a fake Facebook account of the victim, posted some vulgar messages along with the photos of the victim downloaded from her original Facebook account. The accused was charged under Sections 66 (c), 67 and 67(a) of the IT Act. When the accused applied for bail, it was denied by the Madhya Pradesh High Court.
In the case of ***Hareesh v. State of Kerala***[21], the applicant created a fake Facebook profile, posted

[17] Sazzadur Rahman v. The State of Assam and Ors., Criminal Petition No. 654 of 2019.
[18] Shubham Bansal v. The State (Govt of Nct Delhi), Criminal Miscellaneous Petition No. 2024 of 2018.
[19] Jitender Singh Grewal v. The State of West Bengal, Criminal Miscellaneous Petition No. 7252 of 2018.
[20] Prakhar Sharma v. The State of Madhya Pradesh, MCRC No. 377 of 2018.
[21] Hareesh v. State of Kerala, Bail Application No. 4858 of 2018.

morphed obscene photographs of the victim online, posted her mobile number under the said obscene post in order to enable strangers to contact her. Thereafter, an anticipatory bail application was made by the applicant apprehending arrest in respect of offences punishable under Section 354(D) of IPC and Sections 67 and 67E of the IT Act. The Kerala High court denied the application for anticipatory bail on the ground that materials on record affirmed the involvement of the applicant in the offences and it would not be proper for the court to interfere with the investigation.

Bullying Inter-se School Mates

H, a twelve-year-old school boy was increasingly withdrawn and introverted. He looked worried most of the time but refused to divulge his troubles to his parents who were aware that he spent an extra-ordinary amount of after-school time on his I-Pad. One night, after H went to bed, his parents accessed his I-Pad and found that he was on various chat groups and was being bullied online by his classmates. The bullying involved name calling and derogatory remarks regarding his clothes and his grades.

In such scenario, the remedies available to H's parents are as following:

- Take prompt steps to show support to H;
- File a complaint reporting the online bullying to the school authorities. The complaint shall be looked into by the Anti Bullying Committee required to be formed in every school in accordance with the 'CBSE Guidelines for prevention of Bullying and Ragging in Schools';
- Report the online bullying to the nearest police station, who shall refer the matter to the cyber-crime cell for investigation. Thereafter, the cyber-crime cell shall report the matter to the Juvenile Justice Board, which will conduct an inquiry and deal with the incident as per the provisions of the Juvenile Justice (Care and Protection of Children) Act, 2000.

CHAPTER-III
LEGAL CHALLENGES IN ADDRESSING CYBERBULLYING

"The Internet is becoming the town square for the global village of tomorrow"-Bill Gates

As the use of social media and the internet has increased, cyberbullying has become a significant problem affecting people of all ages. Cyberbullying occurs over electronic platforms like social media, messaging apps, gaming platforms, and cell phones. It is a sophisticated and covert form of verbal and textual bullying that entails a pattern of behaviour meant to frighten, enrage, or shame the target. Online bullying is more deadly than traditional bullying since it is anonymous, and it is also more difficult to stop because the victim isn't aware that they are being harmed.

One of the most concerning effects of cyberbullying on psychological health. Cyberbullying victims may experience emotions of isolation and loneliness, as well as low self-esteem, anxiety, depression, a decline in academic performance, and other psychiatric illnesses. Cyberbullying can affect anyone, regardless of their age, gender, or country of origin.

Cyberspace has developed into a genuine world devoid of laws and civilisation because it is challenging in a systematised and organised society, even though the rule of law is intended to prevail and order and authority exist to protect citizens.

- Harassment: This is any inappropriate physical or verbal behavior that aims to make another person feel distressed, afraid, or worried. In the context of cyberbullying, harassment can take many different forms, such as sending messages or frequently releasing harmful content, for which offenders may be subject to fines or jail time in some circumstances.

- Impersonation: Establishing false identities for profiles or accounts in an effort to undermine and defame the victim.
- Exclusion: Willfully excluding someone from online conversations or groups, or spreading lies about the victim to keep them away from their peer group.
- Cyberstalking is the practice of watching someone else's online activities or personal life while using that knowledge to harass, intimidate, or threaten the victim.
- Sexting: Obtaining pornographic images or videos from a victim under duress and disseminating them without the victim's consent.

Legal repercussions:

Cyberbullying can have a range of legal repercussions depending on how serious the behaviour is. Prosecutors frequently cite existing laws when dealing with cyberbullying incidents, and criminal harassment statutes are used as a foundation for rendering decisions in significant situations such as suicides or other terrible events. Here are a few instances of legal repercussions:

- Criminal charges: If cyberbullying involves harassment, hate speech, or threats, there may be legal repercussions. Cyberbullying is forbidden in several countries, including the US. In some circumstances, cyberbullying may be considered a kind of cyberstalking, which is against the law.
- Civil culpability: Cyberbullying may also result in civil liability. Cyberbullying victims have the right to file a lawsuit against the offender for damages including emotional distress, reputational harm, and other associated losses. In some circumstances, parents of minors who engage in cyberbullying may be held responsible for their children's behavior.
- School repercussions: Cyberbullying may result in school-related problems. Many schools have anti-cyberbullying guidelines in place, and students who violate them may be subject to disciplinary measures including suspension or expulsion.
- Workplace repercussions: Employees who engage in cyberbullying may face disciplinary action, which may include termination, as well as other workplace consequences. In some cases, employers may be held accountable for workplace cyberbullying.[22]
- Although there isn't a specific law in India that prohibits cyberbullying, the following rules do exist:

1. According to Section 507 of the Indian Penal Code, if someone is subjected to criminal intimidation through an anonymous message, the offender might spend up to two years in prison.[23]
2. According to Section 509 of the Indian Penal Code, violators who attempt to violate a woman's modesty through words or deeds—which can also be done through electronic means—by invading the woman's privacy are subject to a year in jail, a fine, or both. [24]
3. Among other things, the Information Technology Act of 2000's Section 66A regulates the dissemination of offensive materials through communication services. This Section provided a means for actual victims of online abuse to get instant relief from potentially humiliating or hurtful content. Police officials are now powerless in the face of the growing threat of cyberbullying.
4. A person who intentionally violates someone's privacy might receive up to three years in prison or a fine of up to three lakhs under Section 66E of the IT Act.[25]

[22] Stopbullying.Gov, https://www.stopbullying.gov/ (last visited April 18, 2023)
[23] Indian Kanoon, https://indiankanoon.org/doc/1255223/ (last visited April 22, 2023)
[24] Myadvo.In, https://www.myadvo.in/bare-acts/indian-penal-code/ipc-section-509/ (last visited April 22, 2023)

Additionally, in colleges and institutions that have received UGC approval, anti-ragging committees have been constituted. Furthermore, according to the UGC, institutions and universities must adhere to the anti-ragging policy in order to maintain their accreditation.

Case law:

In the historic ruling of **Vishaka v. State of Rajasthan (1997)**, the Supreme Court acknowledged cyberbullying as a problem for the first time. The Supreme Court established rules and procedures in this case to safeguard women from sexual harassment when dealing with bullying. In the 2015 case of **Shreya Singhal v. Union of India**, Section 66A of the Information Technology Act, 2000, which protected cyberbullying in India, was overturned.

In **Sazzadur Rahman v. The State of Assam and Others**, the defendant made a false Facebook page for the victim, who was 15 years old. The accused used the victim's name in the fake profile, posted lewd photos of her, and made disparaging comments about her, which led to the victim's mental instability and prevented her from advancing academically.

The accused's request pursuant to Section 311 of the CrPC was denied by the trial judge. Following that, a petition under CrPC sections 482 read with 401/397 was submitted to the Gauhati High Court seeking to have the trial court's decision set aside. In rejecting the case, the Guwahati High Court ruled that neither the revisional jurisdiction nor Section 482 CrPC permitted interference with the trial Court's discretion, which appeared to have been used wisely in light of pertinent information.

The victim in **Shubham Bansal v. The State (Govt of NCT Delhi)** experienced discomfort, insult, and harassment as a result of the accused's creation of a fraudulent Facebook account using Nidhi Taneja's name and the victim's phone number. A FIR was then filed against the accused. The matter was remanded to the Metropolitan Magistrate for review after the victim submitted a new application under Section 173 (8) of the CrPC asking that the investigating officer conduct more investigation.

The accused then asked for the abandonment of the case against him in accordance with Sections 66A of the IT Act and 509 of the IPC. The Delhi High Court refused to consider the accused's argument, but it did instruct the investigating officer to hold off on submitting his final report until the Magistrate made a decision on the victim's pending application.

The honourable court stated that the investigating officer was free to submit a report based on the inquiry's findings up to that point, reserving the right to submit a follow-up challan or report in response to the victim's ongoing request for additional investigation under Section 173 (8) of the CrPC.[2627]

Strategies for prevention and intervention:

Parents, schools, and law enforcement must all work together to prevent and address cyberbullying. Some strategies for stopping and addressing cyberbullying include:

- Education: Raising awareness of the dangers of cyberbullying among kids, parents, and educators can help avoid it. In order to raise awareness of cybercrime among students and teachers, schools should conduct anti-bullying initiatives and teach children about internet safety, privacy, and responsible online behavior.
- Internet monitoring: In order to spot instances of cyberbullying or cybervictimization, parents and educators should keep an eye on their kids' online conduct. It's important to encourage kids to use the

[25] The Information Technology Act, 2000 ⁄ India Code, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited April 22, 2023)
[26] Vinod Joseph and Mitali Jain, India: Anti-Cyber Bullying Laws In India - An Analysis (2020)
[27] Shikha Bhatnagar, Cyber Bullying: A brief Analysis, LEGAL SERVICE INDIA

reporting features that are available on many social media sites, which allow users to report abusive behavior.

- Communication: Encouraging open communication between kids, parents, and teachers can help stop cyberbullying before it becomes a major issue. Students should be encouraged to report any instances of bullying or abuse by their parents, teachers, and peers.
- Legal Intervention: In some circumstances, cyberbullying may constitute a criminal offense. Cyberbullying incidents can be investigated by law enforcement, and offenders can be brought to justice.
- Create Safe areas: Schools and other groups should create safe areas where students may talk about issues like cyberbullying. By doing so, the humiliation associated with bullying may be lessened.
- Implement penalties: People who engage in cyberbullying should suffer penalties. In extreme cases, this could result in expulsion from school, a ban on using the internet, or legal action.

Cyberbullying is a severe problem that can have long-term effects on individuals and society. To protect yourself and others from the detrimental impacts of cyberbullying, it is critical to increase awareness about it and educate students, parents, and educators about its hazards. Cyberbullying prevention and intervention necessitate a collaborative effort from parents, schools, and law enforcement. We can make the internet a safer place for everyone if we all work together.[28][29]

Understanding cyberbullying:

Cyberbullying is the use of electronic communications such as social media platforms, email, instant messaging and text messages to harass, threaten or harm an individual. These are deliberate repetitive acts intended to cause emotional distress, embarrassment, and humiliation to the victim. Cyberbullying can take many forms, including spreading rumors, posting offensive or abusive content, identity theft, and extortion and intimidation.[30]

Effects of cyberbullying:

Cyberbullying can have a serious impact on the mental, emotional, and psychological health of victims. It can lead to depression, anxiety, social isolation, low self-esteem, and even suicide in extreme cases. The anonymity provided by the Internet encourages and facilitates perpetrators to commit such acts, often without immediate consequences.

