



Revista Brújula

Investigación formativa sobre ciencias militares

Contenido

- ◆ **The AI dilemma: How does Artificial Intelligence affect Human Rights?** / 4-15
Sergio Andrés López Zamora y Valentina Hernández Chinome
- ◆ **Inteligencia artificial y ciberdelincuencia: amenazas emergentes para la infancia y adolescencia en la era de los deepfakes** / 16-33
Aldair Bueno Atencio
- ◆ **Control+Alt+Delito: Reflexiones jurídicas sobre la cibercriminalidad en Colombia** / 34-42
Angela Rosa Mejía Corrales
- ◆ **Escuela Militar de Cadetes "General José María Córdova": optimización del proceso de contratación del personal docente** / 43-64
Ricardo Andrés Bernal Vallarino, Esteban Darío Maigual Maigual y Cristian Horacio Pérez Navarro
- ◆ **Reseña de libro: El derecho internacional humanitario y Juego de Tronos** / 65-68
Juan Fernando Gil Osorio

Revista Brújula

(Investigación formativa sobre ciencias militares)

eISSN 2346-0628

Volumen 13, número 25, enero-junio 2025

DIRECTIVOS

Escuela Militar de Cadetes

Director

Brigadier General **Milton Cesar Escobar Gallego**

Subdirector

Coronel **Milton Fernando Monroy Franco**

Vicerrector Académico

Coronel **Carlos Mario Bernal Correa**

Jefe Departamento de Investigación, Desarrollo Tecnológico e Innovación

Mayor **Christian Rodríguez Macea**

CONSEJO EDITORIAL

Editor

Coronel (R) **Andrés Eduardo Fernández Osorio**

Corrección de estilo

Jorge Aristizabal Gáfaró

Diseño y diagramación

Rubén Alberto Urriago Gutiérrez



2025, Escuela Militar de Cadetes "General José María Córdova"
Departamento de Investigación, Desarrollo Tecnológico e Innovación (I+D+i)
Calle 80 No. 38-00. Bogotá, D. C. Colombia
Teléfono: 377 0850 Ext. 1104
Licencia Creative Commons: Atribución – No comercial – Sin Derivar
Correo: revistabrujula@esmic.edu.co
Página web: <https://brujuladesemilleros.com>

La responsabilidad por el contenido de los artículos publicados corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Militar de Cadetes "General José María Córdova", el Ejército Nacional de Colombia o el Ministerio de Defensa Nacional.



Respice Militia



CONTENIDO

DOSIER

1. The AI dilemma: How does Artificial Intelligence affect Human Rights? / 4-15

Sergio Andrés López Zamora y Valentina Hernández Chinome

2. Inteligencia artificial y ciberdelincuencia: amenazas emergentes para la infancia y adolescencia en la era de los deepfakes / 16-33

Aldair Bueno Atencio

3. Control+Alt+Delito: reflexiones jurídicas sobre la cibercriminalidad en Colombia / 34-42

Angela Rosa Mejía Corrales

4. Escuela Militar de Cadetes “General José María Córdova”: optimización del proceso de contratación del personal docente / 43-64

Ricardo Andrés Bernal Vallarino, Esteban Dario Maigual Maigual y Cristian Horacio Pérez Navarro

5. Reseña de libro: El derecho internacional humanitario y Juego de tronos / 65-68

Juan Fernando Gil Osorio



Dossier



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, 20254. pp. 4-15

Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.175>

DOSIER

The AI dilemma: How does Artificial Intelligence affect Human Rights?

Sergio Andrés López Zamora 

Valentina Hernández Chinome 

Universidad Santo Tomas Seccional Tunja, Colombia

ABSTRACT

This article analyses the prevalence of human rights in the development of Artificial Intelligence (AI), approaching it from a historical and conceptual review of AI, evaluating its evolution and the impact it has had on society. It highlights how AI has advanced significantly and has been integrated into multiple aspects of human life, facilitating complex tasks and being efficient in various fields; however, it is essential to raise the challenges regarding how it impacts human rights, and the need to establish robust legal and ethical frameworks to regulate its accelerated development and use.

KEYWORDS:

automatic reasoning; globalization; human evolution; regulation; society; specialty; tools.

HOW TO CITE (APA):

López Zamora, S. A., & Hernández Chinome, V. (2025). The AI dilemma: How does Artificial Intelligence affect Human Rights? *r. Revista Brújula de Investigación*, 13(25), 4-15.

