

ICTs as a Means to Incite Bullying, Hatred and Crime

Patricia Rodríguez¹, Gabriel Mendoza¹ and Blanca A. Valenzuela¹

¹ Universidad de Sonora, Blvd. Luis Encinas y Rosales S/N, Col. Centro Hermosillo, Sonora, México

Abstract

This research focuses on the existing possibility for users to engage in the inappropriate use of Information and Communication Technologies (ICT) and aims to understand why individuals resort to acts of harassment, hate, and crime, affecting others in the position of victims. Objective: To study the use of ICT as a means to provoke harassment, hate, and crime. Method: The methodology employed a mixed approach, combining descriptive and non-experimental design. The sample consisted of seven (7) authors for qualitative analysis, examining legal contributions to preventing cybercrime. Additionally, 45 young individuals aged 18 to 25 were analyzed for the quantitative study to demonstrate the prevalence of these incidents in this age range. Triangulation was consistently applied for discussion, aiming to establish a more specific understanding of the reality surrounding harassment, hate, and crime on the web. Results: It was revealed that approximately 60% of the respondents experienced harassment to varying degrees, with 58% falling victim to it. An 82% did not experience threats, and 63% did not feel a negative impact on their mental health due to these online experiences. This indicates a high incidence of online harassment and victimization, especially among young people, along with a significant underreporting of these situations and an impact on mental health in some cases. Conclusion: While freedom of expression is a fundamental right supported by various international legal systems, it is crucial that its exercise be balanced with legal responsibilities to prevent online hate speech and incitement to violence. This balance is necessary to curb the ease with which these crimes occur, ultimately impacting others.

Keywords

ICT's, Cybercrime, Harassment, Hate, Crime

1. Introduction

In recent years, the technology revolution that began in the late 1960s and the proliferation of the Internet since the late 1990s have marked a significant shift that continues to evolve [1]. Consequently, there has been a noticeable increase in the use of social networks, email, the Internet, and, in general, Information and Communication Technologies (ICT), to the extent that they have become indispensable in everyday life. This growth has been further intensified due to the increased use of ICT during the COVID-19 pandemic, leading to a rise in the number of cyberbullying cases and online scams, among other issues [2].

It is important to emphasize that young people are always connected and actively participate in the online world, using devices to carry out their activities in the digital sphere routinely [1]. In this regard, the everyday use of technological devices can lead to excessive trust in them and a neglect of necessary security procedures, resulting in serious problems due to improper usage [3]. The use of computer systems with the purpose of provoking, facilitating, or threatening violence towards individuals, resulting in physical, sexual, psychological, or economic harm or suffering, may involve the exploitation of a person's situation, characteristics, or vulnerabilities. [4]. This phenomenon is known as cyberbullying, where the term "cyber" focuses on the cybernetic aspect, and "bullying" has Dutch origins from "boel," which translates to "lover" but carries negative connotations as it was used towards pimps. In this interpretation, the emphasis


CISETC 2023: International Congress on Education and Technology in Sciences 2023, December 04–06, 2023, Zacatecas, Mexico

✉ patricia.rodriguez@unison.mx (P. Rodríguez Ll.); gabriel.mendoza@unison.mx (G. Mendoza M.); blanca.valenzuela@unison.mx (B. A. Valenzuela)

ORCID 0000-0001-8123-4957 (P. Rodríguez Ll.); 0009-0007-7176-1594 (G. Mendoza M.); 0000-0003-0960-9499 (B. A. Valenzuela)



© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

is on the abuse of power component, as it implies an imbalanced relationship from which the victim cannot free themselves independently [5].

Building on these considerations, the study addresses various dimensions of hate speech, including the means of dissemination, the topic, geographical location, the novelty of the phenomenon, and its evolution, generating quantitative data for each aspect. Additionally, these variables are analyzed multidisciplinarily to comprehend hate violence as the outcome of incidents and crimes that have harmful effects, both short and long term, on the physical and mental health of the victims [1]. Indeed, the use of these platforms has evolved to such an extent that individuals or groups within their communities seek to denigrate, belittle, and harass others based on their preferences, nationalities, situations, or physical characteristics that some consider grounds for degradation and mockery. The influence and pressure exerted by these platforms are so significant that ordinary people have made the decision to take their own lives due to mistreatment, insults, threats, and hatred expressed through various comments involving them, adversely affecting their mental health [6].

1.1. Information and Communication Technologies

The creation and use of Information and Communication Technologies (ICT) have experienced rapid and significant growth, playing a fundamental role in virtually every aspect of today's society. From education to entertainment, social relationships, and the workplace, they are deeply integrated into all these areas, defining contemporary reality in a cross-cutting manner [7]. For several years now, the use of ICT has been progressively increasing, being used daily by millions of people as a complement to their daily functions. While these technologies have represented a significant advancement for society, criminal networks, offenders, and even harassers have also used them to commit crimes, implying that anyone has the freedom to use them without restrictions [2].

