ISSN: 2182-2069 / E-ISSN: 2182-2077

Influence of Social Media and Artificial Intelligence on Cyberbullying for Decision-Making with Legal or Judicial Foundations in Ecuador

Dr. Diego Gustavo Andrade Armas[1], Segundo Moisés Toapanta Toapanta[2*], Eriannys Zharayth Gómez Díaz[3], Dr. Janio Lincon Jadán Guerrero[4], Rocío Maciel Arellano[5], and María Mercedes Baño Hifóng[6]

[1]Centro de Estudios De Seguridad (CESEG), Universidad De Santiago De Compostela (USC), Santiago, España. diegoandradea@hotmail.com, https://orcid.org/0000-0002-1782-8248

[2*]Centro de Investigación En Mecatrónica y Sistemas Interactivos (MIST), Ingeniería En Tecnologías De La Información, Universidad Tecnológica Indoamérica, Quito, Ecuador. moisestoapanta@uti.edu.ec, https://orcid.org/0000-0002-9041-0518

[3]Research Department, Gestión De Tecnologías Para El Mundo (GTM), Quito, Ecuador. zharaythgomez2709@gmail.com, https://orcid.org/0000-0002-6792-6938

[4]Centro De Investigación en Mecatrónica y Sistemas Interactivos (MIST), Maestría en Educación, mención en Pedagogía en Entornos Digitales (MEPED), Universidad Tecnológica Indoamérica, Quito, Ecuador, janiojadan@uti.edu.ec, https://orcid.org/0000-0002-3616-2074

[5]Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México. ma.maciel@academicos.udg.mx, https://orcid.org/0000-0002-5548-2073

[6]Postgraduate Subsystems, Universidad Católica De Santiago De Guayaquil (UCSG), Guayaquil, Ecuador. maria.bano@cu.ucsg.edu.ec, https://orcid.org/0000-0003-2904-3090

Received: November 05, 2024; Revised: December 10, 2024; Accepted: January 06, 2025; Published: February 28, 2025

Abstract

Cyberbullying remains a pervasive issue globally and in Ecuador, fueled by the rapid evolution of the Internet, emerging trends in information and communication technologies (ICT), artificial intelligence (AI), and social networks. One of the primary contributing factors is the influence of social networks and AI, coupled with the absence of robust legal and judicial frameworks. The objective of this study is to propose a conceptual model for cybersecurity management in social networks. A deductive approach and exploratory research methods were used to analyze information from various official sources. The results include a mental map that identifies key stakeholders, a simulation designed to mitigate cyberbullying on social networks, and a conceptual model to address cyberbullying management. The study concludes that mitigating cyberbullying requires the implementation of appropriate AI tools and the development or improvement of cyberbullying laws in each country. Simulations demonstrated that in one scenario, the occurrence of cyberbullying could be reduced to an average of 25%, highlighting both the challenges and the potential of leveraging AI and updated legislation to combat this issue effectively.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 32-50. DOI: *10.58346/JISIS.2025.I1.003*

*Corresponding author: Centro de Investigación En Mecatrónica y Sistemas Interactivos (MIST), Ingeniería En Tecnologías De La Información, Universidad Tecnológica Indoamérica, Quito, Ecuador.

Keywords: Cyberbullying, Social Media, Artificial intelligence, Legal Proceedings, Judicial Proceedings.

1 Introduction

Cyberbullying is a critical global issue. However, in Ecuador and many other countries, it has yet to receive the necessary attention to effectively mitigate this form of cybercrime. The problem persists across all levels of society, including higher education institutions and both public and private sectors, affecting individuals regardless of age, gender, or social background (Deihim et al., 2014). A major contributing factor is the influence of social media, artificial intelligence, the borderless nature of the internet, the evolution of information and communication technologies, and the lack of adequate legal and judicial frameworks to address cyberbullying. In Ecuador, there is no specific law dedicated to cyberbullying within the Comprehensive Organic Criminal Code.

Cyberbullying is particularly harmful to education, especially affecting children and adolescents. It is one of the 20 critical issues identified by the United Nations (UN) that need to be addressed this century. Countries with the highest rates of cyberbullying include Spain, Argentina, Brazil, the USA, and Mexico, which have the highest rates per 100,000 inhabitants. According to Bullying Without Borders, in collaboration with the World Health Organization (WHO) and the Organization for Economic Cooperation and Development (OECD), more than 9,524,000 cases of cyberbullying were detected between 2023 and 2024. Cyberbullying predominantly occurs on social media platforms such as Facebook, Twitter, Instagram, and WhatsApp. Notably, 70% of victims are girls (women), compared to boys (men), and 58% of cases occur via mobile phones, primarily using WhatsApp (Yesmin & Abdul Karim, 2020). According to a May 2024 report from these organizations, Spain leads globally in cyberbullying cases with 2,050,000 incidents, followed by Mexico with 1,950,000 cases, the USA with 1,900,000 cases, Argentina with 1,850,000 cases, Italy with 1,750,000 cases, and Japan with 1,650,000 cases. These incidents affect individuals across various age groups, including adults, teenagers, and children. This data was gathered with the support of students and professors from various prestigious universities, including Harvard University, Yale University, Massachusetts Institute of Technology (MIT), University of California, Los Angeles (UCLA), University of Toronto, Princeton University, University of Chicago, University of Florida, University of Melbourne, Utrecht University, University of Tokyo, University of Buenos Aires (UBA), University of Amsterdam, University of Copenhagen, University of São Paulo, University of Zurich, University of Bologna, Complutense University, University of Barcelona, University of Hamburg, University of Lyon, Catholic University of Chile, and National Autonomous University of Mexico (Planeta, 2024). The document titled "Convention 190 of the International Labour Organization (ILO) and its Importance in the Preventive Management of Digital Violence and Cyberbullying at Work" highlights that with the advancement of information and communication technologies (ICT), the widespread use of social media, and the rise of teleworking, cyberbullying has become more prevalent, contributing to a growing mental health issue. Efforts are currently underway to identify alternatives for mitigating this cybercrime through initiatives such as training programs, the development of laws tailored to each country's context, and other proactive measures (De Vicente Pachés, 2020; Abdullah, 2024). The Constitution of the Republic of Ecuador, according to Official Register 449 of October 20, 2008, with the latest amendment on January 25, 2021, does not specify a clear law to sanction cyberbullying (Martínez et al., 2021). The Comprehensive Organic Criminal Code (COIP), published in Official Registry Supplement 180 on February 10, 2014, with the latest modification on February 17, 2024, does not include any article that directly addresses cyberbullying (Coip, 2024). The Personal Data

Protection Law, published on May 26, 2021, under letter No. T. 680-SGJ-21-0263, does not specifically include any articles related to the protection of personal data to prevent cyberbullying (Ministerio de Telecomunicaciones y de la Sociedad de la Información - MINTEL, 2021). According to the General Regulations of the Organic Law on the Protection of Personal Data, issued by Executive Decree 9041 on November 6, 2023, none of its articles specifically address cyberbullying (Ley Organica de Proteccion de Datos Personales, 2021). The Labor Code of Ecuador, as published in Official Registry Supplement No. 167 on December 16, 2005, with the most recent reform in Official Registry Supplement 242 on February 1, 2023, addresses workplace harassment in Article 42, literal 36. However, it does not directly mention cyberbullying (Orgánica, 2023). At this stage, it is crucial to analyze and determine whether workplace harassment and cyberbullying violate the constitutional rights and guarantees of workers, as Ecuadorian legislation does not specifically address these types of crimes. This lack of legal provisions is one of the reasons why workplace harassment and cyberbullying continue to rise, leaving the responsibility for addressing the issue in the hands of employers, which does not always result in the most effective solutions (Moncayo Valdez & Maldonado Ruiz, 2023). During the COVID-19 pandemic, which became widespread in Ecuador in 2020, cyberbullying significantly increased in educational institutions at all levels, as well as in public and private companies, due to the rise of online classes and teleworking. However, there was no legal or judicial framework in place to effectively mitigate cyberbullying (Toapanta Toapanta et al., 2020). Technological advances and the widespread use of the Internet have brought significant progress in the digital and virtual world, leading to both great advantages and disadvantages. One major downside is the increase in cyberbullying, to which millions of people who use various technological platforms and social networks are exposed (Gaurang et al., 2015). This has raised significant concerns and challenges for the 21st century. Methodological solutions are being proposed to mitigate this form of cybercrime (Nair et al., 2023). To mitigate cyberbullying among children and adults, an appropriate legal framework is essential, which includes the adoption of several laws that declare digital human rights and protect freedom on the Internet and in e-democracy. This would ensure the safeguarding of digital rights in Ukraine (Khomyshyn et al., 2021).