Indian law against cyberbullying:

In India, cyberbullying is covered within the Information Technology Act 2000 and its subsequent amendments. Relevant sections dealing with cyberbullying include:

Section 66A: This section of the Information Technology Act, which was overturned by the Supreme Court of India in 2015, was formerly used to send offensive messages or It was a crime to cause such malice. Although not applicable today, it is important to mention its historical significance.

Section 67: This section is about posting or transmitting obscene content in electronic form. This law makes it a crime to post, transmit, or cause the posting or transmission of obscene or sexually explicit content. This section can address cyberbullying that involves the distribution of explicit or obscene content.

[28] What is Cyber Bullying or Anti-Bullying Laws in India, MYADVO.IN
[29] Ferrara, P., Ianniello, F., Villani, A. et al. Cyberbullying a modern form of bullying: let's talk about this health and social problem. Ital J Pediatr 44, 14 (2018).
[30] Cyberbullying Laws in India – The Law Express

Section 67A: This section focuses specifically on cyberbullying that involves sexually explicit depictions of children. It is a crime to publish, transmit, or cause the publication or transmission of child pornography.

Section 67B: This section is intended for you to post, send, or cause to be posted or sent, sexually explicit material involving a person with whom you have a consensual intimate relationship without that person's consent. It criminalizes the sharing of intimate images and videos without the person's permission and is often referred to as "revenge porn."

Section 66E –

Section of the IT Act provides penalties for breach of privacy. The article states that anyone who intenti onally violates privacy of any kind by sending, taking, posting, or otherwise sending, taking, or posting private photographs of another person shall be punished with imprisonment of up to three years or a fine of up to three lakhs.

IPC Section 507 –

This section states that if someone is criminally threatened by anonymous communication, the person m aking the threat will be punished with some form of imprisonment for up to two years. bullying and cybe rcrime. In this section, bullying is addressed using the term "anonymous."

Classification of cyberbullying as a cybercrime:

Under Indian law, cyberbullying is classified as a cybercrime under the various articles above including Section 66A (before repeal), Section 67, Section 67A, Section 67B and Section 509. These provisions enable the prosecution of individuals involved in cyberbullying. -Participate in activities and provide relief to victims.[31]

Furthermore, it is worth noting that the Indian government is in the process of enacting comprehensive legislation specifically on cyberbullying and related crimes. The bill aims to create a stronger legal framework to combat cyberbullying, including reporting mechanisms, faster investigations and provision for tougher penalties.

Types of cybercrime

Different types of cybercrime are punished differently in India.

Identity

theft When an individual's identity is stolen to misuse their financial resources or to obtain loans or cred it cards on their behalf, such crime is known as identity theft.

Cyber Terrorism – A cyber terrorism offense occurs when an individual, organization, group, or nation is threatened with extortion or harm of any kind. Generally, this involves a well-planned attack strategy against both government and corporate computer systems.

Cyberbullying – When a teenager or young person harasses, defames, or threatens someone through the Internet, phone, chat room, instant messaging, or other social networks, that person commits the crime of cyberbullying. There is a possibility that When adults commit similar crimes, it is called cyberstalking.

Hacking – The most common cybercrime is hacking. In this crime, an individual gains access to another person's computer and passwords for ill-gotten gains.

Defamation – Everyone has a right to speak, including on Internet platforms, but if what you say crosses the line and harms the reputation of an individual or organization, you can be sued for defamation.

[31] What are the Cyber Laws in India? (myadvo.in)

Copyright – With the vast increase in Internet users and the explosion of data/information across all platforms, copyright in a work helps limit the use of the work. Any use of copyright without your consent is punishable by law.

Trade Secrets – Internet organizations invest significant time and money in developing software, applications and tools and rely on cyber laws to protect their data and trade secrets from theft. This is a criminal offense.

Free Speech – When it comes to the internet, there is a fine line between free speech and cybercrime. Because freedom of expression allows individuals to express their opinions, cyber laws prohibit obscene and indecent behavior online.

Harassment and Stalking – Harassment and stalking are prohibited, even on internet platforms. Cyberlaw protects victims and prosecutes perpetrators from this crime.

CHAPTER-IV
COMPARATIVE ANALYSIS OF LEGAL APPROACHES

As a worldwide epidemic in the digital age, cyberbullying is a pertinent but understudied concern—especially from the perspective of language. Elucidating the linguistic features of cyberbullying is critical both to preventing it and to cultivating ethical and responsible digital citizens. In this study, a mixed-method approach integrating lexical feature analysis, sentiment polarity analysis, and semantic network analysis was adopted to develop a deeper understanding of cyberbullying language. Five cyberbullying cases on Chinese social media were analyzed to uncover explicit and implicit linguistic features. Results indicated that cyberbullying comments had significantly different linguistic profiles than non-bullying comments and that explicit and implicit bullying were distinct. The content of cases further suggested that cyberbullying language varied in the use of words, types of cyberbullying, and sentiment polarity. These findings offer useful insight for designing automatic cyberbullying detection tools for Chinese social networking platforms. Implications also offer guidance for regulating cyberbullying and fostering ethical and responsible digital citizens.

Introduction

The development of information and communications technology (ICT), and accompanying popularity of the Internet, mobile phones, and social media platforms, has increasingly led people to socialize online vs. in person. The COVID-19 pandemic has amplified this phenomenon. Figures suggest that more than 4.88 billion people use the Internet worldwide (nearly 62% of the global population), of whom 4.55 billion (57.6%) use social media frequently (DataReportal, 2021). People in China rely heavily on social media sites, such as Weibo (microblogs), WeChat, QQ, Toutiao (Today's Headlines), and TikTok. A report from China Internet Network Information Center indicated that over 1 billion people in the country use the Internet, accounting for more than 1 in 5 of the world's Internet user base. Current trends indicate that social media users in China will surpass the equivalent of 60% of the global population in the first half of 2022 (DataReportal, 2021).

However, people's excessive screen time, insufficient digital knowledge, and poor awareness of rights and responsibilities in cyberspace have spurred cyberbullying on nearly all social media platforms. Cyberbullying refers to aggressive behavior, which may include jokes, threats, and disinformation, that repeatedly harms people (Smith et al., 2008; Patchin and Hinduja, 2010). Social media enables these actions within a convenient environment that attracts a wide audience (Huang and Chou, 2010). Cyberbullying has thus come to pose a new threat to social media users, especially teenagers aged 6–18.

Repeated harm from cyberbullying marked by power imbalances can lead victims to display low self-esteem, anxiety, depression, and even suicidal ideation (Olweus, 2012). A growing number of reports (John et al., 2018; BJNEWS, 2021; Limbana et al., 2021) have indicated that cyberbullying brings grave physical and psychological harm to victims. As a serious global problem, cyberbullying has come to the attention of researchers, administrators, teachers, and parents.

To address this cyber threat, many studies—from theoretical analysis to law promulgation—have focused on the topic and ways to detect it. Mining textual information is a common approach and has shown utility in identifying and predicting human behavior (Davahli et al., 2020). Text features extracted from social media posts were found to be significantly correlated with individuals' characteristics (Farnadi et al., 2016). Numerous studies have attempted to link textual information with human behavior, including in emotional, social, and cognitive respects (Liu, 2012; Gutierrez et al., 2021). For example, Tausczik and Pennebaker (2010) argued that determining the physiological meaning of textual information can provide insight into people's thought processes, emotional states, intentions, and motivations. Semenov et al. (2010) analyzed users' social media posts to try to identify potential school shooters. Negative words in users' comments on social media may also be related to socially aggressive behavior (Gutierrez et al., 2021). The Sapir–Whorf hypothesis suggests that language use influences human behavior, such that a shift in language use can unconsciously influence one's thoughts and actions (Kihlstrom and Park, 2018).

Many factors influence cyberbullying. Individual-level factors have direct impacts, especially in terms of literacy related to digital citizenship (Zhong et al., 2021). Digital citizenship refers to using technology in a safe, responsible, and ethical manner; the concept is closely related to socializing online. A person's level of digital citizenship partly determines their awareness, preferences (e.g., word choice), and behavior. Ideally, if all Internet users are qualified digital citizens, then the incidence of cyberbullying should decline substantially. In other words, cyberbullying can be curbed if people are educated to behave at their best; such habits include pondering how technology might affect others (Ribble, 2015). For instance, one should show respect to others online, be cautious when sharing information or opinions, and pay attention to the wording of posts. Given that many people rely heavily on social networking, which is mainly text-based, digital citizenship is mediated through language. Persistent posting behavior (and the accompanying text, as a form of digital footprints) can inform norms and guidance to improve digital citizenship based on fine-grained analysis of social language. This information can help to mitigate unethical behavior, such as cyberbullying.

To this end, we examine people's use of social language online *via* a linguistic analysis of cyberbullying. Most relevant research has addressed explicit cyberbullying in English contexts (Ying et al., 2012; Ptaszynski et al., 2016; Balakrishnan et al., 2019; Mladenović et al., 2021). Little is known about cyberbullying conducted in Chinese (Li, 2019, 2020; Xu, 2021) or with implicit language (e.g., with positive wording but negative connotations). Ambiguity also pervades Chinese contexts due to polysemy, incompleteness, and abbreviations in sentences. The language is therefore highly likely to be misunderstood or used with ulterior motives, leading to uncertainty or conflict that can gradually evolve into cyberbullying. Therefore, we extract the linguistic features of cyberbullying in a Chinese context from explicit and implicit perspectives on social media to provide guidance for detecting and governing cyberbullying as well as shaping ethical and responsible digital citizens. Specifically, researchers can refer to the study results to formulate automatic cyberbullying detection; administrators can better understand how people behave on social media and develop pertinent guidelines. The findings are also

expected to raise the awareness of users, most of whom are digital natives, about ethical standards and codes of conduct on social networks. The following research questions (RQs) guide this work:
RQ1: What are the linguistic features of cyberbullying on social media in the Chinese context?
RQ2: Do cyberbullying incidents occurring in different domains possess distinct linguistic features?
RQ3: What implications do these features have for (a) the detection and governance of cyberbullying and (b) the shaping of ethical and responsible digital citizens?

Related Work

Cyberbullying

Cyberbullying is an emerging form of bullying carried out *via* the internet and digital technologies (Diamanduros et al., 2008); it represents an increasingly serious online moral failure in the internet age. Scholars have often defined cyberbullying in relation to traditional bullying (Smith et al., 2008; Patchin and Hinduja, 2010). Olweus (1995) stated that cyberbullying involves repetition, intentionality, and power imbalance. Yet these attributes are subject to change given the nature of the digital world. For example, repeated aggression may not apply to cyberbullying; rather, retweets of and "likes" on an image or video may perpetuate a victim's bullying experience (Alsawalqa, 2021) and increase exposure through tags and hashtags (Chan et al., 2021). Accordingly cyberbullying can be defined as aggressive behavior (e.g., jokes, threats, and disinformation) intended to harm other people and communities on the internet.

Cyberbullying can take numerous forms, including flaming, harassment, denigration, impersonation, outing and trickery, exclusion, and cyberstalking (Willard, 2007). The most common types are insults, ridicule, provocation, and ostracism. Literal attacks on others are especially frequent on social media. Typical linguistic features of cyberbullying consist of name-calling, denigration, and mockery. Such language can lead to adverse social, physical, and psychological effects (Nixon, 2014; John et al., 2018; Martínez-Monteagudo et al., 2020). Even so, cyberbullies rarely realize that their harsh or aggressive behavior could be considered bullying, instead perceiving it as humor (Alsawalqa, 2021).