According to a study conducted in Spain for the year 2018, WhatsApp (85%), Facebook (83%), YouTube (63%), and Instagram (44%) were the most frequently used platforms by users in their daily lives, surpassing Twitter. These users are typically young (16-30 years old), more often female than male, and belong to Generation Z, dedicating an average of 58 minutes daily to their use [8]. Without intending to stigmatize ICT, as they offer numerous beneficial possibilities for humanity, it is important to highlight that the increase in cybercrimes, such as fraud, identity theft, and online harassment, along with the growing exposure of the population to these risks, are undeniable facts [7]. The use of ICTs has transformed the way people relate and communicate, allowing information to flow instantly, which can have a significant impact on the dissemination of social issues. They have also provided people with a platform to express their opinions and mobilize around important causes, leading to the creation of powerful social movements and campaigns. However, it is important to note that, despite their potential for positive social change, they can also be used negatively to spread misinformation or incite violence.

1.2. ICT Harassment

Cyberbullying, also known as cyberbullying, represents a contemporary form of peer aggression that utilizes ICTs. In this form, harm is inflicted through digital means and can be perpetrated by a group of people or an individual, while the victim is in a vulnerable position and struggles to protect themselves [3]. One of the most common types of cyber violence is online harassment, involving a constant and repetitive series of actions or "continuous harassment" directed towards a single person with the intention of causing significant emotional distress and, at times, even fear of physical harm. In colloquial terms, cyberbullying is often related to or described as "revenge porn" or "sextortion" [4].

In summary, bullying or school harassment through the use of ICTs is known as cyberbullying, which is a behavior aimed at causing harm and is repeated continuously, occurring in the context of an interpersonal relationship where there is a clear power disparity, adding to this violence through aggressive behaviors towards victims using communication technology devices [1].

Ultimately, sexual harassment on digital platforms encompasses not only lascivious or desired behaviors towards the victim but also involves public defamation through insults, threats, or offensive messages with the intention of damaging the image or moral integrity of the affected person [9]. Among the types of harassment are the following:

1.2.1. Cyberstalking

Also known as online harassment, it refers to the act of using technology, especially the Internet, to harass someone over time through psychological aggression. This behavior, although more common among adults, can be carried out by one or several people. Typical actions involved in cyberstalking include making false accusations, tracking, threats, identity theft, and manipulation or destruction of data, among others [8].

1.2.2. Sextortion

Also known as revenge porn, it is the online dissemination of content with the purpose of exposing, ridiculing, or damaging someone's dignity, usually after a romantic breakup or other motives, without the consent of the person involved. This may include erotic or sexual images, audios, or recordings of a sexual or pornographic nature of a person, even when those images have been obtained with the victim's consent in a private context [11].

1.2.3. Hatred through ICT

The impact of hate-based violence is significant, as it can lead to both physical and psychological effects, alter people's behavior, and even influence the dynamics of the victim's group and the community at large to which they belong. It is worth noting that young people perceive hate speech as an integrated facet in the dynamics of online communication and social media. Although they admit that they do not identify it with the same frequency in the physical environment, they recognize the interconnection between both worlds, understanding that both dimensions mutually influence each other. [1]. Among the types of hatred, these are:

1.2.4. Electronic insults

The use of offensive or derogatory language by a user on social media or other platforms towards another person.

1.2.5. Harassment

Repeatedly sending offensive or harassing messages to a person, either through any type of online messaging.

1.2.6. Denigration

Spreading false or derogatory information about someone, such as the manipulation and publication of edited photos.

1.2.7. Impersonation

The harasser pretends to be the victim or uses third parties to send aggressive or offensive messages on behalf of the victim.

1.2.8. Coaxing

Disclosure of the victim's private information, obtained confidentially or through persuasion, and its subsequent dissemination without the victim's consent.

1.2.9. Exclusion

Deliberately excluding or preventing someone's participation in an online group or community.

1.2.10. Cyberstalking

Repeatedly sending threatening and harassing electronic communications with the aim of stalking someone.

1.2.11. HappySlapping

Recording physical assaults that are later published online for public dissemination.

1.3. Crime through ICT

These types of cyber-violence actions, ranging from unauthorized intrusion into personal data to the deletion of critical information and deliberate obstruction of access to computer systems or data, have the potential to constitute serious crimes in the digital context. This underscores the need for robust legislation and effective security measures to address this growing problem [4]. Among the most common crimes, are identity theft, computer fraud, computer sabotage, computer espionage, unauthorized access to information systems, and fraudulent appropriation through electronic means [10] these crimes arise from racism, gender violence, and homophobia, among others [3]. It should be added that all these cybercrimes, can be caused by copyright infringement, computer fraud, child pornography, hate crimes, network security violations, and seizure of computer data. In this way, the following are presented in Table 1:

Table 1
Male and Female Victimization [2]

Victimizations in Minors	M	F	M	F	M	F	M	F
	2021		2020		2019		2018	
Sexual abuse	3	12	4	6	0	7	2	8
Illegal computer access	0	3	1	6	0	2	1	2
Sexual harassment	2	1	0	1	1	1	0	1
Online threats	23	27	17	24	11	25	10	30
Cyber attacks	0	0	1	0	0	0	0	0
Coercion	3	9	3	4	1	6	3	7
Crime of contacting a minor under 16 through technology for sexual purposes (grooming)	2	16	4	15	7	8	4	12
Discovery/revelation of secrets	1	8	2	5	4	8	0	5
Defamation	1	1	1	0	0	2	1	5
Child pornography	2	3	1	3	2	6	2	2
Sexual provocation	1	2	1	1	4	1	0	4
Sexual abuse	3	12	4	6	0	7	2	8

According to the data from Table 1, victimizations in minors related to crimes involving the use of technology and communications are outlined by gender and years. There is an overall decrease in sexual abuse, illegal computer access, and sexual harassment over the years, although

men seem to be more involved in these crimes. Online threats are a constant concern, with fluctuating figures affecting both genders. Grooming shows a downward trend, while defamation increases, mainly among women. Additionally, cases of child pornography vary. Overall, these data emphasize the importance of addressing online crimes and promoting education and awareness to protect minors in the digital environment.