The objective is to develop a conceptual model for managing cybersecurity on social networks.

Why is it necessary to generate a conceptual model for managing cybersecurity on social networks for decision-making in legal or judicial processes? The purpose is to clearly identify the key actors involved in cyberbullying, select appropriate artificial intelligence (AI) tools, and establish cyberbullying laws to mitigate its risks in educational institutions at all levels, as well as in public and private organizations.

The research uses the deductive method and exploratory research to analyze information from reference documents.

The results of this study include: a mental map of relevant actors, a simulation to mitigate cyberbullying on social networks, and a conceptual model for cybersecurity management.

The findings conclude that to mitigate cyberbullying effectively, it is crucial to use appropriate artificial intelligence tools and develop or enhance cyberbullying laws in each country. The simulations demonstrated that, in scenario two, cyberbullying could be reduced to an average of 25%. This represents a significant challenge, which can be addressed through the strategic use of AI tools and the creation or updating of cyberbullying laws in each country.

2 Materials and Methods

2.1. Materials

The materials used in this research include documents and websites from previous studies that proposed solutions related to the influence of cyberbullying, artificial intelligence, and legal or judicial processes.

- **Cyberbullying**

Technological innovation is advancing rapidly, leading to various effects, one of which is the rise of cyberbullying. Cyberbullying is a crime in which an aggressor targets an individual by provoking online hatred. To address this, a method for detecting cyberbullying based on deep neural networks is proposed, which defines an architectural model for its detection (Banerjee et al., 2019). They believe that the advent of the Internet has been a blessing for society; however, it has also brought many challenges, such as cyberbullying, which cannot be entirely avoided. They suggest that cyberbullying can be identified through the analysis of sentiments and emotions in a given scenario. To address this, they propose a multimodal adversarial multitasking framework for detecting cyberbullying, incorporating two auxiliary tasks: sentiment analysis and emotion recognition (Maity et al., 2023). Cyberbullying intentionally causes harm to individuals through social networks and the Internet using technological devices. It is a significant issue identified among university students. The researchers determined that one of the causes is the subjective nature of norms, attitudes, perceived behavioral control, and the use of social networks, all of which have the potential to influence the occurrence of cyberbullying among university students (Abdul Rahman et al., 2023).

- **Social Media**

They explore attempts to detect cyberbullying using machine learning and deep learning technologies. Cyberbullying is one of the first phenomena to emerge as a result of the proliferation of social media platforms. The researchers present a table listing all the platforms used for cyberbullying, along with their respective evaluations (Hussein & Aleqabie, 2023). Children, adolescents, and individuals in general are exposed to cyberbullying. To mitigate this cybercrime, the authors propose the development of an ICT management mode (Toapanta et al., 2020). Social media amplifies cyberbullying, leading to a negative impact on its victims. Detecting cyberbullying has become a significant challenge. To address this, the authors propose the design of a new chatbot aimed at identifying cases of cyberbullying based on user comments. The chatbot provides emotional support or guidance tailored to each situation. Python was the tool used for this development (Sanu et al., 2023). The authors utilized the state-of-the-art BERT model and the PyThaiNLP library, along with a set of labeled comments from the Criminal Court of Thailand, to identify instances of defamation on social media in Thailand (Patthong et al., 2024). Cyberbullying on social media, particularly the psychological impact of online tweets, is a growing concern. The authors propose an advanced methodology to detect cyberbullying posts using machine learning algorithms, specifically three algorithms: Convolutional Neural Network (CNN), Naive Bayes (NB), and Support Vector Machine (SVM). Among these, cyberbullying can be identified more effectively in tweets using the Convolutional Neural Network (CNN) (Swamy et al., 2023). Cyberbullying on the social media platform Twitter incorporate bystander roles into the corpus, to determine a significant impact on annotators' perception and classification of cyberbullying instances. They conduct a detailed analysis

of the annotation process and examine the influence of observers in greater depth (Alfurayj & Lutfi, 2023). The authors aim to examine the factors influencing cyberbullying on social media among college students. Instagram was selected for this study due to its widespread use and popularity among college students. They developed a conceptual model of influencing factors, which offers a comprehensive and holistic understanding of the elements contributing to cyberbullying (Oladimeji & Kyobe, 2021). Cyberbullying via social media in African secondary schools has seen an increase, with adolescents often identifying themselves as either the bully or the victim. This research explored the nature of the victims and the behavior of mobile bully-victims on Facebook. The study examined various factors of mobile cyberbullying, including anonymity, collective behavior, power dynamics, the use of Facebook, emojis, and Facebook features (Ndyave & Kyobe, 2019). Cyberbullying is a significant issue on digital platforms, with bullying and harassment proliferating across social media. To address this, automated detection systems based on machine learning have been developed to mitigate cyberbullying. The authors highlight the importance of multimodal detection methods for identifying cyberbullying on social networks, as well as the challenges involved in creating effective detection systems. They conduct a bibliometric analysis of cyberbullying detection using machine learning, identify various techniques employed for detection, and present a range of applications for multimodal AI (Vora et al., 2023). The authors state that social media is rapidly proliferating and has become a primary platform for committing crimes such as cyberbullying, cybercrime, and cyberterrorism. Given the prevalence of these issues, they emphasize the need for digital forensic investigations and legal procedures on these platforms. To address this, they propose a systematic structuring and categorization of the digital attributes interconnected across social media platforms through digital ontologies. Furthermore, they introduce a method for creating user profiles by utilizing domain-specific digital artifacts. Their work contributes to the advancement of digital forensic investigations and the handling of cybercrimes related to social media platforms (Grigaliunas et al., 2023). The authors propose a parameter model to determine cyberbullying on social networks in Ecuador; the results they obtained are: A conceptual model for the mitigation of cyberbullying, Four-layer architecture, Indicator detection algorithm expressed in a flow chart (Toapanta et al., 2020). Due to the use of social media, cyberbullying has emerged, especially among young people. They propose a multimodal detection approach that integrates data from various sources, including photos, videos, comments, and temporal information from social networks. Additionally, they propose hierarchical attention networks for recording the characteristics of multimedia information (Ahmad Al-Khasawneh et al., 2024).