<https://doi.org/10.21830/23460628.175>

Recibido: 1April 15, 2025 **Aceptado:** June 20, 2025

Contacto: Valentina Hernández Chinome  valentina.hernandez@usantoto.edu.co



Introduction

During human evolution, humans have had to live in society to ensure their survival. Based on this end, each subject has been entrusted with different tasks, giving rise to work and specialization; however, this division of labor has intrinsically brought with it a solution to the need to meet social requirements, thereby guaranteeing harmonious coexistence and the survival of the species.

Through work, humans have dignified their existence and given it value, engaging in various activities, some of which are more complex than others. However, despite the above, each individual has sought ways to facilitate their work, making use of their instinct for creating tools, just as they have used to create their tools.

That advance is in line with collective activities and needs. The gadgets created have facilitated production and, with it, existence itself, reaching previously unthinkable points; so much so that today we have intangible tools that develop highly complex tasks, and their development continues to advance, as in the case of Artificial Intelligence.

The development of Artificial Intelligence (henceforth referred to as AI) has provided individuals with a tool for accessing the world in its entirety. This has also raised several ethical and legal questions, particularly regarding human rights. On the one hand, AIs offer the community considerable benefits in terms of convenience, speed of access to information, efficiency, and innovation. On the other hand, challenges arise that must be addressed to ensure respect and protection of users' fundamental rights.

In this sense, the question arises: What is the theoretical importance of human rights in the development of AIs? This question provides an analysis that will be developed under the following headings:

The age of Artificial Intelligence

AIs are not a creation of the 21st century; on the contrary, they have been developed since time immemorial. According to Vicenç Torra (2019), "The term artificial intelligence (AI) was adopted during the summer of 1956 in Dartmouth at a meeting that brought together researchers interested in the topics of intelligence, neural networks, and automata theory" (p.7). This circumstance makes it possible to establish that AI is not a recent phenomenon, but rather a thought and idea that has been evolving throughout the annals of history. It is only at a certain point in history, not very distant, that it is given a name of its own.

The rapid advance of AI has marked a new moment in human history. It gives rise to a new beginning in which humanity accesses information and technological tools



instantly, according to its needs. These new intelligences have experienced significant advances, mainly in recent years, resulting in access to sophisticated algorithms that offer substantial data processing capacity, as well as a vast array of information.

Despite the advances it has presented, it has been highly complex to define what an AI is objectively; however, “four approaches have been followed throughout history. As might be expected, there is a clash between human-centred and rationality-centred approaches” (Russell, 2008, p.30).

Among the early approaches to defining AIs, the first two focus on the human. A division is made between concepts, the first to analyse part of the system that thinks like a human: “the new and exciting endeavour to make computers think... machines with minds, in the broadest literal sense” (Haugeland, 1985). This is complemented by “the automation of activities that we link to human thought processes, activities such as decision making, problem solving, learning... (Bellman, 1978)”.

The second concept examines systems that behave like humans. It defines AI as “the art of developing machines capable of performing functions that when performed by humans require intelligence” (Kurzweil, 1990). It also states that it is “the study of how to get computers to perform tasks that, for the moment, humans do best” (Rich & Knight, 1991). This is how one can begin to think of AI as the need to bring some human intelligence to everyday tools.

It then becomes clear that the starting point of AI is the human being, their behavior, thinking, and acting; their whole being, intelligence analysis, and knowledge construction, the latter two points giving way to the next approach to the concept of AI.

The second approach to AI focuses on reasoning. Like the previous one, the concept focuses on two points: the first point is systems that reason. This is based on the definition that AI is “the study of mental faculties through the use of computational models” (Charniak & McDermott, 1985). This is made possible through the “study of computations that make it possible to perceive, reason, and act” (Winston, 1992). A concept that satisfies the claims of the need for information required by humans to fulfil their daily obligations but provided using a pre-coded algorithm.

The second point of reasoning lies in systems that act rationally. This item highlights the fact that AI is a creation that must focus on overcoming intelligence, specifically: “Computational Intelligence is the study of the design of intelligent agents” (Poole et al., 1998).

For researchers and authors interested in defining AI for this new era, an absolute concept has not yet emerged, as it depends on the starting point of analysis. However, even though the concepts are changing, some elements have remained con-



stant, such as thinking of AI as a system; the need for the system to take on human intelligence; the idea that these systems should serve as a tool for human beings but based on human reasoning and planning for it to work on its own, through a computer or technological element.