1.1. Legal considerations for cybercrime

It is a phenomenon that manifests to directly and indirectly incite violence perpetrated by one individual against another, disregarding what the Constitution establishes. This affects a person's reputation, respect, perception of their moral and physical qualities, dignity, and their good name through acts that defame, discredit, distort, and tarnish the image of a citizen, using the power of the internet and social media to carry out this type of violence discreetly and directly against the victims [11]. Currently, there is no legal framework that establishes clear guidelines on how to identify the problem, what actions to take, and how to sensitize people to prevent such behaviors. The responsibility for addressing these issues lies with the autonomous communities, which must develop the corresponding legislation and establish protocols to address these situations [3].

2. Methodology

This concept does not simply involve merging and diluting the distinctive characteristics of each approach but recognizing that its essence lies in fully leveraging the advantages and strengths of each one separately. In mixed research (quantitative and qualitative), both play significant and complementary roles, with neither one predominating over the other. Instead, they collaborate together to achieve a more complete and holistic understanding of the studied reality [13]. Indeed, to learn more about the use of ICT in the midst of harassment, hatred, and crime, conducting a mixed analysis is more congruent for the study, delving into both perspectives, which could ensure a comprehensive analysis of the context.

Continuously, the descriptive method is defined as one that can provide a certain predictive capacity for future events. However, this prediction requires a solid theoretical foundation and previous evidence that provides a clear understanding of what might happen [14]. Thus, a description of the events caused by cybercrime and cyberbullying is carried out, emphasizing the legal and mental health aspects that this generates. In the third place, the study is non-experimental as no specific scenario or condition is created; instead, existing situations that have not been deliberately generated by the researcher are observed. In this approach, independent variables have already taken place and are not subject to manipulation, meaning the researcher lacks direct control over them and cannot exert influence since they have already occurred along with their associated consequences [14]. Within this context, situations of harassment, hatred, and crime carried out through ICT were studied, extracting from its situations such as mental health problems and new legal actions.

Regarding the population, it is formed by applying specific selection criteria, where the key distinction between the theoretical population and the study population lies in the fact that, in the latter, the units of analysis meet predefined selection criteria that are relevant to the research. The theoretical population serves to support with scientifically studied facts [16]. Based on this, the study group consists of seven (7) authors who provide significant contributions regarding the events related to ICT, based on their particular research, serving as a reference. Another group consists of 45 randomly selected individuals aged 18 to 25, aiming to determine if this situation is more common than thought.

To collect data and information from the population, a survey is carried out, which is a tool that is carried out through an instrument called a questionnaire, aimed only at people and providing information about their opinions, behaviors or perceptions [14]. A questionnaire with 12 questions was created, addressing important topics such as sample profile classification, harassment, victimization, discrimination, threats, persuasion, coercion, discomfort, and

insecurity online, as well as the dissemination of private information, identity theft, reporting of these situations, and the impact on mental health.

In the current era, research employs a variety of tools to collect data, highlighting the importance of triangulation. The large amount of data sometimes requires the researcher to use a reliable analysis technique. Triangulation plays a fundamental role, especially when considering the ultimate goal of the research being pursued [17]. As ICT covers a wide range of aspects, from online social interaction to the impact on mental health and cybersecurity, it is essential to use multiple data sources and research methods to obtain a comprehensive and accurate understanding. Triangulation allows contrasting and verifying the information collected in different ways, increasing the reliability and validity of the findings. Addressing such a relevant topic in contemporary society, it is crucial to ensure that the results are robust and representative, further reinforcing the relevance of triangulation in research on ICT and its effects on people's lives.

3. Results

The results allow detecting the differences between actions performed and actions that should be performed; identify strengths and weaknesses of processes; promote proposals and make positive changes, and measure the efficiency of processes [14]. Hence, the purpose of this survey was to investigate the events caused by the use of ICT as a means to provoke harassment, hatred, and crime. The obtained results provided a comprehensive view of how these technological resources, when misused, significantly affect individuals in terms of their integrity and mental well-being, compelling global governments to enforce legal changes.

3.1. Quantitative Analysis

In the quantitative section, 13 questions were established for 45 individuals aged 18 to 25. These questions were specifically designed to gather information about their own experiences using ICT in the context of harassment, hatred, and crime. The goal was to understand how frequent these events are and how they impact mental health.