- **Artificial Intelligence (AI)**

With the accelerated growth of the Internet, social networks and artificial intelligence, great advantages and disadvantages have been generated in human life, one of them being cyberbullying; the authors propose a model that consists of a fusion of two different classifiers: the decision tree classifier and the AdaBoost classifier. The proposed model for identifying cyberbullying demonstrates remarkable skill (Gopalan et al., 2023). They propose the predictive model and consider that the combination of several data sets on cyberbullying allows to create balanced data by applying Bi-LSTM and BERT to improve the performance of the cybercrime prediction model (Gan et al., 2023). They propose to use a set of machine learning methods based on artificial intelligence (AI) to detect bullying behavior. The model also provides the logical reasoning of the extracted evidence. The machine learning model works on a Twitter dataset to suggest the Tweets as bullying or non-bullying category. They use the LIME which is a tool to predict the interpretability of the model (Pawar et al., 2022). Due to the proliferation of fake accounts on various platforms, cybercrime, cyberbullying and

misinformation have been generated. To mitigate these risks, they developed a system for the detection of fake accounts using machine learning techniques. The model using metrics allows to distinguish between real and fake accounts effectively. Administrators will receive alerts of fake accounts for legal and timely compliance (Alekya Rani et al., 2024). Cyberbullying is a major challenge in the development of technologies. In the last ten years, cyberbullying has increased on a large scale, affecting youth, children, adults regardless of age, gender, culture or social position (Donkor & Zhao, 2023). They propose a model to address the problems with the help of artificial intelligence (AI). They consider that machine learning is a subset of artificial intelligence that teaches machines to make appropriate decisions (Kumar et al., 2023). They claim that cyberbullying is a social media problem that affects society. They propose a detailed classification of cyberbullying by integrating neutrosophic logic into the multilayer perceptron (MLP) model. Incorporating neutrosophic logic aims to address uncertainty, ambiguity, and indeterminacy in classification decisions, offering a more comprehensive and flexible approach to handle complex classification scenarios (Ibrahim et al., 2024).

- **Legal or Judicial Grounds**

The authors legally analyzed the crime of technological harassment and Ecuadorian legislation with the legal interpretation of specialists in the area of knowledge and conducted surveys on the subject to students from several Ecuadorian universities and concluded that in Ecuadorian regulations, technological harassment and cyberbullying have not yet been classified in Criminal Legislation as crimes (Gómez-rodríguez & Garcés-córdova, 2023). The problems of cyberbullying in Ecuador are persistent since there is no law in force to punish cyberbullying according to the investigations carried out by researchers (Toapanta Toapanta et al., 2020). With the evolution of the Internet, bullying and cyberbullying have proliferated, creating serious tragic problems such as self-harm, suicides, among others, especially in the West and all countries of the world. To protect victims, many countries such as the United Arab Emirates (UAE), the United States (US), the United Kingdom (UK), and Canada have codified laws that address cybercrimes, including cyberbullying. To address the problem, the authors present a legal analysis of the existing laws against bullying and cyberbullying in the United Arab Emirates, the United States, the United Kingdom, and Canada. They obtained the characteristics of the laws and their capacity to protect society from various forms of crimes associated with cyberbullying and cyberbullying (Hosani et al., 2019). They consider that the Internet is a free medium for communication, it has many advantages but also the dark side. The existing laws in India are not enough to mitigate cybercrime, which is why they suggest debating this critical issue along with the existing laws for proper regulation (Kaur et al., 2022). They analyze the legal remedies available in Malaysia for disruptive AI technology and cyberbullying hate speech. The legal and judicial basis for AI intervention to mitigate cyberbullying needs to be reviewed. They define that there are concerns regarding the impact of artificial intelligence (AI) on freedom of expression and privacy rights. They suggest that artificial intelligence should be adequately regulated to be consistent with international human rights standards and national laws in Malaysia (Saufi et al., 2023). In the United States of America (USA) legal efforts and policies, analyzes judicial and legislative efforts to reduce bullying and makes some recommendations for school policy. In the USA there are laws to mitigate cyberbullying for vulnerable groups such as children, disabled, among others, but not for everyone. They carry out several debates on Civil rights laws and bullying, Legal definitions of bullying, Challenges of combining bullying and intimidation in state laws, Challenges of combining bullying with other peer aggressions in state legislation, Bullying in state criminal laws have generated a Federal Guide on bullying, among others (Cornell & Limber, 2015). In China and around the world, the Internet is in the stage of development and growth, and mitigating cyberbullying remains a

challenge and a challenge at the same time. Therefore, it is necessary to regulate the existing laws on this subject in order to define principles to achieve a balance between freedom of expression and regulation and between regulation by public law and judicial recourse, improve the existing legal provisions on civil remedies and criminal regulation, and clarify the conditions for the application of these legal provisions. The authors concluded that there is no adequate law on cyberbullying in China (Junke, 2020). They say the internet is influencing modern human life with the use of social media, artificial intelligence, and internet use making businesses and individuals vulnerable to cybercriminals. Cybercrime is increasing every year and the consequences include financial and reputational damage, loss of privacy and intellectual property violations. The UAE government has introduced changes to its unique cybercrime law, but there are concerns that it is not comprehensive enough to provide adequate protection to UAE citizens and residents (Rajan et al., 2017).

2.2. Methods

The deductive method is the research procedure based on logical reasoning that moves from the general to the specific, combined with exploratory research for analyzing information from various official websites, regulations, provisions, and laws of Ecuador, which was used as a case study.

In line with the principles of the deductive method and exploratory research, five phases were established for the analysis of the information. These phases will allow us to generate the respective results, which are outlined below:

- Generating the cyberbullying and cybercrime ecosystem
- Analyzing the cyberbullying cycle
- Analyzing the solutions proposed on social networks
- Evaluating the proposed solutions based on Artificial Intelligence (AI)
- Examining the status of cyberbullying laws in different countries.

- **Generating the Cyberbullying and Cybercrime Ecosystem**

In this ecosystem, we include cybercrime because the use of social networks and artificial intelligence increases the likelihood of it evolving into cybercrime or even cyberterrorism. This poses a serious threat to society, exacerbated by the lack of adequate legal or judicial frameworks to address and sanction both cyberbullying and cybercrime, as observed in Ecuador and globally.

In Figure 1, the cyberbullying and cybercrime ecosystem is described with the aim of identifying the relevant actors involved in creating this ecosystem.

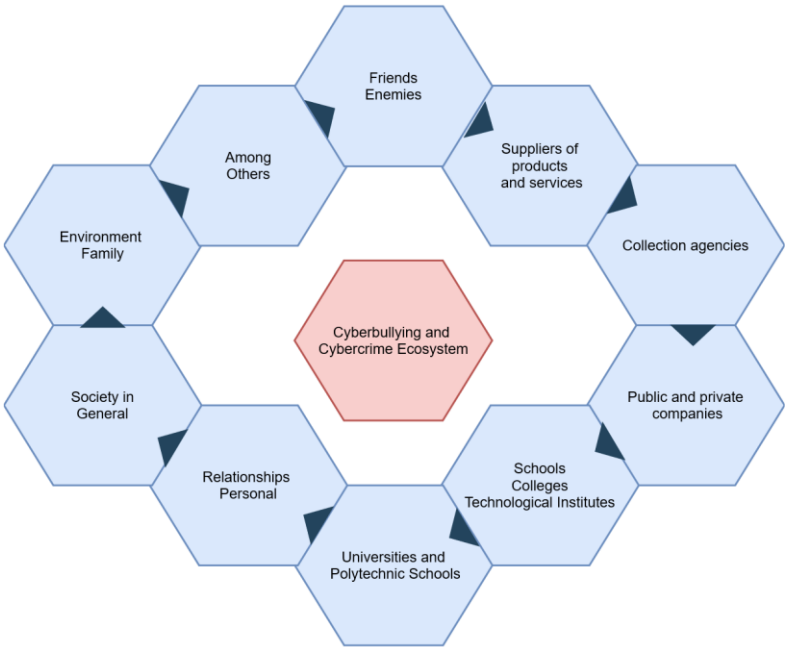

Figure 1: Cyberbullying and Cybercrime Ecosystem

- **Cyberbullying Cycle**

The definition of the cyberbullying cycle was developed in three phases (Nair et al., 2023). The cyberbullying cycle is defined in four phases, with the media serving as the foundation for initiating cyberbullying.