Many methods have been proposed to detect cyberbullying. Machine learning and natural language processing (NLP) techniques are typically used for automatic detection by matching textual data with identified features. Researchers initially applied the bag-of-words approach, part-of-speech tagging, n-gram features, or a combination thereof for feature detection (Dinakar et al., 2011). Most recent studies have focused on content-based features, such as lexical, syntactic, and sentiment information; findings have demonstrated the importance of these words in the automatic detection of cyberbullying (Ptaszynski et al., 2016; Zhao et al., 2016; Zhao and Mao, 2017; Perera and Fernando, 2021).

Even with these advances, cyberbullying detection is inherently difficult and extends beyond simply discerning the negative sentiments or abusive content in a message (Ptaszynski et al., 2016). Online forms of communication are prone to misinterpretation (Tan, 2019), and not all bullying consists of insults (Li, 2020). Additionally, words can be masked (e.g., through metaphors, homophones, and abbreviations) to obscure negative expressions or profanity (Chen et al., 2013; Caselli et al., 2020). Tan et al. (2019) highlighted that spelling alterations are prevalent in cyberbullying, as people tend to simplify words to avoid being caught by the system. Cyberbullying can thus be classified as either explicit or implicit depending on clarity (Tan, 2019; Zeng et al., 2019; Caselli et al., 2020; Li, 2020). In outlining which words did and did not indicate bullying, Waseem et al. (2017) distinguished abusive language by its degree of explicitness. Li (2020) classified words into a cyberbullying word category and

sensitive cyberbullying category. Explicit cyberbullying language has a clear negative meaning and no hidden meaning; implicit cyberbullying language often contains ambiguous words, sarcasm, and/or an absence of profanity or hateful terms (Waseem et al., 2017). Existing methods can only identify specific types of cyberbullying, such as threats, sexual harassment, and aggression (Chatzakou et al., 2017; Hee et al., 2018); sarcasm and euphemisms are more difficult to detect (Dinakar et al., 2011). The rapid evolution of Internet language will affect keyword-based cyberbullying detection as well (Ali et al., 2018; Tan, 2019).

Given the limitations of relevant studies, meta-information—covering characteristics, such as a user's age, gender, location, and posting history—has been considered for cyberbullying detection (Al-garadi et al., 2016; Chatzakou et al., 2017; Hee et al., 2018). More remains to be learned about the linguistic attributes of cyberbullying in addition to expanding the dimensions of and approaches to detection. Much of the extant cyberbullying detection literature has addressed linguistic features; however, a lack of clarity persists around linguistic characteristics and their meanings in this context.

Linguistic Features of Cyberbullying

Cyberbullying represents a language-related problem in interpersonal communication. The language used online reflects people's internal thoughts, emotional states, and intentions (Habsah et al., 2016) and may contain directly or indirectly offensive words (Fortuna and Nunes, 2018). Cyberbullying is conventionally detected based on linguistic features. Early researchers used n-grams, the bag-of-words approach, and similar techniques to make coarse-grained predictions about cyberbullying content (Dinakar et al., 2011; Reynolds et al., 2011) by analyzing certain linguistic features (e.g., personal words, pronouns). Grammatical and sentimental features have been widely used more recently (Zhao and Mao, 2017; Hee et al., 2018), suggesting the utility of lexical features for cyberbullying detection.

Most studies on cyberbullying detection revolve around two linguistic attributes: lexical features and grammatical features. In terms of lexicality, a trademark of cyberbullying is a high density of vulgar words (Ptaszynski et al., 2016). Most offensive sentences include not only offensive words but also user identifiers (i.e., second-person pronouns, the victim's screen name, and other person-centered terms). Punctuation, such as exclamation points, can also predict offensive content by indicating users' feelings or volume of speaking (Ying et al., 2012). Nobata et al. (2016) summarized 13 types of linguistic features to identify abusive language, such as the number of polite expressions and modal words in text. The politeness principle posits that one's politeness can be measured by the extent of indirectness in discourse; that is, the number of indirect words can be used to evaluate the degree of euphemism and credibility in a sentence. Regarding grammatical features, syntactic characteristics (e.g., dependency relationships between words) are of primary interest. The linguistics of cyberbullying involve the tone and syntax of speech. Scholars have found that speakers who frequently use imperative sentences tend to be more insulting as they deliver stronger sentiments (Ying et al., 2012). Text length can also predict cyberbullying (Nobata et al., 2016). Ying et al. (2012) argued that user-level features (e.g., one's writing style, posting patterns, or reputation) can improve the cyberbullying detection rate.

Linguistic forms of cyberbullying can be influenced by cultural contexts (Saengprang and Gadavanij, 2021). Much of the associated literature has analyzed linguistic features of cyberbullying in Western cultures, especially in English; few studies have concentrated on non-English language cyberbullying in Eastern cultures. Saengprang and Gadavanij (2021) compared the linguistic features of cyberbullying between the United Kingdom and Korea. They discovered that indirect speech acts, usually manifesting as one's adoption of the interrogative mood, were more common in Eastern settings than direct speech

acts. Zhang et al. (2019) found that bullying words were useful for classifying cyberbullying in Japan, with informal language and emerging words in tweets affecting the results of sentiment analysis. Research from Pakistan showed that cyberbullies attacked the victim's appearance through comparisons and certain discourse markers (e.g., capitalization, punctuation, and mathematical symbols; Rafi, 2019). Tan et al. (2019) examined linguistic features of cyberbullying among Malaysian youth from the perspectives of victims, perpetrators, and bystanders. Results indicated that the words these groups used spanned three categories of insults: intellect, physical appearance, and value. Also in Malaysia, language use was found to correlate with people's intentions: insults did more than degrade and belittle in self-deprecating body-shaming posts; insults also helped posters save face and reduced backlash from other netizens (Tan, 2019). Mohd et al. (2021) revealed that the profane words used in different cyberbullying roles were somewhat similar but featured distinct weights and percentages, which could guide cyberbullying detection. In the Chinese language specifically, a linguistic analysis of a Chinese cyberbullying incident revealed that bullies tended to use negative words, derogatory nouns, and more second-person pronouns (e.g., "you") or the victim's real name to accuse the victim. In terms of sentence patterns, posters tended to use exclamatory sentences to convey a certain emotion and use affirmative sentences to judge the victim (Xu, 2021). Li (2019) divided insulting words on Weibo into levels of offensiveness; for example, words in Level 5 were inherently insulting and widely used, whereas those in Level 1 were context-dependent. However, not all cyberbullying comments contain directly offensive words. Terms can be further classified as cyberbullying words (e.g., abusive words, sexual words, and swear words) or as sensitive cyberbullying (e.g., emotional words, emphatic and cathartic words, newly emerging words, idiomatic set phrases, and ordinary words with special meanings; Li, 2020). Li (2020) additionally discovered that cyberbullying words in Chinese and English differed in the use of verbs, adjectives, and nouns. Overall, Chinese cyberbullying words appear more complex than those in English.

Cyberbullying and Digital Citizenship

Cyberbullying is a form of online anomie related to technology misuse, spurred by the ubiquity of the Internet and social networking. Cyberbullying incidents are tied to a lack of digital citizenship education: many people are unaware of how to use technology safely, legally, and responsibly and lack an adequate understanding of what constitutes sound digital citizenship. Unsurprisingly, individuals can be less inhibited and present a unique virtual self under ineffective supervision without realizing whether their behavior has hurt others. A growing number of people are misusing technology or using it freely to the neglect of others' feelings. Confrontation and even cyberbullying have thus become unavoidable. In essence, cyberbullying on social media is closely related to one's level of digital citizenship (Zhong et al., 2021).

From a digital citizenship standpoint, refraining from cyberbullying is an important social skill. The International Society for Technology in Education (ISTE) defines a digital citizen as a person who "recognizes the rights, responsibilities, and opportunities of living, learning and working in an interconnected digital world and acts and models in ways that are safe, legal and ethical" (Brooks-Young, 2017; International Society for Technology in Education, 2019). It is crucial to respect others and to protect oneself and others (Ribble, 2015) when using online social networks. Digital citizenship education is crucial to this aim and has become popular in many countries (e.g., the United States, Singapore, and Australia). We found cyberbullying to be a required module in many online courses, including *Cyberbullying, Digital Drama & Hate Speech* from Common Sense Media; *Ethics and*

Empathy from MediaSmarts; and the *Interland* gaming module from Google. Cyberbullying, as a global issue and common online behavior, will likely continue to be a vital aspect of digital citizenship education.

Cyberbullying entails three elements of digital citizenship: digital etiquette, digital law, and digital rights and responsibilities (Ribble, 2015). Instead of merely improving existing laws and regulations, cultivating ethical digital natives can more effectively combat cyberbullying. Researchers have conducted empirical investigation (Chai et al., 2013; Abd Rahman et al., 2014) but have paid limited attention to devising specific behavioral guidelines (Anderson, 2016; Mangkhang and Kaewpanya, 2021). In a digital society, the civility of language is the most direct and explicit manifestation of a person's level of digital citizenship. Digital citizenship education, supplemented with online social standards based on linguistic analysis, will likely be conducive to developing qualified digital citizens.

Fombad has argued that, legal research on any legal system, legal traditions or topic is either explicitly or implicitly comparative because none is self-contained or self-reliant. Comparative legal research and comparative law is evolving and attracting a lot of attention in the legal scholarly work. Africa, as a region is not an exception. It is very common in Africa to come across research papers or thesis dissertations at undergraduate, masters and doctorate level, where the authors assert that they are undertaking a comparative study. In most cases, the comparative legal research will involve countries beyond the African borders, or doctrines that have evolved and are more established in other jurisdictions. But do the outcome of the research reflect a comparative legal research or what should authors consider when selecting a comparative research method?

In short, at what point does a researcher conclude that, indeed, a comparative study is relevant for their research project? It was during my own research presentation, when I posited that, my study was a comparative study between the European Union (EU) and Common Market for Eastern and Southern Africa (COMESA), I realized despite having used the term 'comparative analysis' on various occasions, it was more than what I had contemplated. The questions that followed left me dumbfounded and I could not answer them clearly and with certainty.

The questions asked were: how was my study an actual comparative study?; why a comparative study?; why did I choose the EU and not the US or any other existing regional regime in Africa?; what was the 'construct equivalence'?; what was I going to compare? and why the comparison?; how was I going to compare the two?; and which method of data collection was I going to use in carrying out the comparative analysis? Finally, what was my research question and how was I going to use both cases to provide an answer? Was a comparative research necessary? Would I still answer my research question and objectives without a comparative study?

The essence of these questions border on understanding comparative research methods. It also seeks to enable a researcher answer the why, where, what, when and how questions in selecting a research method and design. Having difficulty answering these questions I decided to delve further into what comparative research method constitutes by attending research methods classes and reviewing available literature on comparative research methods and I hope this article helps anyone who is seeking to employ a comparative legal research.

Selecting a research method and design

Before you select any research method and design, the first thing as a researcher, is to formulate a clear research question informed by your research topic, aim, interests and theoretical framework. The

assumption is that, you have selected a research topic that not only interests you, but is relevant and contributes to the ongoing conversation.

The next step as vogt provides is to select a research design and method that will provide an answer to the research question. This implies that, you must have a great understanding of research methods and designs as noted by Cane and Kritzer in his detailed book on empirical legal research. Choosing a research method or design is not easy and it is not exclusive either. A researcher can employ mixed methods if necessary to provide an answer to the research question and provide evidence to their argument in a logical manner.

What is comparative legal research?