1. Have you experienced any form of online harassment or bullying (cyberbullying) in the last 12 months?

Table 2
Harassment Experience

Responses	Quantity	Percentage
No, I have never experienced online harassment.	27	60%
Yes, once.	9	20%
Yes, a few times.	9	20%
Yes, frequently.	0	0%
Total	45	100%

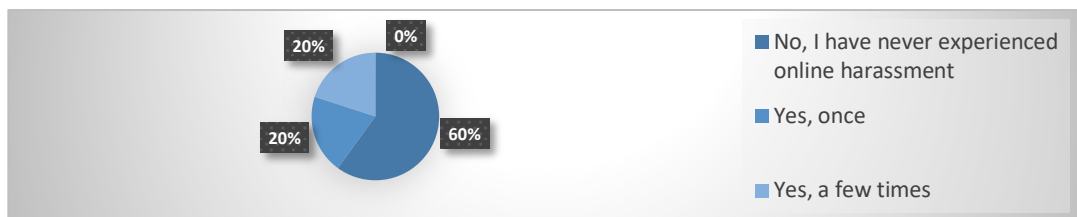


Figure 1: Harassment Experience

It is revealed that 60% of the respondents have experienced some level of online harassment during that period. Of these, 29% reported experiencing it once, while 42% experienced it a few times. Surprisingly, 15% of the participants claimed they had never experienced online harassment in the last 12 months. These results highlight the prevalence of cyberbullying in the sample and the importance of addressing this issue in research on the impact of ICT on online harassment, hatred, and crime.

2. Have you been the target of discrimination or hate comments online due to your gender, sexual orientation, ethnicity, religion, or another characteristic?

Table 3
Discrimination

Responses	Quantity	Percentage
No, I have never experienced online discrimination	27	60%
Yes, on one occasion	10	22%
Yes, on several occasions	8	18%
Yes, on many occasions	0	0%
Total	45	100%



Figure 2: Discrimination

It was found that 40% of the respondents have experienced some form of online discrimination, with 22% reporting having encountered it on one occasion and 18% on multiple occasions. The option for “many occasions” was not selected. These results highlight the presence of online discrimination and underscore the need to address this issue in the context of research on Information and Communication Technologies (ICT) and their relationship with this study.

3. Have you received threats of physical violence or harm through messages or online posts?

Table 4
Threats

Responses	Quantity	Percentage
No, I have never received online threats	37	82%
Yes, on one occasion	7	16%
Yes, on several occasions	1	2%
Yes, on many occasions	0	0%
Total	45	100%



Figure 3: Threats

It was demonstrated that the vast majority, 82%, has not experienced this type of online threats. However, 16% reported having received threats on one occasion, and a small percentage of 2% indicated having received them on multiple occasions. There were no responses indicating having received online threats many times, explaining that while the threat of physical violence or harm online is not a widespread issue among the respondents, there is still a significant number of people who have faced this form of online harassment.

4. Have you witnessed the dissemination of images or private information about yourself or others without consent online?

Table 5
Someone Close

Responses	Quantity	Percentage
No, I have never witnessed this situation	25	56%
Yes, on one occasion	13	29%
Yes, on several occasions	5	11%
Yes, on many occasions	2	4%
Total	45	100%

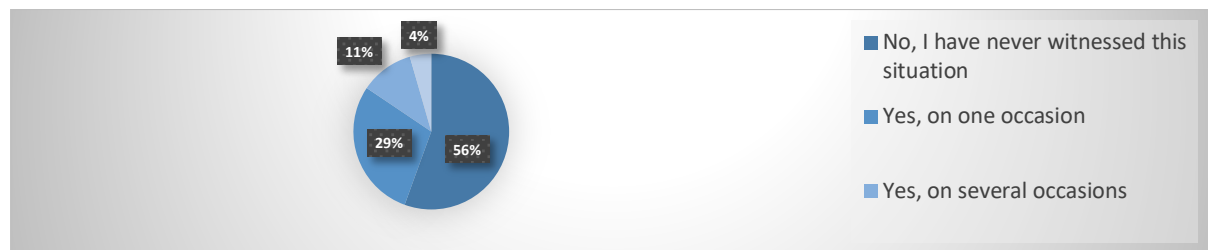


Figure 4: Someone Close

It is shown that approximately 56% of the respondents indicated that they have never witnessed this situation. On the other hand, 29% claimed to have witnessed it on one occasion, while 11% reported seeing it several times, and 4% mentioned observing it many times. These results suggest that the non-consensual dissemination of private information online is a problem that some participants have experienced at different levels of frequency, emphasizing the importance of addressing online privacy protection and preventing this type of behavior.

5. Have you been persuaded or coerced online to do something you did not want to do?

Table 6
Persuasion

Responses	Quantity	Percentage
No, I have never been persuaded or coerced online	34	76%
Yes, on one occasion	10	22%
Yes, on several occasions	1	2%
Yes, on many occasions	0	0%
Total	45	100%