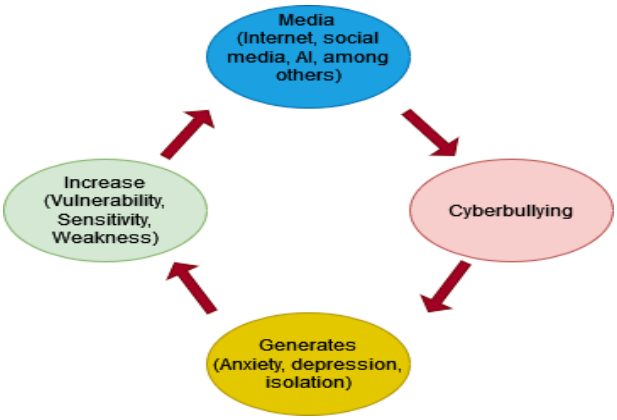

Figure 2: Cyberbullying Cycle

In Figure 2, the cyberbullying cycle is defined, which will help us identify the issues arising from bullying and cyberbullying in everyday life within society.

- **Analysis of the Solutions Proposed on Social Networks**

An analysis was conducted of the various solutions proposed for social networks that aim to mitigate cyberbullying, exploring them from different perspective.

Table 1: Proposed Solutions on Social Networks

No.	Proposed solutions	Ref.
1	Machine learning and deep learning technology.	(Hussein & Aleqabie, 2023)
2	ICT management model.	(Toapanta et al., 2020)
3	Chatbot design to identify cases of cyberbullying based on user feedback.	(Sanu et al., 2023)
4	State-of-the-art BERT model and PyThaiNLP library.	(Patthong et al., 2024)
5	Advanced methodology for detecting cyberbullying posts using machine learning algorithms.	(Swamy et al., 2023)
6	Roles of viewers within the corpus, to determine a significant impact on the annotators' perception and classification of cyberbullying instances.	(Alfurayj & Lutfi, 2023)
7	Conceptual model of influencing factors.	(Oladimeji & Kyobe, 2021)
8	Defining the nature of the victim, the behavior of the mobile stalker-victim on Facebook.	(Ndyave & Kyobe, 2019)
9	Automated detection systems based on machine learning.	(Vora et al., 2023)
10	Systematically structure and categorize the digital attributes that are interconnected across social media platforms.	(Grigaliunas et al., 2023)
11	Parameter model to determine cyberbullying on social networks in Ecuador.	(Toapanta et al., 2020)
12	Multimodal detection approach that integrates data from various sources including photos, videos, comments, and temporal information from social media.	(Ahmad Al-Khasawneh et al., 2024)

In Table 1, the various solutions aimed at mitigating cyberbullying are presented, including models, prototypes, software, machine learning, and other approaches.

- **Analysis of the Proposed Solutions based on Artificial Intelligence (AI)**

Artificial intelligence (AI) from Web 2.0 is integrated into social networks, which bring both advantages and disadvantages. Below, we outline the various proposals related to this integration.

Table 2. Proposed Solutions Artificial Intelligence

No.	Proposed AI solutions	Ref.
1	Model for the fusion of two different classifiers: the decision tree classifier and the AdaBoost classifier.	(Gopalan et al., 2023)
2	Predictive model applying Bi-LSTM and BERT.	(Gan et al., 2023)
3	Artificial Intelligence (AI)-based machine learning methods for detecting cyberbullying behavior.	(Pawar et al., 2022)
4	System for detecting fake accounts using machine learning techniques.	(Alekya Rani et al., 2024)
5	Model to address problems based on artificial intelligence (AI), supported by machine learning to make appropriate decisions.	(Kumar et al., 2023)
6	Detailed classification of cyberbullying by integrating neutrosophic logic into the multilayer perceptron (MLP) model.	(Ibrahim et al., 2024)

In Table 2, the various proposals based on artificial intelligence to mitigate cyberbullying on social networks are analyzed.

- **Cyberbullying Law Status in Different Countries**

The Law for Cyberbullying: In most countries, there is still no comprehensive law addressing cyberbullying. Below, we provide a general analysis based on expert opinions and the information available in scientific databases from the references.

Table 3: Status of the Cyberbullying Law and Countries with the Highest Cyberbullying Rates

Countries	**It has**		**Situation**					**Ref.**
	S	**N**	**D**	**I**	**P**	**S**	**A**	
Ecuador		√						(Gómez-rodríguez & Garcés-córdova, 2023)
Ecuador		√						(Toapanta Toapanta et al., 2020)
United Arab Emirates (UAE)	√				√			(Hosani et al., 2019)
United States (US)	√				√			(Hosani et al., 2019)
United Kingdom (UK)	√				√			(Hosani et al., 2019)
Canada	√				√			(Hosani et al., 2019)
India	√			√				(Kaur et al., 2022)
Malaysia	√		√					(Saufi et al., 2023)
United States (US). For children and vulnerable groups	√					√		(Cornell & Limber, 2015)
China	√				√			(Junke, 2020)
United Arab Emirates (UAE)	√			√	√			(Rajan et al., 2017)
Spain (First place)	√			√				(Planeta, 2024)
México (Segundo lugar)	√			√				(Planeta, 2024)
USA (Third place)	√			√				(Planeta, 2024)
Argentina (Fourth place)	√			√				(Planeta, 2024)
Italy (Fifth place)	√			√				(Planeta, 2024)
Japan (Sixth place)	√			√				(Planeta, 2024)

Description

S=Yes; N=No;
D= Development; I= Insufficient;
P= Partial; S= Enough;
A= Adequate.

In Table 3, we describe the status of cyberbullying laws over the past five years, based on information from the references. Additionally, we highlight the countries with the highest rates of cyberbullying according to 2024 reports. One of the main contributing factors is the inadequacy of laws addressing cyberbullying, particularly in terms of legal and judicial frameworks(Planeta, 2024).

3 Results

The results obtained in this research are:

- Mind map with relevant actors.
- Simulation to mitigate cyberbullying on social networks.
- Conceptual model for the management of cyberbullying.

3.1. Mind Map with Relevant Actors

Based on the information analyzed during the methodology phase, the result is the identification of the key actors needed to construct the cyberbullying mental map. This map enables a clearer understanding of the stakeholders involved, facilitating a more structured approach to addressing the issue.