As this article focuses on comparative legal research, before choosing to employ it, it is critical to understand what it constitutes. Hoecke notes that, 'researchers get easily lost when embarking on a comparative legal research. The main reason being that there is no agreement on the kind of methodology to be followed, nor even on the methodologies that could be followed'. According to Paris the lack of definition of what comparative law is, or what the method of comparative law is has exacerbated the situation.

Despite these concerns, comparative legal research emanates from comparative research methods which is the study of more than two or more macro-level units with the aim of explaining the differences and similarities between the units of analysis. The term 'comparative' implies that, a researcher seeks to compare one subject with another.

At the core of comparative research methods, some authors argue that some extent of similarities referred to as, the 'comparability' or 'construct equivalence' should exist. Esser and Vliegenthart assert, 'a key issue in concluding comparative empirical research is to ensure equivalence, that is, the ability to validly collect data that are indeed comparable between different contexts and to avoid biases in measurement, instruments and sampling`. Yet, in real life scenarios, 'comparability' may not reflect similarities. Explaining equivalence is also undermined by the single reason that, meaning of any concept is contextual.

Örücü has argued that the concept of comparability which stipulates that things to be compared must be comparable is not entirely practical. What a researcher requires to show, is why they believe that the two unit of analysis should be compared by studying both similarities and diversity and taking into consideration the social context. Understanding the aim and goal of comparative study is therefore critical. This takes us to the next question, why comparative legal research?

Why comparative legal research?[32]

After understanding, what is comparative legal research, you have to justify why you selected it. Paris posits that, 'the researcher in a comparative law, while going through the different stages of the comparative analysis, has to set her own parameters of research within the theoretical framework provided in the comparative law literature and has to justify the direction she chooses to give as regards her methodological choices. In short, the researcher has to master the art of justifying her choices about why and how she uses comparative law'.

In answering the why question, it will be prudent to understand the aims and theoretical underpinnings of comparative research methods which seek to provide conclusions beyond single cases. Mills and others argue that, 'the underlying goal of comparative analysis is to search for similarity and variance'.

[32] https://www.afronomicslaw.org/2020/01/24/comparative-legal-research-a-brief-overview

According to Wilson, 'by looking overseas, by looking at the other legal systems, it has been hoped to benefit the national legal system of the observer, offering suggestions for future developments, providing warnings of possible difficulties, giving an opportunity to stand back from one's own national system and look at it more critically, but not to remove it from first place on the agenda'.

In the modern globalized world and multidisciplinary research, comparative legal research is not limited to the analysis of national legal systems as was conceptualized in the 19th and 20th century. Further the traditional aims of comparative legal studies which sought to harmonize laws especially in the Europe are questionable in the modern age. For instance, after colonization, most of the African countries adopted laws that were entirely a transplant of their former colonies as a result of western imperialism missing the contextualization of the African societies. This has led to massive reforms of the laws to reflect the realities in the various African societies. Scholars such as Shako have called for the need to dismantle the legacies of colonization.

Justifying the case selection

As you seek to justify why you selected comparative legal research methods, another hurdle is justifying case selection. Case selection and the sampling in comparative research methods is closely linked to the concept of 'comparability' and 'construct equivalence' as discussed above. As a researcher you must carry out a thorough contextual approach. This will involve considering the historical and socio-economic context of the subjects under study to provide a better understanding and avoid unnecessary biasness.

In essence case selection, narrows down to the 'why' question and understanding the aim of comparative research methods. For instance, you can use comparative analysis where a doctrine originated in a certain jurisdiction and it is well embedded to inform its application in another jurisdiction where the doctrine is still novel. So, before you indicate that you are carrying out a comparative analysis study between Nigeria and the US, on the fight against terrorism, you must justify why you chose US and not Kenya. For guidance see Erbele, Eser, Fombad. Epstein and Martin, Cane and Kritzer.

You have justified why you selected a comparative legal research to answer your research question and also your case selection, the next hurdle is to explain how you are going to use the comparative legal research design. In what way are you going to compare these two cases? Hoecke, posits six methods for comparative research: 'the functional method, the structural method, the analytical method, the law-in-context method, the historical method and the common-core method'. To understand these methods and how you can employ each see Michaels, Karst, Monateri, Leckey, Eberle, and Frohlich.

Definition of Cyberstalking

Cyberstalking involves the use of technology (most often, the Internet!) to make someone else afraid or concerned about their safety[33]. Generally speaking, this conduct is threatening or otherwise fear-inducing, involves an invasion of a person's relative right to privacy, and manifests in repeated actions over time[34]. Most of the time, those who cyberstalk use social media, Internet databases, search engines, and other online resources to intimidate, follow, and cause anxiety or terror to others[35].

[33] Fisher, B.S., F.T. Cullen, and M.G. Turner, Being pursued: Stalking victimization in a national study of college women. Criminology & Public Policy, 2002. 1(2): p. 257-308.

[34] Spitzberg, B.H. and G. Hoobler, Cyberstalking and the technologies of interpersonal terrorism. New media & society, 2002. 4(1): p. 71-92.

[35] Loftus, M., The Anti-Social Network: Cyberstalking Victimization Among College Students. Journal of the American Academy of Child & Adolescent Psychiatry, 2016. 55(4): p. 340-341.

Surprisingly, cyberstalking rarely occurs by a stranger (although we do hear about those cases when they involve celebrities and rabid fans), and most often is carried out by a person the target knows intimately or professionally.[36]. For example, the aggressor may be an ex-girlfriend or ex-boyfriend, former friend, past employee, or an acquaintance who wants to control, possess, scare, threaten, or actually harm the other person. In many cases, they have had access to certain personal information, accounts, inboxes, or other private knowledge regarding their target's daily routine, lifestyle, or life choices[37].

Difference between Cyberstalking and Cyberbullying

We argue that cyberstalking is one form of cyberbullying, especially when considering our definition of the latter ("willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices"). Cyberstalking behaviors may include tracking down someone's personal and private information and using it to make them afraid, texting them hundreds of times a day to let them know you are watching them, "creeping" on their social media accounts to learn where they are so you can show up there uninvited, or posting about them incessantly and without their permission[38]. The common denominator is that the behavior makes the target extremely concerned for their personal safety and causes some form of distress, fear, or annoyance.

Stories of cyberstalking are frequently covered by the mainstream media when famous people are involved (you can find incidents related to Selena Gomez, Madonna, Justin Bieber, Beyonce, Justin Timberlake, Kim Kardashian, Britney Spears, and others with a simple Google search) but media headlines often do not accurately convey the true nature and extent of the phenomenon. Unfortunately, academic researchers have largely neglected studying cyberstalking on a broad scale, and we only have a couple recent national studies from which to draw upon. The cool thing is that their prevalence rates are pretty darn close to another, and I believe paint an accurate picture of how often this is occurring across America.

How Often Does Cyberstalking Occur?

First, the Data & Society Research Institute and the Center for Innovative Public Health Research[39] published findings from a 2016 nationally-representative study of 3,002 persons 15 and older, and found that of 8% of American internet users have been cyberstalked to the point of feeling unsafe or afraid. Second, the Pew Research Center [12] surveyed 4,248 US adults online in 2017, and identified that 7% of Americans have been stalked online. Young persons under the age of thirty, and particularly women between the ages of 18-24, seemed vulnerable to the most "severe" forms, including physical threats and sexual harassment. Indeed, based on their analyses of data from multiple years, Pew has argued that the proportion of Americans who have been subjected to these types of behaviors is rising at a modest clip[40].

What are Some Features of Cyberstalking?

While the phenomenon of stalking has been around for decades – warranting numerous laws on a state and national level prohibiting it and setting penalties for law violation – it is arguable that cyberstalking

[36] Sheridan, L.P. and T. Grant, Is cyberstalking different? Psychology, crime & law, 2007. 13(6): p. 627-640.

[37] Reyns, B., B. Henson, and B. Fisher, Being pursued online: Applying cyberlifestyle-Routine Activities Theory to cyberstalking victimization. Criminal Justice and Behavior, 2011. 38(11): p. 1149-1169.

[38] Nobles, M.R., et al., Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. Justice Quarterly, 2014. 31(6): p. 986-1014.

[39] Lenhart, A., et al., Online harassment, digital abuse, and cyberstalking in America. 2016: Data and Society Research Institute.

[40] Duggan, M. Online Harassment 2017. 2017.

occurs more readily given the use of already ubiquitous Internet-based platforms and resources to help accomplish the victimization[41]. Indeed, it is difficult to conceptually differentiate between the two because of their undeniable overlap given the explosion of social media and 24/7 connectivity and the reality that stalkers would naturally extend their reach through online means[42].

A primary factor has to do with instant gratification. That is, the perpetrator can find and target his or her victim immediately and without many obstacles. To be sure, cyberstalking can occur in a most efficient manner since many individuals share much of their lives online via social media, which provides background information, location, personal interests, family and relationship details to learn and exploit. Social media, the constant presence and use of our phones, tablets, and other devices, and our 24/7 reachability and connectivity can provide would-be aggressors the ability to constantly message, post, or otherwise invade the mind and emotions of targets. If this has happened to you, you deeply understand the feelings of invasion and violation that surface.

Another reason why stalking online may be more attractive to perpetrators is because they can easily pursue their targets from a geographically-distant location, making it exponentially harder to identify, locate, and prosecute them. Armed only with Internet access and their phone, tablet, or laptop, a stalker can get online and threaten his or her target from another city, state, or continent, and even shield or hide his or her location. This introduces much fear and worry as to what the perpetrator may do next, and whether that person is far away or very close nearby.

Aside from that, jurisdictional issues become more complex when dealing with , as it is not clear whether prosecutors should look to state law or apply federal law in cases where events cross state lines [5, 19]. In addition, if there is evidence in various jurisdictions, how does one collect it all? Should other law enforcement agencies get involved or offer assistance? What primary or secondary role should they play, and how should they work with Internet or cell phone companies, or social media sites, in order to obtain the digital evidence necessary to build out a case? In these situations, the proverbial waters are very murky.

What Are Some Examples of Cyberstalking Laws?

Even though there is no federal law on cyberbullying, there absolutely is one that covers cyberstalking. It stipulates various ranges of imprisonment for anyone who uses electronic communications technology to engage in conduct that places a person, an immediate family member, or a spouse or intimate partner in reasonable fear of death or serious bodily injury, or "causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person."

Over the last few decades, states also have realized the necessity to pass laws concerning stalking by electronic means to protect their citizens. For instance, Florida incorporates cyberstalking into its (traditional) stalking statute (§ 784.048) and states that cyberstalking means engaging "in a course of conduct to communicate … words, images, or language by or through the use of … electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose." In that state, "willfully, maliciously, and repeatedly" cyberstalking

[41] Goodno, N.H., Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. Mo. L. Rev., 2007. 72: p. 125.
Parsons-Pollard, N. and L.J. Moriarty, Cyberstalking: Utilizing what we do know. Victims and Offenders, 2009. 4(4): p. 435-441.

[42] Alexy, E.M., et al., Perceptions of cyberstalking among college students. Brief treatment and crisis intervention, 2005. 5(3): p. 279.

another is a first-degree misdemeanor, and can be a third-degree felony when coupled with a credible threat.

California also incorporates cyberstalking into its stalking statute. Section § 646.9 of the California Penal Code (entitled "Stalking") provides in part that: "Any person who willfully, maliciously, and repeatedly follows or … harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking." California law states that a "credible threat" can be verbal or written, "including that performed through the use of an electronic communication device, or a threat implied by a pattern of conduct or a combination of verbal, written, or electronically communicated statements and conduct, made with the intent to place the person that is the target of the threat in reasonable fear for his or her safety or the safety of his or her family, and made with the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety or the safety of his or her family." This crime is punishable by up to one year in jail, or by a fine of $1,000, or by both.