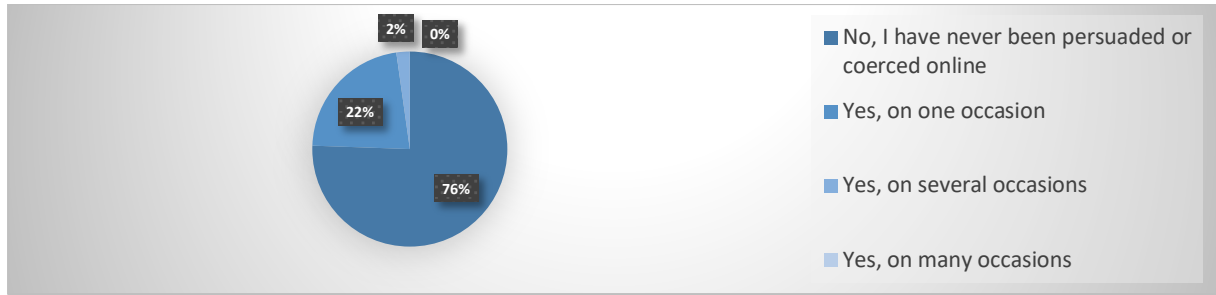


Figure 5: Persuasion

The majority of respondents, at 76%, indicated that they have never experienced this type of online persuasion or coercion. However, 22% mentioned being persuaded on one occasion, and 2% stated that this has happened on multiple occasions. No participant reported experiencing this situation many times. While online persuasion is not a common experience for most respondents, there is still a significant segment of the population that has faced this type of pressure in their online interactions, underscoring the importance of addressing online safety and awareness on various fronts.

6. Have you experienced identity theft online by someone else?

**Table 7
Identity Theft**

Responses	Quantity	Percentage
No, my online identity has never been usurped	38	84%
Yes, on one occasion	5	11%
Yes, on several occasions	2	5%
Yes, on many occasions	0	0%
Total	45	100%



Figure 6: Identity Theft

A significant portion of the respondents, 84%, reported that they have never been victims of online identity theft. However, 11% mentioned that it has happened to them on one occasion, and 5% stated that it has occurred on multiple occasions. It concludes with no participant reporting experiencing online identity theft many times. These results indicate that, although online identity theft is not a common experience for the majority of the respondents, there is still a small percentage of the population that has faced this issue, emphasizing the importance of cybersecurity and education on online identity protection.

7. Do you feel that negative online experiences have had an impact on your emotional and mental well-being?

**Table 8
Mental Health**

Responses	Quantity	Percentage
No, I do not feel a negative impact	19	63%
Yes, on one occasion	12	31%

Yes, on several occasions	13	4%
Yes, on many occasions	1	2%
Total	45	100%

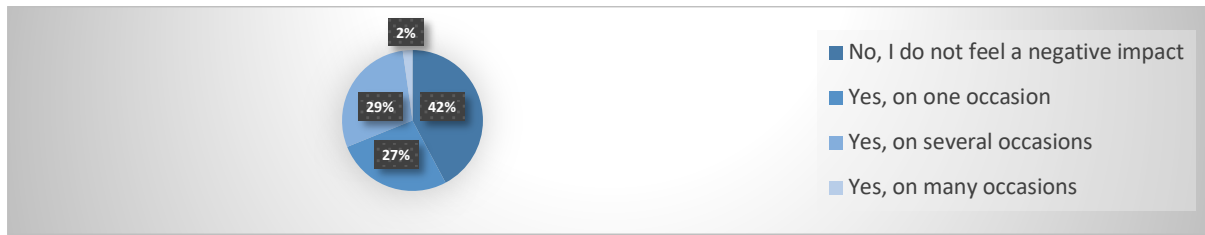


Figure 7: Mental Health

To conclude, the majority of respondents, 63%, do not feel a negative impact on their mental health. However, a significant 31% stated they have experienced an impact on their emotional and mental well-being at least once due to these experiences. Additionally, 4% mentioned feeling this impact multiple times, and a small 2% said they have felt it many times. Indeed, it is important to address the negative consequences that online experiences can have on people's mental health and provide support and resources for those who face them recurrently.

3.1. Qualitative Analysis

To begin this section of the study, the qualitative analysis was conducted in Table 15 by examining seven (7) authors who explored the topic. These authors were randomly selected from Google Scholar based on the current period from 2019 to 2023 to understand their contributions in the legal and criminal context, as they are the ones most researched to control the issues of harassment, hatred, and crimes using ICT.

Table 9
Qualitative Analysis

No.	Author(s) and year	Title	Journal, University, and website
1	Gómez, M., Garcés, F. y Moran, M. (2023)	The crime of technological harassment and Ecuadorian legislation.	IustitiaSocialis, VIII, VIII, (1), 105 – 120
2	Moreno y Arroyo (2022)	The Crime of Technological Harassment and Ecuadorian Legislation.	RLCS, (80), 347 – 363
3	Quezada, et al., (2022)	Networks, Monitoring Systems, and Mobile Applications to Combat Hate Speech and Crimes in Europe.	RISTI, E54, 419 – 435.
4	Carriedo, L. (2022).	Teenagers' Overexposure to Cybercrimes in Ecuador.	Research and Innovation Center in Information and Communication Technologies.
5	Cook (2022)	Computer Crimes in the Face of Human Rights Standards and Freedom of Expression in Mexico.	Comparitech
6	Val, L. (2019)	Data and Statistics on Cyberbullying from 2018 to 2022. Comparitech.	University of Valladolid
7	Aguilar, S. (2021)	Hate Crimes on Social Media.	CEUTEC Technological University Center

In the global context, when analyzing articles and declarations of human rights from various international legal systems, such as the Universal System, the American System, the African System, and the European System, which emphasize the right to freedom of expression and the importance of receiving and disseminating information and ideas without unjustified restrictions, they establish that freedom of expression is a fundamental right that includes the right to seek, receive, and communicate information by any means and without limitation of borders [11]. In historical terms, the concept of “hate crimes” has been a subject of debate and definition in academic circles, without reaching a clear consensus. For some, these crimes are characterized by the presence of prejudices that motivate the offense, while others argue that the victim's belonging to a hated social group defines them. The origin of this concept dates back to 1985 in the United States when numerous crimes based on racial and ethnic prejudices were investigated. The FBI adopted the term due to its media impact and message [6].