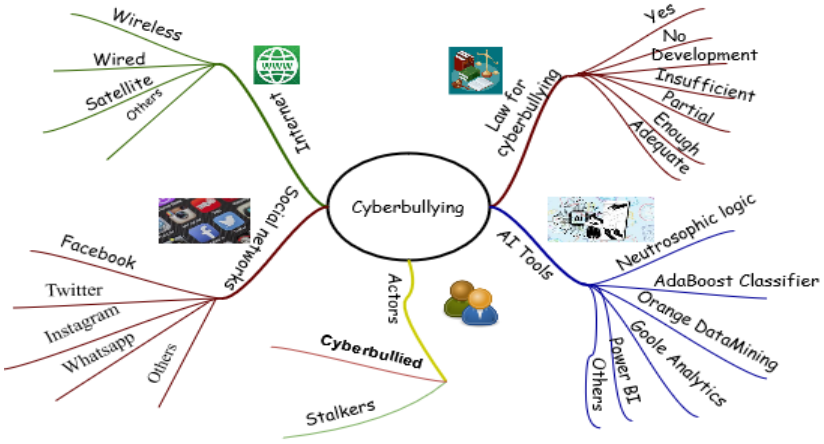

Figure 3: Cyberbullying Mind Map

In Figure 3, we identify the key actors involved in cyberbullying. With the unregulated growth of the internet, the uncontrolled use of various social networks, and the limited availability of tools or artificial intelligence software to mitigate cyberbullying, the situation has become increasingly concerning. It is important to note that most countries, including Ecuador—our case study—lack comprehensive laws addressing cyberbullying. This absence of legal frameworks has contributed to the widespread increase in cyberbullying, affecting individuals across all ages, genders, cultures, and social positions.

3.2. Simulation to Mitigate Cyberbullying on Social Networks

To conduct the simulation, five scenarios were analyzed, each varying in the number of social networks, the number of artificial intelligence tools used to mitigate cyberbullying, and the presence of at least one cyberbullying law in the country. The objective was to determine the level of cyberbullying and its corresponding percentage. This was calculated using the following formula (1) and (2):

$$=((1-(D5/C5))/E5) \quad (1)$$

$$=F5*100 \quad (2)$$

Description of formulas.

- 1: Corresponds to the condition that there must be at least one cyberbullying law in a country.
- D5: Corresponds to the number of artificial intelligence tools to mitigate cyberbullying. The higher the number, the greater the mitigation.
- C5: Corresponds to the number of social networks used.
- E5: Corresponds to the level of cyberbullying available.
- F5: Corresponds to the percentage of cyberbullying available.

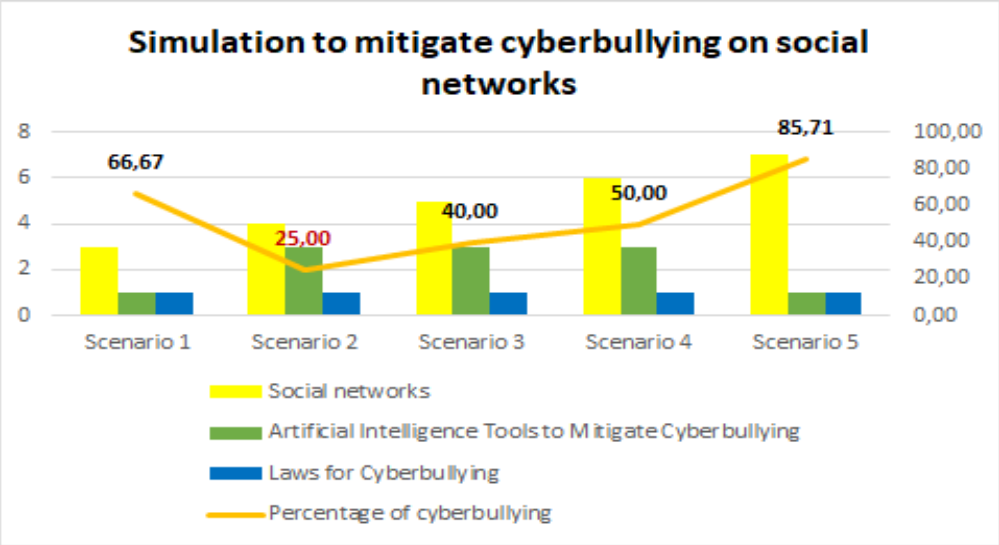

Figure 4: Simulation to Mitigate Cyberbullying

In Figure 4, a simulation was conducted to analyze different scenarios and their impact on cyberbullying. Below is an analysis of the findings:

- **Scenario 1 and Scenario 5:** These scenarios exhibit the highest levels of cyberbullying, as the number of social networks used is double the number of artificial intelligence tools implemented to mitigate cyberbullying.
- **Scenario 2:** This scenario achieves the lowest percentage of cyberbullying. The simulation involved the use of four social networks and three AI tools, making it the most effective configuration for reducing cyberbullying.
- **Scenario 3 and Scenario 4:** The percentage of cyberbullying ranges between 40% and 50%, attributed to the increased use of social networks without a proportional increase in mitigation measures.

According to data from *Bullying Without Borders*, in collaboration with the World Health Organization (WHO) and the Organization for Economic Cooperation and Development (OECD), approximately 58% of cyberbullying incidents occur through social networks like Facebook, Twitter, Instagram, and WhatsApp via technological devices. In Scenario 2 of the simulation, it was determined that cyberbullying could be reduced to 25% by adopting the proposed approach. This involves a balanced combination of a manageable number of social networks, adequate AI tools, and the implementation of a robust cyberbullying law.

3.3. Conceptual Model for the Management of Cyberbullying

Figure 5 presents a conceptual model for cyberbullying management, developed for our case study in Ecuador. The model is designed with a generic structure, making it adaptable for implementation in other countries. The primary outcome of this research phase is a conceptual model that facilitates the effective management of cyberbullying. This model enables the identification and visualization of the sequence of processes in a comprehensive and structured manner. To successfully mitigate cyberbullying, it is crucial to implement appropriate artificial intelligence tools, establish a robust cyberbullying law with detailed regulations, and incorporate other essential measures.