In contrast with states that incorporate the new behavior into older laws, the Washington State Legislature created a new statute for cyberstalking (RCW 9.61.260) that is completely separate from its (traditional) stalking statute. The particular language of Washington's cyberstalking law states that a "person is guilty of cyberstalking if he or she, with intent to harass, intimidate, torment, or embarrass any other person … makes an electronic communication to … a third party … using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act; anonymously or repeatedly whether or not conversation occurs; or threatening to inflict injury on the person or property of the person called or any member of his or her family or household." In Washington, cyberstalking is classified as a misdemeanor, unless the perpetrator has previously been convicted of harassment or threatens to kill his or her target. In that case, the crime is classified as a felony.

CHAPTER-V
IMPACT ON VICTIMS AND SOCIETY

The negative implications of bullying on victims are well documented in literature (see, for instance, P. Smith et al., 2006), and many countries have attempted to address this issue through a wide range of regulatory instruments. Nonetheless, bullying persists in workplaces, schoolyards, and various other public and private spaces, and it is now also exacerbated by the use of information and communication technologies (hereinafter: ICT).

ICT offer potent means for perpetrators to target potential victims. These technologies can involve text messages, picture/video clips, phone calls, emails, chat-rooms, websites/online fora, social network sites, etc. (R. Dredge et al., 2014). The term that has been used most often to describe aggressive conducts, including bullying, carried out through ICT is "cyberbullying". As we highlight in the course of this study, cyberbullying is a particularly pernicious phenomenon, since it can cause significant negative consequences on victims with "just a few clicks" (M. Fertik and D. Thompson, 2010, p. 2). Most of the research on cyberbullying, so far, involves adolescents and educational settings (for instance, P. Smith, 2016). Fewer studies, instead, have been devoted to cyberbullying in the world of work. The increasing and pervasive use of ICT in modern work environments and arrangements, nonetheless, calls for much more attention to the implications of cyberbullying in this context.

Notably, the instruments on violence and harassment that have recently been adopted by the ILO pay heed to these developments. Article 3 of the Violence and Harassment Convention, 2019 (No. 190) understands violence and harassment[43] in the world of work as "occurring in the course of, linked with or arising out of work" also "(d) through work-related communications, including those enabled by information and communication technologies;". The use of ICT to conduct unacceptable behaviour is, then, included in the scope of the instruments as long as this concerns "work-related communications". Moreover, Article 4 mandates to adopt "an inclusive, integrated and gender-responsive approach for the prevention and elimination of violence and harassment in the world of work", which should also "take into account violence and harassment involving third parties, where applicable".[44] The instruments, therefore, arguably cover work-related communication between workers (broadly understood as discussed below), employers, and third parties.

As we point out in the course of the study, a broad understanding of the "world of work" is essential to adequately address all instances of cyberbullying, which, by its very nature, can occur anytime and anywhere. In addition to this broad understanding, Articles 2 and 4 of Convention No. 190 indicate that all individuals who are involved in a work or professional scenario are potentially addressed by the instrument. The Convention, therefore, has both a broad spatial and personal scope. It protects workers and other persons in the world of work, including employees as defined by national law and practice, as well as persons working irrespective of their contractual status, persons in training, including interns and apprentices, workers whose employment has been terminated, volunteers, jobseekers and job applicants, and individuals exercising the authority, duties or responsibilities of an employer. Third parties such as clients, customers, service providers, users, patients and members of the public should also be taken into account when devising measures to prevent and eliminate violence and harassment in the world of work.[45] This study also espouses such a broad understanding and, therefore, it also adopts an inclusive view of the potential beneficiaries of measures against cyberbullying.

This means that workers, jobseekers, managers, supervisors, employers and third parties should all be protected against violence and harassment, including cyberbullying, in the world of work.4 As shown in the appendix, a high number of regulatory provisions concerning bullying and harassment pay regard to the implication of these phenomena on "human dignity". A comparative analysis of national legislation in this area seems to confirm that harassment, bullying and similar forms of unacceptable behaviours can be seen as forms of "human rights violation or abuse".[46] As we argue below, this warrants that protective measures go beyond the traditional boundaries of employment regulation and, in particular, cover all workers, regardless of their contractual arrangement or employment status. This contribution thus aims at embracing the world of work in general. Literature and legislation, however, mainly focus on workers; hence, our analysis sometimes reflects such focus. Nonetheless, the study makes as many references as possible to employers and third parties and calls for further interdisciplinary studies to expand research in this area towards a broader personal scope.

[43] Under the Violence and Harassment Convention, 2019 (No. 190), "the term "violence and harassment" in the world of work refers to a range of unacceptable behaviours and practices, or threats thereof, whether a single occurrence or repeated, that aim at, result in, or are likely to result in physical, psychological, sexual or economic harm, and includes gender-based violence and harassment" (Article 1).

[44] Violence and Harassment Convention, 2019 (No. 190), Articles 3 and 4.

[45] Violence and Harassment Convention, 2019 (No. 190), Articles 2 and 4; see also Violence and Harassment Recommendation, 2019 (No. 206), paragraph 8.

[46] The quoted text is in the Preamble of Convention No. 190.

The primary aim of this study is to examine legal sources around cyberbullying and other ICT-mediated aggressive conducts in the world of work. Our entry point was to understand how law-makers take ICT and its abuses into account when drafting measures against aggressive and unacceptable conducts. When undertaking this study, we realized the paucity of legal provisions concerning cyberbullying around the world as it is a relatively novel phenomenon. Therefore we thought it helpful to conduct our research by framing cyberbullying also against the background of legal provisions and case law that address conducts such as traditional bullying and harassment in the world of work (and their counterparts in non-English-speaking countries). We followed the same approach when reviewing the psycho-sociological literature to support our legal analysis. Our main interest was to examine whether this literature permits to understand how technology can influence and shape the traditional concepts of bullying and harassment in the world of work, the conducts of the perpetrators and the impact on victims and societies at large. It is not the aim of this study to be a general reference about these traditional conducts, let alone psychosocial risks at large. We advance conclusions regarding these conducts only if we see it useful also to address ICT-mediated conducts.

Another word of caution is needed concerning the ILO Convention concerning the elimination of violence and harassment in the world of work, 2019 (No. 190) and Recommendation concerning the elimination of violence and harassment in the world of work, 2019 (No. 206). These instruments were adopted by the International Labour Conference at its 108th session in June 2019 while this study was being prepared. Hence the reference to some of their provisions, as they were pertinent to the subjects of this study. This study is not aimed at providing a commentary to these newly-adopted ILO instruments whose scope is much broader than ICT-based unacceptable conducts.

Definitions and understanding of cyberbullying

What is (cyber)bullying?

There is no single definition of cyberbullying, or of bullying, which is internationally accepted. "Cyberbullying", instead, continues to be used as an umbrella term for a range of aggressive behaviours that are perpetrated through ICT (J. Bailey, 2014). The absence of an established definition is, in fact, seen as problematic by some scholars (H. Hoel and D. Beale, 2006). Having regard to this, our working definition is based on established literature tackling the issue of bullying in the world of work. It refers to relevant research in social sciences, as well as on legal definitions found in national regulation.

In particular, we draw on the psychological and sociological literature on bullying. Some definitions from that literature have been referenced and relied upon by numerous sources, as we discuss below. Cyberbullying is not explicitly defined in this literature; it is, however, commonly considered an extension of bullying. Both bullying and cyberbullying are seen, in fact, as forms of, or linked to, aggressive behaviour (P. C. Rodkin and K. Fischer, 2012; L.R. Betts, 2016, p. 2). In the course of this study, we follow a similar approach – our understanding of cyberbullying shares several structural elements with traditional bullying.[47]

[47] For views that argue the contrary, according to which bullying and cyberbullying are fairly distinct, see for example Corcoran, L. et al., 2015. L. R Betts (2016, p. 4) reports: "In particular, some authors argue that cyberbullying represents a distinct phenomenon which should be defined as such (e.g., Pieschl, Kuhlmann, & Prosch, 2015), whereas other authors advocate that cyberbullying is an extension of face-to-face bullying (e.g. Juvonen & Gross, 2008; Olweus, 2013) with researchers seeking to apply definitions of face-to-face bullying to cyberbullying (e.g. Calvete, Orue, Estévez, Villardon, & Padilla, 2010)".

A definition of "bullying at work" that has gained considerable influence has been proposed by Einarsen et al. In these authors' view, "bullying at work means harassing, offending, socially excluding someone or negatively affecting someone's work tasks. In order for the label bullying (or mobbing) to be applied to a particular activity, interaction or process it has to occur repeatedly and regularly (e.g. weekly) and over a period of time (e.g. about six months). Bullying is an escalating process in the course of which the person confronted ends up in an inferior position and becomes the target of systematic negative social acts. A conflict cannot be called bullying if the incident is an isolated event or if two parties of approximately equal 'strength' are in conflict" (S. Einarsen et al., 2011, p. 22; see also K. Lippel, 2010; L. Barmes, 2015; P. D'Cruz, 2015).

Several elements can be clearly identified in this definition: a certain degree of repetitiveness or persistence of the conducts; the fact that "exposure [to the behaviour] occurs over a long time-period" (M. B. Nielsen and S. Einarsen, 2018, p. 73) and an unequal power relation. These elements are all extensively discussed in the existing literature (see, for instance, C. Privitera and M. A. Campbell, 2009; C. Langos, 2012).

Concerning the element of repetition and duration, a crucial question is whether the perpetrators' acts have to be repeated, or whether it suffices for the victims to be repeatedly exposed to their effects. In both cases, the exact frequency and duration needed for a certain behaviour to be considered bullying are arguably vague (L. Barmes, 2015, p. 14). The original reason to identify these elements in bullying was the need to differentiate it from "personal conflicts of a more episodic character" (M. Agervold, 2007, p. 165). This traditional view on bullying would not consider single events to constitute "bullying", even if victims are repetitively confronted with the effects of that one incident.

One-off events, however, can also significantly harm victims (P. D'Cruz, 2015, pp. 12-13). Some authors, thus, suggest that a singular event can in some cases be deemed bullying, having regard to its impact (R. Slonje et al., 2012, p. 245; S. Branch and J. Murray, 2015, p. 288). The consequences of the one-off event would have to be repeated regularly for a prolonged period (S. Einarsen et al., 2011, pp. 11-13).

The third element of the definition above implies the existence of an unequal power relationship between the victims and perpetrators. The imbalance of power as a defining feature, nevertheless, may be overlooked by victims of bullying, as indicated by the answers given to semi-structured interviews on the matter (R. Dredge et al., 2014, pp. 17-18). An imbalance of power can be due to the perpetrators' characteristics, such as a physical advantage, social status and/or the vulnerability of the victim, related, for instance, to problems in communicating or ICT illiteracy (H. J. Thomas et al., 2015, p. 136). It is worth noting, however, that power imbalance is not necessarily a static fact. The victims might react to the bullying behaviour and might, for example, show resilience and reverse the power relationship, or might indeed be overwhelmed by the perpetrators' acts, thereby finding it hard to react in the course of the bullying process. Even in situations of initial equal strength between two parties, bullying can occur when one party – the prospective victims – becomes defenceless in comparison to the perpetrators (S. Matthiesen and S. Einarsen, 2007, p. 735; S. Branch et al., 2013, p. 282; P. D'Cruz, 2015, pp. 11-12). Power imbalances, therefore, can fluctuate, making them also a problematic element to assess (P. Lutgen-Sandvik, 2006; E. Menesini et al., 2012, p. 459).