Thus, AI should be understood as a system created by human beings that possesses intelligence capable of rationalizing actions through algorithms specifically encoded with a function, and whose operation materialized through technological instruments. "AI... is related to intelligent behavior in artefacts" (Nilsson, 1998). It is worth noting that in the 21st century, access to technological artifacts has become common, resulting in widespread access to AI for the broader community.

Over the last decade, access to technological elements has increased, resulting in the fact that almost everyone has a computer, a mobile phone, a tablet, and internet access. As we have been saying, to access an AI, it is only necessary to have a computer. This means that technology itself represents AI: an artefact with intelligence capable of instant rationalization, and which is available to a large percentage of human beings around the world.

The fact that every human being can nowadays have access to AI has meant that it must have specific characteristics, which must be approved. The primary need for AI is intelligence, which must be equal to or superior to that of a human being. To determine if it can make decisions, it must be subjected to the Turing Test, proposed by Alan Turing (1950).

Alan Turing proposed that: "if a computer program could fool a set of human judges into thinking it was human, then that program must be intelligent" (Angeles, 2019). The Turing test states that the system must have several features:

- Natural language processing to enable him/her to communicate successfully in English.
- Knowledge representation to store what is known or felt.
- Automatic reasoning to use stored information to answer questions and draw new conclusions.
- Machine learning to adapt to new circumstances and to detect and extrapolate patterns (Russell, 2008, p.31).

In trying to resemble human intelligence, in order to fulfill the above capabilities, AI must learn as humans do. It is in this way that Machine Learning is incorporated, which is a "method of data analysis that learns from experience, allowing computers to find hidden information without being explicitly programmed" (Angeles, 2019). However, despite this and as is recognizable throughout this analysis, AI evolves and



its elements with it; in such a way that the union of Deep learning is realized. Deep learning is a concept that emerged in 2010:

It aims to mimic a human neural network through artificial intelligence, deep learning as it is also known, which is based on the design of individual layers of connections that maintain communication with other layers of information subject to an unlimited amount of data that is used first individually and then generally, for a specific task (just like a human neural network), is an aspect of machine learning that was designed to expand the contexts in which it was applied (Morán, 2020, p. 281-322.

This is centered on the fact that, in this technological era, artefacts are beginning to feature AI, endowing objects (such as cars, computers, appliances, tools, and even accessories) with the ability to serve humans. This is a result of the technological quest and the need to upgrade items to perform increasingly complex tasks that only human intelligence can perform.

Thus, for this era, it is established that AI systems are evolving and endowed with human intelligence, created to facilitate the existence of subjects. Due to globalization, they must be able to serve everyone, which is why they are constantly advancing; however, it should be noted that the use and access to intelligence by different subjects are beginning to generate an ethical and social debate.

Although they are great tools for this new technological era, adapted to the needs of subjects in general, they can be used in a counterproductive way against a third party. Some thinkers, such as Volker Türk, the United Nations High Commissioner for Human Rights, have established that AI is the future of humanity, a change that will lead to economic, social, political and cultural globalization; on the contrary, others, such as Yuval Noah Harari, author of "Sapiens" and "Homo Deus", have stated that AI can threaten the work of the community, provoke mass unemployment and economic inequality. This extends to affecting human rights, which are fundamental guarantees for every individual.

Challenges for the law in the face of artificial intelligence

As mentioned, the new era of AI brings about technological advances, but these advances also raise legal issues. AI is a human creation that seeks perfection, but throughout history, it has been shown that perfect is not a universal term but a personal one; the example of the Second World War and its implications.

Thus, it cannot be denied that personal biases of each user can be found within the algorithms that feed AI. Indeed, AI learns empirically about human behavior, but this is where one of the many concerns begins to emerge: human behavior is not always



the most appropriate, and this leads to the AI adopting discriminatory, immoral, or unlawful behavior, which in turn affects the social environment.

Algorithms can be biased if they are based on incomplete data or if different perspectives are not considered. It can already be affirmed that the main problem law faces is the lack of regulation for the development of ethical, but mainly legal, issues that come with these technologies. This is how the law, being “a set of rules that control the conduct of men” (Carnelutti, 2018, p. 3), must offer a limitation for the functioning of these AIs; as tools they are excellent, but as weapons they can be fatal, “their improper use, intentional or not, can also damage people’s rights” (Carnelutti, 2018, p. 3). Ethical and legal issues debate the allocation of responsibilities and obligations in situations involving intelligent systems (Grigore, 2022).