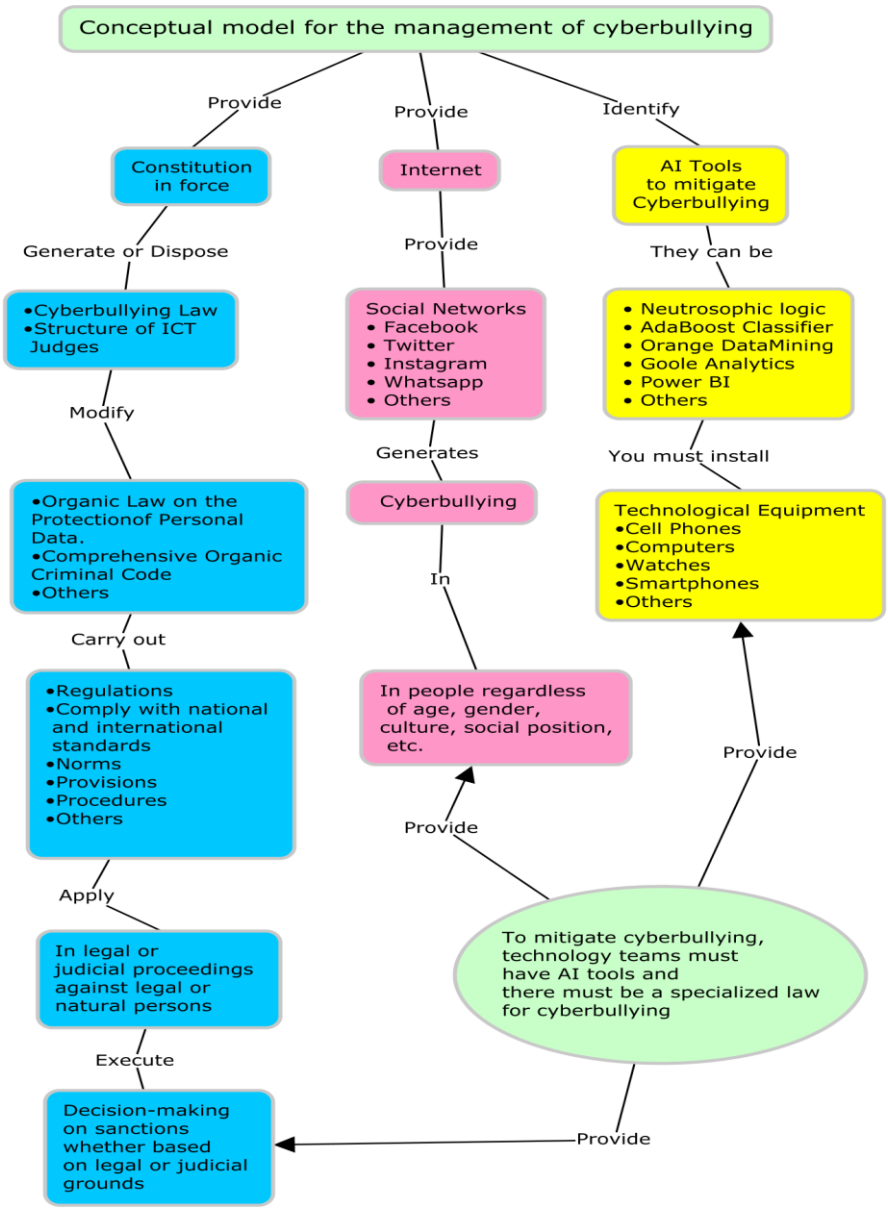

Figure 5: Conceptual Model for Cybersecurity Management

4 Discussion

The results of this research include: a mental map identifying key stakeholders, a simulation aimed at mitigating cyberbullying on social networks, and a conceptual model for cyberbullying management. These tools provide a comprehensive overview of the cyberbullying situation in Ecuador and globally.

During the methodology phase, we developed a cyberbullying and cybercrime ecosystem, outlined the cyberbullying cycle, analyzed proposed solutions implemented on social networks, proposed solutions leveraging Artificial Intelligence (AI), and examined the legal landscape for cyberbullying in various countries. These efforts aimed to provide a multidimensional perspective on cyberbullying and review the scope of existing research.

In the introduction phase, we reviewed documents and materials related to cyberbullying, social networks, AI, and legal frameworks. A consensus emerged: cyberbullying is a significant global issue affecting individuals regardless of age, gender, culture, or social status. The proliferation of information and communication technologies, borderless Internet access, social networks, and the misuse of AI have exacerbated this problem.

Our research contributions include the methodology used to achieve these results, offering a novel approach to cyberbullying management compared to existing literature. These results are applicable in countries with similar cultural and demographic characteristics, particularly those lacking specific cyberbullying legislation and ready to confront this challenge.

The United Nations has identified cyberbullying as one of the top 20 global issues requiring urgent attention. Cyberbullying has become entrenched in society and disproportionately affects vulnerable groups. For instance, societal biases may lead to different perceptions of similar behaviors based on socioeconomic status or physical appearance.

A notable limitation in Ecuador is that only a member of the National Assembly can introduce a bill to address cyberbullying, which complicates legislative progress. Additionally, limited financial resources hinder access to licensed AI tools tailored to mitigating cyberbullying, as well as the development and enforcement of laws, regulations, and provisions to combat this issue effectively.

5 Future Works and Conclusion

Research on cyberbullying, both globally and in Ecuador, must continue to explore alternative perspectives and propose strategies to mitigate its impact on social networks.

This study concludes that mitigating cyberbullying requires the essential use of appropriate artificial intelligence (AI) tools and the creation or improvement of cyberbullying laws in every country. Simulations conducted during the research revealed that, in scenario two, cyberbullying could reach an average prevalence of 25%. This highlights the critical need for AI-driven solutions and updated legislation to address this challenge effectively.

Creating a mental map that identifies the key stakeholders involved in cyberbullying is essential to gaining a clearer understanding of the issue in each country. One proposed approach is the development of a conceptual model for cybersecurity management. Conceptual model would serve as a guide, outlining the necessary elements to mitigate cyberbullying, such as the technological infrastructure, appropriate AI tools, and specialized legal frameworks.

The lack of dedicated cyberbullying laws—or the existence of insufficient legal frameworks—poses a significant barrier. Without proper legislation addressing legal and judicial processes, educational institutions, public organizations, and private companies may face unfair sanctions due to the absence of clear, enforceable guidelines.

Additionally, this study emphasizes the need to establish specific legislation governing the use of AI in legal and judicial processes. AI currently operates without a robust legal foundation, which risks its misuse in ways that could exacerbate cyberbullying rather than mitigate it.

Finally, the research offers contributions that could assist Ecuadorian authorities in advocating for the creation of a Cyberbullying Law. This includes the establishment of specialized ICT judges, akin to those in fields such as juvenile, traffic, or criminal justice. With the expectation that 100% of legal processes will eventually be automated, the need for trained and specialized personnel is pressing. The

findings of this study may also serve as a reference for conducting diagnostic assessments in other countries with similar contexts.

Acknowledgements

The authors thank the Center for Security Studies (CESEG), Universidad de Santiago de Compostela (USC) Spain, Information Technology Engineering-Universidad Tecnológica Indoamérica, Research Department, Gestión de Tecnologías Para El Mundo (GTM), Information Systems Department of the CUCEA University of Guadalajara (UDG), Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG) and RNI-Senescyt.

References

[1] Abdul Rahman, N. S., Sahabudin, N. A., Eh Phon, D. N., Ab Razak, M. F., & Mat Raffei, A. F. (2023). Factors Affecting Cyberbullying Behaviours among University Students: A Review. *8th International Conference on Software Engineering and Computer Systems, ICSECS 2023*, 342–346. https://doi.org/10.1109/ICSECS58457.2023.10256292

[2] Abdullah, D. (2024). Enhancing cybersecurity in electronic communication systems: New approaches and technologies. *Progress in Electronics and Communication Engineering*, *1*(1), 38-43.

[3] Ahmad Al-Khasawneh, M., Faheem, M., Abdulsalam Alarood, A., Habibullah, S., & Alsolami, E. (2024). Toward Multi-Modal Approach for Identification and Detection of Cyberbullying in Social Networks. *IEEE Access*, *12*(July), 90158–90170. https://doi.org/10.1109/ACCESS.2024.3420131

[4] Alekya Rani, Y., Srividya, G., Balaram, A., Kumar, K. H., Kiran, A., & Silparaj, M. (2024). Fake Account Detection using ANN Based Model in Machine Learning. *Proceedings of 2024 International Conference on Science, Technology, Engineering and Management, ICSTEM 2024*, 1–7. https://doi.org/10.1109/ICSTEM61137.2024.10561061

[5] Alfurayj, H. S., & Lutfi, S. L. (2023). Exploring Bystanders' Roles in Labeled Cyberbullying Threads on Twitter: A preliminary analysis. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 1018–1023. https://doi.org/10.1109/TENCON58879.2023.10322517

[6] Banerjee, V., Telavane, J., Gaikwad, P., & Vartak, P. (2019). Detection of Cyberbullying Using Deep Neural Network. *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 604–607. https://doi.org/10.1109/ICACCS.2019.8728378

[7] Coip. (2024). Código Orgánico Integral Penal (COIP)-2024. In *Registro Oficial - Ógano del Gobierno del Ecuador*.

[8] Cornell, D., & Limber, S. P. (2015). Law and policy on the concept of bullying at school. *American Psychologist*, *70*(4), 333–343. https://doi.org/10.1037/a0038558

[9] De Vicente Pachés, F. (2020). El Convenio 190 OIT y su trascendencia en la gestión preventiva de la violencia digital y ciberacoso en el trabajo. *Revista de Trabajo Y Seguridad Social. CEF*, *448*, 69–106. https://doi.org/10.51302/rtss.2020.1004

[10] Deihim, J., Sadeghi, T., & Rezaei, S. (2014). Role of information technology and information systems in the process of improving the quality of education manager's decisions. *International Academic Journal of Organizational Behavior and Human Resource Management*, *1*(1), 54–70.