To address technological harassment, the United States enacted the State Communications Act, which focuses on punishing those who attempt to extort by threatening to harm someone's reputation or property. This law provides for fines, imprisonment of up to two years, or both penalties. Additionally, there is the Interstate Stalking and Prevention Act, which establishes different levels of penalties based on the severity of the case for anyone using technological means to cause serious emotional distress to another person or to put them in reasonable fear of harm, including death [12]. It is important to note that hatred itself is not a crime, as the protection of civil rights in the country gained significant momentum after the murders of civil rights workers in 1964. The Supreme Court ruling also emphasizes that hate speech cannot be a punishable offense and that legislation varies based on each state's historical experience. Hate crimes are defined as those committed due to race, religion, gender, sexual orientation, gender identity, or perceived or actual disability, and were addressed by the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act [6]. The right to freedom of expression may be subject to certain restrictions, such as the protection of national security, public order, public health, public morals, and the rights and reputation of others, highlighting the need to balance freedom of expression with appropriate legal responsibilities and limitations in a democratic society. It is emphasized that propaganda in favor of war and the advocacy of national, racial, or religious hatred that incites violence or illegal actions against individuals or groups is prohibited [11].

Statistically, according to research published in the Multimedia Systems journal, the majority of cases of cyberbullying in Canada, the United Kingdom, and the United States involve minors. Studies conducted in the United States by the Cyberbullying Research Center revealed that among students aged 12 to 17, 7% have experienced digital harassment, while 30% have been victims of rumors and gossip on social media. Another study by the National Crime Prevention Center found that 43% of young people were victims of this type of online crime. Additionally, the Pew Research Center reported in its records that 59% of the surveyed individuals had experienced cyberbullying [18]. In Spain, statistical data from the report on the evolution of incidents related to hate crimes shows 1,334 incidents related to hate crimes, with 189 of them occurring on the Internet (45%) or social media (23%). This is compounded by an abundance of intolerant comments, popularly dubbed “hate”, against xenophobia and intolerance in digital newspapers [1]. Furthermore, according to [8], Spanish criminal legislation addresses various types of cybercrimes, including:

3.1.1. Threats

Protecting individual freedom and the sense of security, regulated in articles 169 to 171 of the Penal Code, often related to harassment such as cyberbullying.

3.1.2. Coercion

Protecting individual freedom, regulated in articles 172 and 173 of the Penal Code, often related to acts of “stalking” (harassment).

3.1.3. Sexual Abuse

Regulated in articles 181 to 183 BIS of the Penal Code, addressing offenses against sexual freedom or integrity without the need for violence or intimidation, including “grooming” in article 183 ter.

3.1.4. Exhibitionism and Sexual Provocation

Penalizing obscene acts and the sale, dissemination, or exhibition of pornographic material, regulated in articles 185 and 186 of the Penal Code.

3.1.5. Child Pornography

Penalizing the production, sale, distribution, and exhibition of child pornography in articles 187 to 189 of the Penal Code, with legal liability for legal entities.

3.1.6. Disclosure and Revelation of Secrets

Regulated in articles 197 to 201 of the Penal Code, protecting privacy and sanctioning unauthorized access or disclosure of data, electronic documents, or the interception of communications.

3.1.7. Slander and Libel

Articles 205 to 210 of the Penal Code sanction the imputation of false facts constituting a crime and injury to honor, respectively.

3.1.8. Computer Damage

Article 264 of the Penal Code punishes damage to others' computer systems, including unauthorized access.

3.1.9. Identity Theft

Although not an autonomous crime, it can be part of other offenses, such as “stalking” or “child grooming”.

3.1.10. Incitement to Hate and Violence against Groups

Article 510 of the Penal Code sanctions the provocation of hatred, discrimination, or violence against groups based on racist, religious, sexual, among other motives.

In another context, Ecuador's Comprehensive Organic Penal Code (COIP) addresses a National Cybersecurity Policy, emphasizing the awareness of technology companies regarding the issue to provide protection to their users and benefit the national economy [9]. The latest reform of Honduras' Penal Code in 2020 addressed various cybercrimes but did not specifically classify sexual harassment on online platforms. Given the breadth and constant evolution of social media, current legislation has gaps in regulating crimes committed online, underscoring the need for a more comprehensive and adaptable legal framework to address these issues [10].