An additional element, not evident in the definition discussed above, is the intention to target the victim, which some scholars identify as an additional definitional criterion (P. Saunders et al., 2007, p. 345). Other studies, however, explicitly dismiss this criterion, as well as the need for an intention to harm, as

parts of the definition of bullying (M.B. Nielsen and S. Einarsen, 2018, p. 73; P.C. Rodkin and K. Fischer, 2012, p. 624). Motives or reasons underlying the relevant behaviour can change in the course of the bullying process. They can also vary according to the specific environment in which they take place. The reasons behind bullying someone at work can, for instance, be different from the ones found in educational settings.[48]

In this respect, it is also worth noting that the potential victims may, of course, have different sensitivities. Victims can be distressed regardless of the bullies' intent to harm and what might not be regarded as bullying by one individual can be perceived as bullying by another. As such, whether or not a specific act is apt to harass, offend, socially exclude or negatively affect the victim's work is to be objectively approached. It suffices for the behaviour to have a foreseeable effect on the target. Someone might, therefore, perpetrate bullying unconsciously (S. Einarsen et al., 2011, p. 9), as long as the behaviour is knowingly directed at the victims. Objectively minor behaviours shall, consequently, not constitute bullying (S. Branch et al., 2013, p. 281). As already said, however, in general, intention to harm is not perceived as a key element in the literature on bullying in the world of work (S. Einarsen et al., 2011, p. 18).

What are the differences between bullying and cyberbullying?

Even though definitions of cyberbullying usually draw upon the same essential elements identified for bullying (P. Smith et al., 2006, p. 6; R. M. Kowalski et al., 2014, p. 1074; H. J. Thomas et al., 2015, p. 137), the use of ICT may still alter some essential features and implications of traditional bullying (R. Dredge et al., 2014).

One element that is affected considerably is repetition. Some authors argue that repetition manifests itself differently in the case of cyberbullying (L.R. Betts, 2016, pp. 38-39). The repetitiveness of acts of cyberbullying is more difficult to ascertain. ICT, for instance, may allow individuals to repeatedly access the aggressive content that has been posted online in one sole occasion. One act could also confront the victims repeatedly without the perpetrators having necessarily intended such an outcome. In such instances, other individuals, instead of the primary perpetrator, might have caused the harmful conduct to be repetitive (D. B. Sugarman and T. Willoughby, 2013, p. 2; L. R. Betts, 2016, p. 38). This, in turn, may make "repetition" less reliable as a defining criterion for cyberbullying (E. Menesini et al., 2012, p. 459). If repetition is indeed seen as a proxy for severity (P.C. Rodkin and K. Fischer, 2012, pp. 624-625), then the unwanted reverberations of one act of cyberbullying should be considered as indicators of repetition. Such reverberations, which, for instance, can come in the form of re-tweets, shares, forwards, etc., can reach an enormous and uncontrollable audience (D. Kernaghan and J. Elwood, 2013). Related to this is the fact that, contrary to traditional bullying, records of cyberbullying may end up being unerasable in practice. In this respect, it has been argued that "direct cyberbullying involves a perpetrator repeatedly directing unwanted electronic communications to a victim" while "indirect cyberbullying involves directing a single or repeated unwanted electronic communications" (C. Langos, 2012, p. 288). Indirect cyberbullying requires the perpetrator to use "reasonably public areas of

[48] Internal competition and difficulties in laying off employees have, for example, been mentioned as incentives for workplace bullying (D. Salin, 2003, p. 1218). Others identify working environments and destructive forms of leadership as factors that influence the incidence of bullying at work, or assert that "a conflict between superiors and subordinates is an important antecedent of bullying, and more so than organizational changes" (A. Skogstad et al., 2007, p. 84; see also L. J. Hauge et al., 2007, pp. 239-240).

cyberspace" instead of private channels (C. Langos, 2012, p. 286). Direct cyberbullying, instead, would necessitate direct contact with the victims.

A second element that is affected is the "unequal power" between the victims and perpetrators. Technological savviness can result in a power imbalance (R. M. Kowalski et al., 2014, p. 1107). This is also true, according to some authors, for the possibility to bully anonymously (P.C. Rodkin and K. Fischer, 2012, p. 626; D. B. Sugarman and T. Willoughby, 2013, p. 2). Moreover, while, on the one hand, the use of ICT might exacerbate existing imbalances of power, on the other hand, it might also mitigate or reverse this imbalance. Indeed, supervisors, managers, or even employers can be victimized by persons or groups of persons who report to them, through the use of ICT means, particularly because they facilitate anonymous conducts.

Another remark concerns the reasons and drivers of cyberbullying behaviours. Social networks can, for example, offer "new arenas to harass, humiliate, or threaten" (D. B. Sugarman and T. Willoughby, 2013, p. 2), and coincidentally cyberbullying can serve as an "alternative medium" (C. Privitera and M. A. Campbell, 2009, p. 395) to help the perpetrators' ends. Some studies, nevertheless, argue that cyberbullying is rather one new – unique – phenomenon, instead of merely an alternative iteration of bullying (A. Baroncelli and E. Ciucci, 2014, p. 813). For instance, this could be because "the reward for engaging in cyberbullying is often delayed (in contrast to face-to-face interactions), and this is anticipated to have an effect on how goals for these aggressive interactions are formed and pursued" (J.J. Dooley et al., 2009, 187).

Although some differences in the reasons and drivers of cyberbullying relative to bullying may exist, these differences should be taken with caution. It should not be neglected that perpetrators may attack the victims through both traditional and cyber-means (J. Raskauskas and A.D. Stoltz, 2007, p. 570; R. M. Kowalski et al., 2014, pp. 1123-1124), something that can have a particular bearing in work-related matters (I. Coyne et al., 2016), especially when it comes to internal bullying. This could be different for external bullying, where contact can be more casual, and chances may be lower for the behaviour to repeat itself. External perpetrators may also be less likely to know the actual personal identity of the victims.

Another critical feature of cyberbullying is the potential for an easier moral detachment of "cyberbullies" from the victim, than what would be the case for bullying. This view originates from the understanding that, to bully another, perpetrators go through certain psycho-cognitive processes. Those processes might not be entirely identical in case of bullying and cyberbullying.13 Moral disengagement is defined in the relevant literature as "the socio-cognitive process through which humans are able to harm others without having a bad conscience" (S. Wachs, 2012, p. 349). Some studies indicate that cyberbullies show even less remorse than traditional bullies (R. Slonje et al., 2012, p. 254), and that moral disengagement can be higher for cyberbullies than for traditional ones (S. Wachs, 2012, p. 350). In this regard, C. D. Pornari and J. Wood (2010, p. 89) observe: "It is likely that the anonymity, the distance from the victim, and the consequences of the harmful act do not cause so many negative feelings (e.g. guilt, shame, self-condemnation), and reduce the chance of empathizing with the victim".

Although these studies concern children and adolescents, a similar dynamic may occur among adults. In comparison to traditional bullying, therefore, cyberbullying may lead to an increased emotional disconnection between the perpetrators and victims, since the perpetrators are not directly confronted with the victims' reactions and emotions. Some authors refer to this phenomenon as an "online disinhibition effect", which amounts to people saying and doing things "in cyberspace that they

wouldn't ordinarily say and do in the face-to-face world" (J. Suler, 2004, p. 321). As a result, less empathy and remorse would be shown and perpetrators would say and do things online that they would not say or do offline (T. Aricak et al., 2008, p. 256; R. M. Kowalski et al., 2014, p. 1107).

An indicative example of such behaviours can be traced in abusive tweets sent to members of national parliaments (MPs), especially when it comes to women MPs. It has been noted: "while online abuse is certainly not limited to women in the public eye, women politicians face an extraordinary amount of abuse on social media" (A. Dhoria, 2017). Online abuse against women can thus be facilitated by the use of ICT and by the emotional detachment between the victims and the perpetrators that can come with it. Interviews with women MPs also highlight the severe psychological impact of online abuse (Amnesty International, 2018).

Besides, contrary to popular belief, the Internet is not a neutral place (S.U. Noble, 2018). Social network timelines tend to reflect individuals' opinions and biases, and as such, reinforce stereotypes (echo-chambers). This may exacerbate the propensity of pursuing aggressive conducts. Such conducts, moreover, are not limited to verbal abuses. In a case in Australia, for instance, one of the actions that the Fair Work Commission considered, in issuing an order to stop some bullying conducts at work, was the perpetrator unfriending the victim on Facebook (J. Pearlman, 2015).[49]

Cyberbullying, of course, is not limited to conducts occurring on social media. For instance, a study about Australian manufacturing workers found that "the most frequently reported negative act via modern technology was "someone withholding information" by email […] and/or by telephone […]". Some 37.5 per cent of the respondents also reported having been exposed to an unmanageable workload by email or having being affected by the spread of gossip by telephone as instances of cyberbullying they experienced (C. Privitera and M. A. Campbell, 2009, p. 398).

This propensity is also linked to the fact that cyberbullying can lead to extensive anonymous bullying (J. J. Dooley et al., 2009, p. 184). Research on adolescents has shown that the percentage of victims of cyberbullying that knows the identity of the perpetrators varies from 43 per cent to 80 per cent (W. Cassidy et al., 2013, p. 579). Such potential for anonymous bullying is problematic because research indicates that anonymity is a risk factor for future cyberbullying behaviours (C. P. Barlett and D.A. Gentile, 2016, p. 179). This is possibly due to a "misgiven" sense of impunity that comes with anonymity – a sense of impunity that is linked to the belief that it becomes more difficult to identify the perpetrators for both the victims and law enforcement through cyberbullying (N. H. Goodno, 2007, p. 131; J. D. Lipton, 2011, p. 1114). Certain digital communication tools like Snapchat, where messages are temporary by default, might even exacerbate this sense of impunity.

Finally, another factor that plays into this feeling of impunity is the fact that an online environment may have fewer direct bystanders than an offline environment has (S. Wachs, 2012, p. 356). This can be consequential for the victims. Existing literature presents mixed evidence on the role of bystanders. On the one hand, the presence of bystanders can stimulate bullying; on the other hand, bystanders can also counter it (C. Salmivalli, 2014, p. 286). It is, therefore, all the more important to reduce the likelihood of bystanders playing a negative role in the world of work. Promoting participation in anti-bullying programmes, for instance, has been shown to give positive outcomes in relation to school students (S. Saarento et al., 2015, p. 71).

[49] See Fair Work Commission, [2015] FWC 6556.

Based on our findings, it is evident that despite the shared features between bullying and cyberbullying, ICT-elements have the potential of exacerbating the already negative implications of traditional bullying, by magnifying the repetitiveness of aggressive conducts, augmenting moral disengagement and facilitating anonymous behaviours. This is also particularly important because, as discussed below, cyberbullying can occur and affect the victims anytime and anywhere.

Multiple overlapping concepts

A research conducted by the European Foundation for the Improvement of Living and Working Conditions (Eurofound) on violence, bullying and harassment in the workplace distinguishes between "physical violence", "harassment, bullying or psychological violence" and "sexual harassment" (Eurofound, 2007, p. 3). Psychological violence would often manifest itself through repeated acts, "which cumulatively can become a very serious form of violence" (V. Di Martino et al., 2003, p. 4). This category of psychological violence, according to some authors, includes bullying, mobbing and sexual harassment (D. Chappell and V. Di Martino, 2006, p. 17). According to other studies, conducts such as bullying, mobbing, acoso, hostigamiento moral, harcèlement moral, harcèlement psychologique and psychological harassment all fall under the category of "psychological violence" (K. Lippel, 2016, pp. 9-10).