[11] Donkor, K., & Zhao, Z. (2023). Building Brand Equity Through Corporate Social Responsibility Initiatives. Global Perspectives in Management, 1(1), 32-48.

[12] Gan, M. F., Chua, H. N., Jasser, M. B., & Wong, R. T. K. (2023). Experimenting Datasets and Machine Learning Techniques for Enhancing Cyberbullying Detection. *2023 IEEE 11th Conference on Systems, Process and Control, ICSPC 2023 - Proceedings*, *December*, 379–383. https://doi.org/10.1109/ICSPC59664.2023.10420359

[13] Gaurang, G., Kumar, S., Dave, G., John, H., Mudita, S., & Rob, R. (2015). Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6(4), 47-63.

[14] Gómez-rodríguez, M. E., & Garcés-córdova, F. A. (2023). The crime of technological harassment and Ecuadorian legislation. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, *VIII*(1), 105–120.

[15] Gopalan, A., Allin Geo, a. V., Kavitha, T., Mohanavel, V., Vinoth Rajkumar, G., & Pooja, P. (2023). Experimental Evaluation of Robust Cyberbullying Detection over social media using Intelligent Learning Scheme. *2023 IEEE International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering, RMKMATE 2023*, 1–7. https://doi.org/10.1109/RMKMATE59243.2023.10368747

[16] Grigaliunas, S., Bruzgiene, R., & Venckauskas, A. (2023). Ontology-Driven Digital Profiling for Identification and Linking Evidence Across Social Media Platform. *IEEE Access*, *11*(October), 111672–111691. https://doi.org/10.1109/ACCESS.2023.3322162

[17] Hosani, H. Al, Yousef, M., Shouq, S. Al, Iqbal, F., & Mouheb, D. (2019). A comparative analysis of cyberbullying and cyberstalking laws in the UAE, US, UK and Canada. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *2019-Novem*, 1–7. https://doi.org/10.1109/AICCSA47632.2019.9035368

[18] Hussein, F. N. A., & Aleqabie, H. J. (2023). Cyberbullying Detection on Social Media: A Brief Survey. *2nd International Conference on Advanced Computer Applications, ACA 2023*, 142–147. https://doi.org/10.1109/ACA57612.2023.10346758

[19] Ibrahim, Y. M., Essameldin, R., & Saad, S. M. (2024). Social Media Forensics: An Adaptive Cyberbullying-Related Hate Speech Detection Approach Based on Neural Networks With Uncertainty. *IEEE Access*, *12*(April), 59474–59484. https://doi.org/10.1109/ACCESS.2024.3393295

[20] Junke, X. (2020). Legal Regulation of Cyberbullying - From a Chinese perspective. *Proceedings - IEEE 18th International Conference on Dependable, Autonomic and Secure Computing, IEEE 18th International Conference on Pervasive Intelligence and Computing, IEEE 6th International Conference on Cloud and Big Data Computing and IEEE 5th Cybe*, 322–327. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00063

[21] Kaur, G. D., Iyer, S., & Shukla, V. K. (2022). Cyber Harassment In Transgender Community: Status And Legal Regulation In India. *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2022*, 1–4. https://doi.org/10.1109/ICRITO56286.2022.9964575

[22] Khomyshyn, I., Parpan, U., Lesko, N., Slyvka, M., & Tsvok, M. (2021). Legal principles of counteracting cyberbullying against children. *Journal of Education Culture and Society*, *12*(2), 67–76. https://doi.org/10.15503/jecs2021.2.67.76

[23] Kumar, R., Sharma, A., Kaur, M., Joshi, K., & Singh, S. (2023). Role of Artificial Intelligence to address Cyberbullying and Future Scope. *Proceedings of International Conference on Computational Intelligence and Sustainable Engineering Solution, CISES 2023*, 974–977. https://doi.org/10.1109/CISES58720.2023.10182406

[24] Ley Organica de Proteccion de Datos Personales. (2021). *Reglamento-Ley-PDP-Decreto-Ejecutivo-No.-9041*.

[25] Maity, K., Saha, S., & Bhattacharyya, P. (2023). Emoji, Sentiment and Emotion Aided Cyberbullying Detection in Hinglish. *IEEE Transactions on Computational Social Systems*, *10*(5), 2411–2420. https://doi.org/10.1109/TCSS.2022.3183046

[26] Martínez, I., Reyes, D., & Rosero, F. (2021). Constitución de la Republica del Ecuador. In *Alteridad*. https://doi.org/10.17163/alt.v2n2.2007.04

[27] Ministerio de Telecomunicaciones y de la Sociedad de la Información - MINTEL. (2021). *Reglamento a Ley Orgánica de Protección de Datos Personales - LOPDP*. https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

[28] Moncayo Valdez, M. M., & Maldonado Ruiz, L. M. (2023). Acoso laboral desde el marco legal y sus efectos en la sociedad. *Reciamuc*, *7*(1), 817–827. https://doi.org/10.26820/reciamuc/7.(1).enero.2023.817-827

[29] Nair, M. M., Fernandez, T. F., & Tyagi, A. K. (2023). Cyberbullying in Digital Era: History, Trends, Limitations, Recommended Solutions for Future. *2023 International Conference on Computer Communication and Informatics, ICCCI 2023*, *Iccci*, 1–10. https://doi.org/10.1109/ICCCI56745.2023.10128624

[30] Ndyave, Z. C., & Kyobe, M. (2019). Mobile Bully-victim Behaviour on Facebook: The case of South African Students. *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*, 743–749. https://doi.org/10.1109/IEMCON.2019.8936272

[31] Oladimeji, A., & Kyobe, M. (2021). Factors influencing cyberbullying on instagram among university students. *2021 Conference on Information Communications Technology and Society, ICTAS 2021 - Proceedings*, 139–144. https://doi.org/10.1109/ICTAS50802.2021.9394974

[32] Orgánica, L. (2023). *Suplemento del Registro Oficial No. 167, 16 de Diciembre 2005 Normativa: Vigente Última Reforma: Suplemento del Registro Oficial 242, 1-II-2023* (Issue 167).

[33] Patthong, P., Doungdee, T., Songmuang, P., & Kongkachandra, R. (2024). Detecting Defamation Words from Social Media Comments. *International Conference on Cybernetics and Innovations, ICCI 2024*, 1–6. https://doi.org/10.1109/ICCI60780.2024.10532559

[34] Pawar, V., Jose, D. V., & Patil, A. (2022). Explainable AI Method for Cyber bullying Detection. *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications, ICMNWC 2022*, 1–4. https://doi.org/10.1109/ICMNWC56175.2022.10031652

[35] Planeta, E. por el observatorio mundial de bullying y de ciberbullying de bullying sin fronteras con profesionales en 140 países de todo el. (2024). *Estadísticas Mundiales de Ciberbullying 2024. World Cyberbullying Stats 2024.* 2012 ONG Bullying Sin Fronteras / NGO Bullying Without Borders / ONG Harcèlement Sans Frontières 2023. https://bullyingsinfronteras.blogspot.com/2016/12/primer-estudio-sobre-el-ciberbullying.html

[36] Rajan, A. V., Ravikumar, R., & Shaer, M. Al. (2017). UAE cybercrime law and cybercrimes - An analysis. *2017 International Conference on Cyber Security And Protection Of Digital Services, Cyber Security 2017*, *2*, 1–6. https://doi.org/10.1109/CyberSecPODS.2017.8074858