To establish a starting point, AI, as seen from the Turing concept (developed in the previous title), can potentially compromise individual rights, including privacy, intellectual property, equality, and labor rights, among others. Thus, the union of these rights gives rise to fundamental guarantees, which must be protected, as they are derived from the dignification of the human being through struggles and evolution itself.

Law cannot be taken merely as a limiting norm but must also address collective advancement; it must be appropriate to the context. Thus, “law is a social phenomenon, and society is a different object from nature because it comprises a completely different network of elements” (Kelsen, 2011, p. 41). In this sense, it becomes clear that the social phenomenon represents human behavior, which changes over time, and it is the duty of the latter to adapt to and protect from the same evolution what is, by nature, the property of man, such as his fundamental rights.

Thus, it is the duty of law to begin to protect human rights, for although many belong to man by nature, others have been the result of a struggle. “Every right in the world had to be acquired by struggle” (Von Ihering, 2015, p. 40-60). Moreover, for the protection of these, it is necessary to establish criteria that go beyond grammatical and interpretative systems, and contrary to these, limited conduct responds to personal freedoms. It regulates behaviors that have “objective meaning that is linked to the act, and the meaning it has” (Kelsen, 2011, p. 41). This is to set aside the mere narrativization of conduct and begin to truly protect rights, as Kelsen stated within the real utilities of law.

Therefore, the lack of regulation of AIs poses another challenge for the law, which is to address the potential human rights violations that may occur through their use. This is because, by not limiting the development of AIs and not regulating their ethical and legal use, there is no guarantee of transparency in their use; in other words,



Als acquire autonomy, which can lead to their algorithms violating rights, both consciously and unconsciously.

In order to understand the above, the case of Tay will be taken as an example:

Tay is a bot for Twitter developed by Microsoft (a bot is a program that executes tasks on the internet), capable of automatically interacting with users and learning from them. In a few hours, Tay learned racist, xenophobic, misogynistic, and fascist expressions and had to be blocked from the social network (Grigore, 2022, p. 165).

It is challenging to make use of AI when the value of these technologies is inclined to ignore respect for other users, not by creation, but by algorithmic data collection and the omission of transparent data collection models; a situation that has left a clear precedent for the use of AI and the vulnerability of users and their rights when it comes to their use. It is clear that the violation of these guarantees in many cases is unintentional, but their existence cannot be ignored.

There must be a sense of equality among developers and creators of intelligence. However, they must also create methods for selecting information, not radicalizing topics, but rather contexts. In other words, AI must be an impartial entity, in which respect for equality and diversity stand out; this is the way for systems to limit themselves to adopting the necessary information, but to discard the prejudices represented by the mass of the population.

In this understanding, it is clear that the purpose of AI is not to offend anyone, much less to violate rights in general; on the contrary, it aims to facilitate human activity and existence in general, but "in order to fulfil this task, to behave like humans, to place people at the center of the development of new technologies, any solution, any regulation, must be based on respect for human rights" (Türk, 2023).

The law must adapt to the rapid evolution of Als; however, currently, only a limited number of countries have regulated this issue. By 2024, the United Nations (UN) General Assembly adopted a "historic solution on the promotion of 'safe and reliable' artificial intelligence (AI) systems that also benefit sustainable development for all" (UN, 2024).

However, even though the scope of AI is beginning to regulate, it is also necessary to understand that there will continue to be harm. One of these is the aspect of the right to privacy and data protection, as we must not lose sight of the fact that these intelligences work through the collection of algorithm information, a circumstance that, on the part of Als could undermine people's autonomy and freedom, as well as expose them to risks such as manipulation and discrimination.



Regarding the latter, it can be argued that discrimination is one of the primary violations that AIs exhibit. It is not against their development per se, but against the algorithm that prioritizes unfiltered adoption of data, thereby taking personal biases into account. This poses a significant challenge to justice and the protection of fairness and equality, presenting severe problems for the criminal justice system, fundamental guarantees, and access to employment, among others.

Work and economic acquisition are other challenges that the law will face. For it is no riddle that many of the AIs currently being developed are ultimately intended to replace human tasks. This situation would leave many workers or laborers both jobless and economically helpless. The industry will produce more goods and services with AI than with human labor; a point that, beyond technological advancement, results in a deterioration of human dignity.