Although some authors argue that harassment is inherently characterized by the targeting of someone because of a specific characteristic, in particular on the basis of discriminatory grounds (C. Caponecchia and A. Wyatt, 2009, p. 442), harassment is sometimes also used as a stand-alone concept. This is illustrated, for instance, in Brodsky's definition of harassment: "repeated and persistent attempts by one person to torment, wear down, frustrate, or get a reaction from another. It is treatment that persistently provokes, pressures, frightens, intimidates, or otherwise discomforts another person" (C. M. Brodsky, 1976, p. 2). Compared to bullying, the element of an unequal power relationship is not present in this definition of harassment.

One reason in favour of using the concept of "harassment", instead of "bullying", in regulation might be that if lawmakers intend to grant preventive and redress mechanisms for victims of aggressive behaviours, the inclusion of an "imbalance of power" as a legal requirement might be problematic, given the potential difficulties in defining this element in legal terms, let alone identifying it in practice and providing evidence about it. These difficulties would limit access to legal mechanisms for victims of aggressive behaviours. To mitigate this risk and face these difficulties, legislative policies can adopt a broad definition of their scope. For instance, the Multi-sectoral Guidelines to Tackle Third-Party Violence and Harassment Related to Work take an extensive understanding of "third-party violence and harassment" (European Social Dialogue, 2011). The newly adopted ILO Convention No. 190 and Recommendation No. 206 similarly hinge on "violence and harassment", by defining them as a range of unacceptable behaviours and practices, or threats thereof.

Concerning "cyberbullying", as we already observed, there is no consensus on a specific definition. Various terms, however, have been used to describe other relevant conducts. "Workplace aggression", "abuse", "bullying", "mobbing" and "harassment" are just some examples (W. Martin and H. La Van, 2010, p. 176).

Concepts chosen in national jurisdictions are influenced by the countries' social structures and legal traditions (L. Barmes, 2015, p. 12). Not only do these differences impact national concepts but linguistic problems also exist when trying to draw a comparative reconstruction of the legislation concerning this phenomenon (P. Smith et al., 2002, 1131-1132). "Bullying" is a term more likely to be used in English-

speaking countries, while "harassment" ("harcèlement") is more commonly used in French-speaking countries (B. West et al., 2014, p. 599). Some national legal systems may also use multiple overlapping legal concepts to deal with what may be considered bullying in psycho-sociological terms. An act of cyberbullying can, for example, be considered to constitute unlawful threats, assault, stalking, defamation or a cybercrime (C. Langos, 2013). Due to these reasons, some scholars, such as Schat et al: "reconcile this definitional dilemma by pointing to the fact that '... the behaviors that constitute workplace aggression are generally consistent with the behaviors that constitute these related constructs'" (A.C.H. Schat et al., 2006, p. 49; cited by W. Martin and H. La Van, 2010, p. 176).

CHAPTER-VI
EMERGING SOLUTIONS AND BEST PRACTICES

A substantial body of evidence has established the protective power of a supportive parent-child relationships to strengthen pro-social behaviors and reduce adolescent risk behaviors. Across Western and Eastern cultures, parent supportiveness and communication are associated with academic success, empathy, and pro-social behaviors.[50],[2],[3],[4] Parental monitoring reduces youth substance use, delinquent behaviors, sexual risk behaviors, and bullying in all its forms.[5],[6] However, parents report feeling overwhelmed by technology when it comes to online risks. Unsure of how to successfully monitor online behavior,[7] many parents worry about the effects of cyberbullying on their children. Parents are a critical protective factor for reducing cyberbullying risk at the relational level of the ecological system.

Supportive parent-child relationships protect against cyberbullying and enhance resilience of children who encounter high-risk environments. In a review of the literature, Elsaesser and colleagues found that most studies of parenting and cyberbullying suggested that parent-child relationships were negatively related to cyberbullying perpetration and victimization.[8] Parental monitoring may be less salient than warmth and connectedness.[9] Other research has found mixed results regarding parental monitoring in online contexts, suggesting that restrictive monitoring may not be the most effective.[10],[11] This hypothesis needs further examination, particularly in Eastern cultures. Notably, the majority of these studies were cross-sectional, which underscores the emerging nature of this research.

Because 70% of cyberbullying occurs at home and parents have expressed a need for digital safety information,[12] clear guidance and preventative programming is needed for parents. We know from research across several countries that cyberbullying prevention programs are effective.[13],[14],[15] A large majority of these programs have been implemented in schools and few have included parent support in their programming. Additionally, the majority of cyberbullying preventative interventions have been in European countries, with only a few scattered studies in the US, Middle East, and Australia.[16] In this chapter, we present the current knowledge of parenting strategies that are associated with low cyberbullying, highlighting available longitudinal research. We also emphasize the ways that online contexts may be similar and different to parenting in face-to-face contexts.

[50] Doty JL, Gower AL, Rudi JH, McMorris BJ, Borowsky IW. Patterns of bullying and sexual harassment: Connections with parents and teachers as direct protective factors. J Youth Adolesc 2017 4611. 2017;46(11):2289-2304. https://doi.org/10.1007/s10964-017-0698-0

PARENT-CHILD CONNECTEDNESS AND FIRMNESS AS PROTECTION AGAINST CYBERBULLYING

Warm and caring relationships between parents and children balanced with rules and monitoring directly protect against cyberbullying victimization and perpetration. It may buffer against the negative outcomes of cyberbullying, promoting resilience.[17] Based on these characteristics, four parenting styles have been identified: 1. authoritative parenting characterized by warm and supportive yet firm parenting (e.g., listening to children's perspectives while being consistent with rules); 2. authoritarian parenting characterized by controlling parenting (e.g., being rule and punishment focused); 3. permissive parenting characterized by warmth and support with little support for rules; 4. neglectful parenting characterized by low warmth and low control. Authoritative parenting has repeatedly been shown to have the best outcomes for youth.

With respect to cyberbullying, youth entering secondary school in the Netherlands who reported having authoritarian parents had the lowest levels of cyberbullying victimization and perpetration.[18] Their parents were both warm and set firm rules. However, few longitudinal studies have examined cyberbullying and parenting. In a notable exception of 488 youth in the northwest of the U.S., researchers examined parenting styles, including authoritative parenting and authoritarian parenting.[19] They found that warm and supportive aspects of parenting at age 12 were related to cyberbullying perpetration at age 19. Authoritarian parenting, though, was related to increased risk of cyberbullying perpetration. Similarly, a larger Cyprus study examining the longitudinal effects of parenting on cyberbullying and victimization found that parenting predicted face-to-face and cyber bullying and victimization. Authoritarian parenting had a positive effect on aggression.

Other studies have noted that youth who reported parental warmth had reduced exposure to cyberbullying and were less likely to experience the negative effects of cyberbullying when it did occur. Accordino & Accordino noted that students with closer parental relationships experienced less bullying.[21] Further, in a national U.S. sample, parental support (e.g., helping and comforting) was linked to lower risk of cyberbullying victimization and perpetration. Another study found that cyberbullying and depression were more likely in adolescents with perceptions of low parental attachment compared to adolescents with more restrictive parents.

THE IMPORTANCE OF PARENT-ADOLESCENT COMMUNICATION

Communication between parents and adolescents also has been identified as a protective factor against cyberbullying. In a study of high school students in Valencia, Spain, open communication with mother and father was more prevalent among students who had not been cyberbullied. Avoidant communication was more likely among students who had experienced cyberbullying either occasionally or severely. Similarly, parent-child connectedness, as measured by open communication, was negatively related to cyberbullying victimization and perpetration above and beyond the effects of parents' online monitoring. This suggests that a strong relationship featuring open communication may be more important than monitoring youth behaviors online.

The importance of communication to prevent cyberbullying and protect against its negative outcomes was reinforced in qualitative interviews with parents. For example, in the south of the U.S., parents were intentional about teaching their children to take a different perspective when cyberbullying occurred. An example of one such conversation was, "[I'll ask,] 'Why do you think someone else would do that? They must be sad.' Like, [I'll] talk about these people when they're bullying, 'They have an issue. If they

don't like you, it's an issue in them, not in you. It's not something you did'.[26] They also wanted their children to understand the potential reasons why someone might cyberbully (e.g., poor home life; low self-esteem). Parents also employed communication strategies to empower their children. They taught their children to stand up to bullies to protect others who were vulnerable. They also worked to instill a sense of self-confidence in their own abilities. One parent said, "[My daughter] had an innate talent for music, so we signed her up for piano classes and enrolled her in the school orchestra. She got chosen to represent and sit in the front row and that was a big deal. Beyond that, her grades went up, and she was focusing on her studies, so then we would remind her of that. [We would say,] 'These other kids may be bigger than you …, but you can make music like they cannot'".[27] These parents took a preventative stance against cyberbullying. Given the focus on collective interdependence in India and other Eastern cultures,[28] qualitative research is needed to understand how parents' strategies may differ from parents in Western cultures.

Other research has found that when students did experience cyberbullying, talking to parents was a helpful coping strategy.[29] However, in a mixed methods study of parents and children (6th – 9th grade) in England, Cassidy et al. reported a discrepancy in youth report of cyberbullying (32% victimization; 36% perpetration) and parent knowledge of cyberbullying (11% were aware of cyberbullying incidents).[30] These findings indicate that youth do not always communicate experiences of online harassment with their parents. This is similar to findings in Barlett and Fennel,[31] where parents believed their enforcement of rules to be greater, and their child's cyberbullying behaviors to be lower, than the youth actually reported. In a second study, the researchers also found that cyberbullying behaviors were positively associated with, and predicted by, the extent to which parents were unaware of their children's internet use (see also Chapter 5 on online safety). It may be that youth do not seek adult support because they don't believe that adults will be able to successfully intervene, or they fear losing access to their devices. However, without adult help youth are more likely to engage in maladaptive coping such as avoidance, becoming cyberbullying perpetrators themselves, or physical retaliation against the perpetrator(s). All of these may allow an increase in cyberbullying.[32]

WHY AUTONOMY SUPPORTIVE PARENTING IS IMPORTANT

Experts advocate a mix of parenting strategies to curb cyberbullying and increase online safety. A strong emphasis on active media monitoring and autonomy may be the most effective parenting approach.[33] Media parenting refers to "goal-directed parent behaviors or interactions with their child about media for the purpose of influencing some aspect of the youth's screen media use behaviors."[34] Parents and youth naturally negotiate boundaries—including limits for online activities—over the course of adolescence as young people strive to become more independent and parents strive to keep them safe.[35] Parents and youth demonstrate a range of patterns in these negotiations, but families where parents exert high control and youth push for high autonomy are likely to have the most conflict.[36]

One study found that when youth reported high parental control, they also were likely to report high levels of cyberbullying.[37] In contrast, Ghosh and colleagues found that parents who were involved and autonomy granting, who strictly supervised adolescents online had adolescents who were likely to report low cyberbullying victimization.[38] In other words, a balanced approach may be the best. Similarly, in a study of adolescents, Padilla-Walker et al. found that autonomy supportive media parenting (whether active or restrictive) was associated with high media disclosure.[39] The study also found that when

children voluntarily tell their parents about their online activities, they tend to engage in more pro-social activities and less relational aggression.