4. Discussion

The analysis of the data collected in the mixed-method research on Information and Communication Technologies (ICT) as a means to incite harassment, hatred, and crimes reveals

significant findings about individuals' experiences in the digital environment regarding these issues. Despite cyber violence often originating online, its consequences transcend the virtual world, causing harm to both victims and their families. This form of violence poses moral and psychological threats, with individuals experiencing anxiety and depression as a result [4]. The sample profile is characterized by a gender balance, with 47% males and 53% females, ensuring the representativeness of the sample and enabling a comprehensive analysis of how ICT affects individuals of different genders in relation to online harassment, hatred, and crime. In terms of age, the majority of participants are young adults, with 25% at 18 years, 40% at 19 years, and 22% at 20 years. Thirteen percent are 22 years old, and no participants over the age of 22 were recorded in the sample.

These results indicate that the research primarily focuses on young adults, which may be relevant for understanding how ICT impacts this particular demographic concerning the studied issues. Regarding the authors cited in the qualitative section, the information is based on studies from various sources and perspectives providing a broad and detailed insight into the topic, as well as the legal and social responses implemented in different contexts. Firstly, it is noteworthy that 60% of the participants reported experiencing some level of online harassment during the studied period, indicating the prevalence of cyberbullying in the sample and emphasizing the importance of addressing this issue. Within this group, 29% mentioned experiencing it once, while 42% claimed to have experienced it multiple times. Furthermore, 58% of respondents indicated experiencing some level of online victimization, demonstrating that almost six out of every ten have been subjected to offensive or hostile online comments at some point. Of these, 24% reported experiencing it on one occasion, while 27% experienced it multiple times.

Regarding online discrimination, 40% stated having experienced some form of discrimination, indicating they have faced these situations. However, 22% of participants claimed to have experienced it once, and 18% experienced it multiple times. While the percentages are lower than those of harassment and victimization, they still point to the need to address the issue of online discrimination. On the other hand, a concerning aspect is that 16% claimed to have received online threats on at least one occasion. Although not a widespread issue among participants, this result underscores that a significant number of individuals have faced online threats, highlighting the importance of addressing cybersecurity and preventing such behavior. Regarding online identity theft, 84% reported never having experienced this type of issue, while 11% mentioned it occurring on one occasion. This indicates that a small percentage of the population has faced this problem, emphasizing the importance of cybersecurity and education on protecting online identity. These findings underscore the need to address and promote online security, manage online interactions, and prevent negative behaviors in the digital environment.

On a global scale, there is universal recognition of the right to freedom of expression as a fundamental principle. However, this right is not absolute and may be subject to certain legal restrictions, such as protecting national security, public order, public health, and the rights and reputation of others. This balancing act of freedom of expression with other responsibilities and legal limitations is crucial in a democratic society. It is important to note that incitement to national, racial, or religious hatred that incites violence or illegal actions against individuals or groups is prohibited in many international legal systems, reinforcing the need to effectively address online hate speech. Furthermore, statistics on online harassment show that this problem is prevalent in various countries, especially among young people. In the United States, for example, digital harassment affects a significant proportion of students aged 12 to 17, with 7% experiencing digital harassment and 30% falling victim to rumors and gossip on social media. Additionally, the Pew Research Center reports that 59% of surveyed individuals have experienced cyberbullying. In Canada, the United Kingdom, and the United States, most cases of cyberbullying involve minors. These statistics highlight the importance of addressing online harassment as a serious issue that particularly affects the youth.

In the same vein, the United States has enacted specific laws to address online harassment and hate crimes, such as the State Communications Act and the Interstate Stalking and Prevention Act, imposing significant penalties on those engaging in criminal online behaviors, such as extortion and threats of emotional or physical harm. This signifies that hate speech itself is not a crime, and

legislation varies based on each state's historical experience. The Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act is a significant example of legislation protecting individuals against prejudice-based violence and harassment. In Spain, progress has been made in legislation and prevention of online hate crimes. The report on the evolution of incidents related to hate crimes shows a significant number of incidents related to online hate crimes and social media. The legislation addresses a variety of cybercrime-related offenses, such as threats, coercion, sexual abuse, exhibitionism, child pornography, disclosure of secrets, defamation, and computer damage, among others. This legislation is essential for addressing various forms of online crimes and protecting the rights and security of individuals, serving as an example that can be expanded globally.

In summary, information collected from different sources and contexts highlights the importance of addressing online harassment, hate, and crimes from legal, social, and educational perspectives. Fundamental rights, such as freedom of expression, must be balanced with appropriate legal restrictions to prevent incitement to hatred and violence. Statistics show that online harassment is a widespread problem, especially among young people, underscoring the urgency of taking measures to protect online users. Legislation and national cybersecurity policies are crucial tools for addressing these challenges and promoting a safer and more respectful online environment.

5. Conclusions

In general, it is essential to promote open communication with minors to identify possible cases of cyberbullying early on. Instead of downplaying or exaggerating the situation, it is crucial to approach it with support. Blaming the Internet is not the solution; rather, the focus should be on listening and providing an appropriate response that does not expose the victim further or increase their humiliation. Encouraging conversations about the issue with friends, avoiding keeping it a secret, and not responding to online provocations while preserving evidence in case of harassment are highly recommended practices [8]. Efforts to change hate speech through ICT span several dimensions, where legal actions complement social and educational approaches. This requires commitment to ensure this change. Together, these efforts aim to promote democratic values and create a safer and more respectful online environment for all, discouraging the spread of hate messages facilitated by the anonymity offered by online media [1].