[37] Sanu, E., Mummigatti, M., & Mohana. (2023). Design of Chatbot to Prevent Cyberbullying from Social Media. *International Conference on Sustainable Communication Networks and Application, ICSCNA 2023 - Proceedings*, *Icscna*, 1437–1441. https://doi.org/10.1109/ICSCNA58489.2023.10370729

[38] Saufi, N. N. M., Kamaruddin, S., Mohammad, A. M., Jabar, N. A. A., Rosli, W. R. W., & Talib, Z. M. (2023). Disruptive AI Technology and Hate Speech: A Legal Redress in Malaysia. *2023 International Conference on Disruptive Technologies, ICDT 2023*, 759–763. https://doi.org/10.1109/ICDT57929.2023.10150942

[39] Swamy, M., Gopalakrishnan, J., Dhasarathan, D., Alfred Christo, W., Hariharan, S., & Kukreja, V. (2023). Cyberbullying Avoidance and Impact from Online Tweets. *2nd International Conference on Automation, Computing and Renewable Systems, ICACRS 2023 - Proceedings*, 390–394. https://doi.org/10.1109/ICACRS58579.2023.10405204

[40] Toapanta Toapanta, S. M., Alfredo Espinoza Carpio, J., & Mafla Gallegos, L. E. (2020). An Approach to Cybersecurity, Cyberbullying in Social Networks and Information Security in Public Organizations during a Pandemic: Study case COVID-19 Ecuador. *2020 Congreso Internacional de Innovacion Y Tendencias En Ingenieria, CONIITI 2020 - Conference Proceedings*. https://doi.org/10.1109/CONIITI51147.2020.9240375

[41] Toapanta Toapanta, S. M., Tacuri López, I. L., & Mafla Gallegos, L. E. (2020). Analysis of the legal basis to mitigate cyberbullying in social networks in Ecuador. In *Frontiers in Artificial Intelligence and Applications* (Vol. 331, pp. 223–233). https://doi.org/10.3233/FAIA200702

[42] Toapanta, S. M. T., Kevin Enrique Yagual, E., & Gallegos, L. E. M. (2020). Parameters to Determine Cyberbullying in Social Networks in the Ecuador. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3404663.3404677

[43] Toapanta, S. M. T., Ramirez, K. J. R., Arellano, M. R. M. I., & Gallegos, L. E. M. (2020). Definition of an ICT management model to mitigate cyberbullying risk in social networks. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 699–706. https://doi.org/10.1109/WorldS450073.2020.9210384

[44] Vora, D., Mukherjee, A., Repaka, S., Das, S., & Ingle, S. (2023). Multimodal Cyberbullying Detection on Social Media: Review and Challenges. *2023 International Conference on Integration of Computational Intelligent System, ICICIS 2023*, 1–8. https://doi.org/10.1109/ICICIS56802.2023.10430250

[45] Yesmin, S., & Abdul Karim, M. (2020). Professionalism in Using Online Social Networking Tool: An Assessment of LIS Students' Facebook Profiles. Indian Journal of Information Sources and Services, 10(2), 10–13. https://doi.org/10.51983/ijiss.2020.10.2.493

Authors Biography

Dr. Diego Gustavo Andrade Armas, PhD., holds a PhD in the Doctorate Program in Law from the University of Santiago de Compostela in Spain, a Master's Degree in Judicial Social Sciences from the Central University of Ecuador, a Higher Diploma in University Teaching, a Doctorate in Jurisprudence and a Bachelor's Degree in Legal Sciences from the Pontifical Catholic University of Ecuador. He has published several scientific articles in journals and conferences of worldwide impact indexed in Scopus and Web of Science with SJR/JCR impact respectively. He is currently Notary 4 in the city of Ibarra. He is a research professor at several universities in Ecuador and has held various public and private positions in Ecuador and Spain.

Prof. Segundo Moisés Toapanta Toapanta, Prof. Moises Toapanta T. holds a PhD in Information Technology from the University of Guadalajara, Mexico, a Master's Degree in Communications and Information Technology Management from the National Polytechnic School (EPN), and a degree in Computer Engineering and Computer Science. He is an accredited evaluator and researcher, categorized as Principal 1 in the RNI-Senescyt. He has presented scientific articles in person in 40 countries in Europe, Asia and America. Research areas: Strategic Alignment of ICT, Information Security, Cryptography, Cybersecurity, Cyberbullying, Cybercrime, Education, AI, Robotics, Blockchain Technologies and Applications.

Prof. Eriannys Zharayth Gómez Díaz, is a PhD candidate in the "Doctorate in Educational Sciences" at the Universidad Pedagógica Experimental Libertador de Venezuela, Master in Educational Pedagogy with a mention in Virtual Learning Environments and Specialist Professor in the area of Physics. She is a professor in Master's degrees and teaching assistant at Universities in Mexico and Spain. She is an external researcher at the company Gestión de Tecnologías para el Mundo "GTM". She has several scientific articles published in journals and conferences of worldwide impact indexed in Scopus and Web of Science with SJR/JCR impact respectively, she has made several scientific presentations in China, Japan, the USA, Peru and other countries. She is a reviewer in journals and conferences of worldwide impact. Her research areas are: Education and innovation, Virtual environments, Information Security, Cyberbullying, Robotics and Information Technologies.

Dr. Janio Lincon Jadán Guerrero, PhD, holds a PhD in Computer Science and Informatics and a Master of Science in Computer Science and Informatics from the University of Costa Rica, a Master of Administration and Marketing from the Universidad Tecnológica Indoamérica, and a Computer Science Engineer from the Universidad Central del Ecuador. He has several publications in journals and conferences indexed in Scopus and Web of Science with SJR/JCR impact respectively. He has given scientific presentations at several universities in North America, Europe, and Latin America. He is currently Vice-Rector of Research at the Universidad Tecnológica Indoamérica. His lines of research are: Teaching, Cyberbullying, AI, Robotics, Information Technologies, and IoT.

Prof. Rocío Maciel Arellano, is a Research Professor in the Information Systems Department of the CUCEA University of Guadalajaraand is currently Coordinator of Linking and Talent at the Center for Innovation in Smart Cities of the UDG. She is a member of the academic nucleus of the Doctorate in Information Technology, of which she was coordinator from 2013 to 2016, obtaining her accreditation in the National Quality Standard (PNPC) by the National Council of Science and Technology (CONACYT). He has extensive experience in the field of virtual education through online platforms and has directed several research and postgraduate thesis, in addition to supporting projects in Information Technology. Additionally, it has scientific publications and has participated in international conferences and panels. Manage national and international projects. Research Areas: Smart Cities, Education and innovation, Virtual environments, Information Security and Cyberbullying.

Prof. María Mercedes Baño Hifóng, is Doctor in Strategic Business Administration from the Pontifical Catholic University of Peru, Master in education and educational innovation. She also has a master's degree in international public accounting and a diploma in the same specialty from the University of Guadalajara (Mexico), a degree in economics with a mention in business management. She has extensive experience as a financial consultant for national and international companies. She has participated in presentations, publication of scientific articles, book chapters and books contributing from the financial and accounting perspective to the sustainable development of the business environment. She is the functional coordinator of the Vice President for Research and Postgraduate Studies at the Catholic University of Santiago de Guayaquil, where she participates in inter-institutional research projects at the local and regional levels. She is the leader of the research table at the Finance and Accounting Observatory of the Accreditation Council for Business Schools and Programs (ACBSP). Research Areas: Strategic Alignment, International Business, Information Security, Business Administration and Information Technology.