A persistent global phenomenon…

Cyberbullying is an attack on people, committed out using digital resources. This type of online behavior is constantly developing and expanding globally. A comparative study (with 25 countries taking part) carried out by Microsoft[51] in 2019 then in 2020, conducted among 12,520 adults, found, for example, that 64% of French respondents and 52% of respondents in the United Kingdom have already been victims of cyberbullying. Another American study[52] found that 41% of American respondents (out of a sample of 10,093 adults) have already been victims of cyberbullying, 28% of whom mentioned serious forms of bullying such as physical threats and sexual harassment.

International researchers currently face epistemological and methodological difficulties, and studies fail to offer a multidisciplinary understanding of cyberbullying, making it difficult to measure and making its prevalence difficult to assess. For example, frequently cited difficulties include access to data, geographically limited samples, or samples that are limited to a specifically targeted population such as minors.

The types and consequences of cyberbullying remain difficult to define. Cyberbullying leads to social exclusion from digital tools: categorizing specific practices means that everyone involved can prevent and effectively combat this social reality.

Cyberbullying is becoming a social reality and is difficult to manage, which makes effective coordination between public and private stakeholders difficult. In order to gain a better understanding of this phenomenon and to avoid unclear definitions, a research project[53] with Bordeaux Montaigne University and the French National Gendarmerie aims to collect and analyze specific data about online attacks or violence, in terms of cyberbullying, so as to specifically categorize the forms that it takes. How can this be achieved?

… With lack of a clear definition

The first step to take in order to delineate cyberbullying from a legal, social and technical perspective is to examine the way in which researchers have dealt with it, both in terms of the associated definitions and in the cases observed.

An initial search of articles using keywords yielded 14,267 articles, in international academic journals, accessible on portals such as Academic Research Ebsco, CAIRN, Open Edition and Scopus Elsevier. Several different terms were included, including online harassment, cyberbullying, cyber aggression, online aggression, and online violence. 311 articles, in French and in English, covering all continents were selected for peer review.

Based on this review of articles, there appears to be very few longitudinal studies. If they do exist, they are often linked to intergovernmental programs involving primary and secondary school students. Though most of the studies concern minors, and a few articles focus on professional groups such as

[51] Microsoft Digital Civility Index (DCI) 2020: Study conducted by "Telecommunications Research Group for Microsoft Corporation", Annual Report entitled "Civility, Security and Online Interaction": https://news.microsoft.com/fr-fr/2021/02/09/safer-internet-day-le-civisme-en-ligne-sameliore-de-3-points-dans-le-monde/

[52] Pew Research Center, January 2021, "The State of Online Harassment": www.pewresearch.org

[53] Project funded by the Digital Enterprise Research Area, led by Guillaume Tardiveau, Research Program Manager at Orange Innovation.

journalists or influencers. It also appears that all disciplines (educational sciences, sociology, psychology etc.) are represented.

More specifically, many articles refer to online attacks directly aimed at the victim, both verbally, for example in the form of argumentative strategies (impoliteness, insults, threats on forums), or in the form of social attacks that may lead to the victim becoming excluded from online groups. Others discuss strategies to cause harm, such as creating a false profile for the victim, impersonating them, or hacking into their personal account.

It appears that, among victims, these forms of cyberbullying generate a change in the way they perceive the online environment, and specifically have a negative impact on their decision-making. Some victims reduce their online activities and connections while others remove them completely due to concerns about their professional reputation [54], suffering a loss of confidence in their effective management of social networks and traditional media[55]. Severe impacts on mental health are noted: this phenomenon produces lasting effects on victims offline, namely mental trauma, emotional stress, loss of motivation and research into retraining[56].

Based on this review of articles, there is a marked tension between the democratic rights that justify some types of misuse (freedom of expression, equal access to networks) and morality, what is legal and what is illegal. Though legislation is evolving, the laws that govern cyberbullying are still very recent, and the burden of proof makes complaints difficult and therefore rare[57].

In summary, cyberbullying, the forms and consequences of which are still difficult to define[58], leads to social exclusion from digital tools (platforms etc.) for victims, a deterioration in social networks and a decrease in the quality of self-expression in public spaces (self-censorship), and even loss of income, creativity and productivity.

A first response aiming to improve the classification of cyberbullying…

As part of the partnership between Orange, Bordeaux Montaigne University and the French National Gendarmerie, a multidisciplinary team harnessing skills in sociology, communication sciences and criminology aims to categorize existing cyberbullying practices and to put effective measures in place in order to help the victims and stakeholders involved to handle them. To this end, a survey was carried out in 2020 on a sample of 150 streamers and YouTubers, in addition to around 30 partially structured anonymized interviews with victims of cyberbullying, key witnesses (e-sports, web TV etc). In addition to these surveys, court records can also be used, which are a unique and exceptional source of analysis. In addition, exploratory interviews can be carried out with various stakeholder in the field of

[54] Bossio, D., and A. E. Holton, 2019. “Burning out and Turning off: Journalists’ Disconnection Strategies on Social Media.” Journalism 20. doi:10.1177/1464884919872076.

[55] Chen, G. M., P. Pain, V. Y. Chen, M. Mekelburg, N. Springer, and F. Troger. 2020. “‘You Really Have to Have a Thick Skin’: A Cross-Cultural Perspective on How Online Harassment Influences Female Journalists.” Journalism 21 (7): 877–895.

[56] Ferrier, M., and N. Garud-Patkar, 2018. “TrollBusters: Fighting Online Harassment of Women Journalists.” In Mediating Misogyny, edited by J. Vickery and T. Everbach, 311–332. Cham: Palgrave Macmillan.

[57] In practice, the police or gendarmerie services have the capacity to file complaints by victims, to investigate cases or, at the discretion of the Public Prosecutor, to engage relevant specialized services: https://www.numerama.com/politique/533735-cyberharcelement-quatre-ans-apres-avoir-porte-plainte-des-victimes-attendent-toujours.html

[58] Joissans S., Bigot J., 2020, “Rapport d’information n° 613 (2019-2020), Cybercriminalité : un défi à relever aux niveaux national et européen” [Information Report No. 613 (2019-2020), Cybercrime: a challenge to be addressed at a national and European level], filed on July 9, 2020, URL: http://www.senat.fr/rap/r19-613/r19-613_mono.html#toc127

cyberbullying: psychologists, investigators in the Gendarmerie, lawyers, scientists, reception staff at facilities, cybersecurity experts etc.

CHAPTER-VII
SUGGESTIONS AND CONCLUSION
SUGGESTIONS
Unique Characteristics of Cyberbullying

While all bullying is characterized by intentional, often repetitive, hurtful behavior toward another person or group, there are distinguishing elements when it happens online or via smartphone, which include:

- Persistent. Most students have access to some form of technology at all times, which means cyberbullying can happen any time—in the morning, afternoon, and evening—not just while children are at school. It happens while at home or in the community.
- Hard to detect. While some bullying is very overt, such as pushing or damaging belongings, cyberbullying happens through phones and on computers or tablets, making it much more difficult for adults to detect.
- Anonymous. Cyberbullying can be done anonymously. Those being bullied might not even know who is perpetuating the behavior, which makes it easy for one child to hurt another and not be held accountable.
- Shared to a potentially larger audience. Information online can be easily and quickly shared, which makes it difficult to contain or stop negative messages once they are posted online.
- Easier to be hurtful. It is often easier to bully using technology because of greater physical distance The person bullying doesn't see the immediate response from the person being targeted They might not recognize the serious harm caused by their actions because technology distances them from the real-life pain they could be causing.
- Permanent.* Once something is shared on the internet, it is often available to everyone, everywhere It can be challenging to completely delete information once it is on the internet.

CONCLUSION

Teenagers are facing the problem of cyberbullying at a high rate. The cases are increasing day by day. They are bullied online as a result of which their growth gets affected. There are no strict laws that punish bullies. Being an emerging centre of Information Technology, the problems related to technology are also increasing and cyberbullying is one of the problems. Lawmakers must pay attention to it. Awareness programs must be organised so that parents and teachers can easily identify this problem in their children. They must support the victim and help them to recover from it and live a healthy life.

Remember, it can be a very small step to go from what is intended to be a harmless joke to a full-blown cyberbullying campaign. The lack of face-to-face interaction and the feeling of power one gains from sitting behind a computer screen can turn what might normally be a traditional case of schoolyard teasing into a steady onslaught of harassment, shaming, and threats of bodily harm. The impact can leave lasting emotional harm and, as mentioned above, lead to suicide.

If you suspect your child is a victim of cyberbullying, don't wait until it's too late. Don't be afraid to broach the subject with your child for fear that they will repel your attempt to help. Cyberbullying affects all types of children, in all facets of society. Campaigns, legislation, school administrative

programs, and other movements to recognize and stop cyberbullying are a good first step toward tackling this problem. But only you, as a parent, can directly offer advice and assistance immediately.

CHAPTER-VIII
BIBILOGRAPHY

1. Bauman, S., & Cross, D. (2019). Cyberbullying and online harassment in legal perspective: An international perspective. Routledge.
2. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (Eds.). (2012). Cyberbullying: Bullying in the digital age. John Wiley & Sons.
3. Hinduja, S., & Patchin, J. W. (2015). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Corwin Press.
4. Belsey, B. (2013). Cyberbullying: What counselors need to know. Counseling Today, 55(8), 20-25.
5. Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. Developmental Psychology, 43(3), 564-575.
6. Patchin, J. W., & Hinduja, S. (2011). Traditional and nontraditional bullying among youth: A test of general strain theory. Youth & Society, 43(2), 727-751.
7. Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26-32.
8. Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. Journal of Adolescence, 27(3), 319-336.
9. Navarro, R., Yubero, S., & Larrañaga, E. (2015). Cyberbullying across the globe: Gender, family, and mental health. Springer International Publishing.
10. Wong-Lo, M., & Bullock, L. M. (2017). Legal implications of cyberbullying. In Bullying, Prejudice and School Performance (pp. 247-261). Springer, Cham.
11. Smith, P. K., & Slonje, R. (2013). Cyberbullying: The nature and extent of a new kind of bullying, in Cyberbullying through the new media: Findings from an international network. Psychology Press.
12. Diamanduros, T., Downs, E., & Jenkins, S. J. (2008). The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. Psychology in the Schools, 45(8), 693-704.
13. Agatston, P. W., Kowalski, R., & Limber, S. P. (2007). Students' perspectives on cyber bullying. Journal of Adolescent Health, 41(6), S59-S60.
14. Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206-221.
15. Didden, R., Scholte, R., Korzilius, H., de Moor, J., Vermeulen, A., O'Reilly, M., & Lang, R. (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. Developmental Neurorehabilitation, 12(3), 146-151.
16. Langos, C. (2012). Cyberbullying: The challenge to define. Cyberspace Law and Policy Centre.
17. Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), 265-277.
18. Belsey, B. (2012). Cyberbullying: An emerging threat to the “always on” generation. In The media and the adolescent (pp. 193-205). Springer, Dordrecht.

19. Brown, B. B., & Kellner, C. D. (2011). Cyberbullying and suicide: A review of the legal challenges posed by kids killing kids in cyberspace. Psychology, Public Policy, and Law, 17(4), 321-352.
20. Navarro, R., Serna, C., Martínez, V., Ruiz-Oliva, R., & Jiménez, T. I. (2013). The role of Internet use and parental mediation on cyberbullying victimization among Spanish children from rural public schools. European Journal of Psychology of Education, 28(3), 725-745.