Regarding these considerations, the triangulation of data and information through different research methods, such as surveys and theoretical analyses, provides a more comprehensive understanding of issues related to ICT and online harassment. In this context, survey results show that online harassment and victimization are common challenges, emphasizing the need to address online security and promote greater awareness. While most respondents have not reported instances of online harassment, it is essential to encourage reporting and provide support to those facing these issues. Despite freedom of expression being a fundamental right supported by various international legal systems, its exercise must be balanced with legal responsibilities to prevent online hate speech and incitement to violence. Hate crimes, though subject to debate in terms of definition, have a significant impact on victims and require appropriate preventive and punitive measures.

The pioneering legislations of the United States and Spain, addressing a variety of technology-related crimes from digital harassment to child pornography, underscore the need for specific regulations in the digital environment. Additionally, the impact on individuals' mental health due to negative online experiences is a relevant aspect that deserves attention and resources for psychological support. Moreover, it serves as certified evidence when prosecuting those who have harmed the affected person. Finally, online identity theft is less common but remains a significant concern in terms of cybersecurity and protection of online identity. Overall, this study highlights the complexity of issues related to ICT, online harassment, and hate speech, emphasizing the need for a multifaceted approach involving society, online platforms, and legislation to effectively address these challenges.

References

- [1] Moreno, R., & Morelo, S. (2022). Communication on Networks and Hate Speech in the Spanish Context. *International Visual Culture Review*, 2–9. doi: <https://n9.cl/3ozk8m>
- [2] Ros, N. (2022). Analysis and Evaluation of the Impact of Crime Using ICTs, in Especially Vulnerable Collectives. (Undergraduate Thesis). Higher Polytechnic School. University of Alicante. doi: <https://n9.cl/tck8f>
- [3] Navarro, T. (2019). Risks Among Adolescents due to the Misuse of ICTs: Cyberbullying. (Undergraduate Thesis). University of Zaragoza. doi: <https://n9.cl/i2wlg>
- [4] Febro, J. & Tinam, M. (2022). Exploring Cyber Violence against Women and Girls in the Philippines through Mining Online News. *Scientific Journal of Educommunication, Comunicar*, 70, (XXX), 125–138. doi: <https://n9.cl/neiqlz>
- [5] Torres, M. (2021). Cyberbullying from the Perspective of Extracontractual Civil Liability. (Undergraduate Thesis). Miguel Hernández University of Elche. doi: <https://n9.cl/h1g90>
- [6] Val, L. (2019). Los delitos de odio en las redes sociales. (Undergraduate Thesis). University of Villadollid. doi: <https://n9.cl/s32y5>
- [7] Hernández, M., & Pina, M. (2020). Hate Messages on the Internet. V International Virtual Congress on Education in the 21st Century. [March 2020]. doi: <https://n9.cl/a7p5r>
- [8] Vadillo, L. (2019). Harassment of minors and young people through social networks. (Undergraduate Thesis). Miguel Hernández De Elche University. doi: <https://n9.cl/t1xzyh>
- [9] Quezada, P., Suárez, E., Coloma, A., Ruiz, R., Pinos, B., Espinoza, E., Arrobo, C. & Martínez, C. (2022). Overexposure of Adolescents to Cybercrimes in Ecuador. *RISTI*, E54, 419–435. doi: <https://n9.cl/hje2b>
- [10] Aguilar, S. (2021). Cybersexual Harassment through Online Platforms in Honduras, the Crime of the 21st Century. (Undergraduate Thesis). Centro Universitario Tecnológico CEUTEC. doi: <https://n9.cl/jos21>
- [11] Carriedo, L. (2022). Computer Crimes in the Face of Human Rights Standards and Freedom of Expression in Mexico. (Undergraduate Thesis). Center for Research and Innovation in Information and Communication Technologies. doi: <https://n9.cl/7vr84>
- [12] Gómez, M., Garcés, F., & Moran, M. (2023). Technological Harassment and Ecuadorian Legislation. *IustitiaSocialis*, VIII, VIII, (1), 105–120. doi: <https://n9.cl/3bz8l>
- [13] Salas, D. (2019). The Mixed Research Approach: Some Characteristics. [June 4, 2019]. doi: <https://n9.cl/hd2v>
- [14] Arias, J. (2021). Design and Methodology of Research. First Edition. Peru: Enfoques Consulting EIRL. doi: <https://n9.cl/vbqz4>
- [15] Valle, W. (2022). Non-experimental research designs. *Experimental Psychology*. Catholic University the Angeles of Chimbote. doi: <https://n9.cl/y7ilm>
- [16] Mucha, L., Chamorro, R., Oseda, M. y Alania, R. (2020). Evaluation of procedures used to determine the population and sample in postgraduate research work. *Scientific Journal of Social Sciences and Humanities, Challenges*, 12, (1); 44-51. doi: <https://n9.cl/6kr95>
- [17] Jiménez, V., & García, M. (2021). Methodological Triangulation in Research. *United Scientific Journal*, 5, (2), 70–73. doi: <https://n9.cl/76lm8s>
- [18] Cook, S. (2022). Data and Statistics on Cyberbullying from 2018 to 2022. *Comparitech*. [December 9, 2022]. doi: <https://n9.cl/o5eep>