Ultimately, to address the various challenges posed by AI, a comprehensive legal framework must be implemented, accompanied by clear context and a focus on the ethical use of AI. These rules should focus primarily on implementing transparent means for collecting algorithm data that respects diversity, equity, and privacy, among other values. However, the implementation of these technologies should be designed and regulated to benefit humans rather than harm them.

Human rights as an interpretative framework for AI

Human rights have various definitions; however, there is a meeting point in their conceptualization, and it is that "human rights are norms that recognize and protect the dignity of all human beings" (Unicef, 2015). In this understanding, it can also be understood that human rights are a set of rules and principles that lead to norms, which focus on guaranteeing the dignity, freedom and equality of all people "without distinction of any kind, such as race, sex, nationality, ethnic origin, language, religion or other status" (UN, 2023).

Human rights have five characteristics that articulate their existence: "they are rights, first, moral, second, universal, third, fundamental, fourth, abstract, and fifth, in terms of moral validity, they have priority over all other norms" (Alexy, 2015, p. 194). AIs must initially respond to the interpretation and guarantee of these universal mandates. Although their evolution has been beneficial for existence, it is also a reality that no limits have been placed on them, as stated in the previous title. These limits must be regulated in light of human rights, which serve as the basis for all regulation.

To talk about human rights, according to the High Commissioner for Human Rights, one must talk about:



Risks, with a focus on self-regulation and self-assessment by AI developers. Instead of adhering to detailed rules, risk-based regulation emphasizes identifying and mitigating risks to achieve results (Türk, 2023).

Thus, to regulate the application, operation, creation, and development of AI, one must begin to respect moral rights. This means that “moral rights represent more than individual will and could not exist if social life played no role” (Dávila, 2014, p. 20). Norms must address a broad social field, such as a population, but their application must be between autonomous individuals; disrespect for these mandates can break individual fundamental rights.

To complement the above, there is the case of deepfake or fake images, of which, in recent times, different women, especially those with a public image, have been victims. These are “videos in which false images are shown, usually of a person’s face, which appear to be real, and which have been produced using artificial intelligence” (Visus, 2021). Through this, content has been created mainly with sexual themes, which have had repercussions on the personal lives of those who falsely appear in the reproduction; thus, generating a violation of human rights and their moral themes.

On another point, the universality of human rights must be established, and this is where the responsibility of AI becomes necessary. AI “can create the basis for designing even more powerful tools for societal control, surveillance, and censorship” (Türk, 2023), which can be detrimental to states at war, in internal and external conflicts, with totalitarian and arbitrary rulers, and as the UN High Commissioner for Human Rights, Volker Türk, mentions: “can become vehicles for mass surveillance in our public spaces, ending any concept of privacy” (2023).

The aforementioned responds to the basis of human rights, materialized within states, i.e., fundamental rights. The fact that the use of AIs is not regulated also means that violations of fundamental rights will occur within each State; this is evident in the personal aura of each individual, as exemplified by the cases mentioned above, including discrimination, political participation, civil liberties, and access to public services.

Therefore, in terms of control and respect for fundamental rights, as a materialization of human rights within each State, it is necessary for:

All states must protect people from AI-induced human rights abuses, which means aligning their regulatory frameworks with their obligations under human rights law (UN, 2023).

Therefore, each State must legislate what is necessary for the protection of these rights, with the understanding that despite the existence of global measures, these have to be grounded in each specific territory, thus fulfilling the abstraction of



human rights, which occurs when “we idealize human beings, we assign them a series of adjectives and we define them as a desirable profile that should be attended to” (Durán, 2016, p. 75–81).

Nowadays, the majority of people worldwide have access to technological elements, including AI. Understanding that not all cultures are the same, it is necessary to regulate access to AI and its development according to the needs and management of these in each territory; it is not the same to generate a regulation in the United States, where its progress is abysmal, as in an African country where technology and internet progress is an innovation. “Existing regulations and protections must be applied, for example, regulatory frameworks on data protection, competition law, as well as sectoral regulations, including in the fields of healthcare, technology, or financial markets” (Türk, 2023).

Moreover, it is here that the last point for interpreting human rights must be addressed, as this is the priority that this regulation must have over the other rules. Thus, as a guarantee of human dignity, AI developers and creators must ensure that, in every algorithm, respect for human rights is paramount, thus avoiding transgressions based on race, gender, and other factors, in the words of Volker Türk:

The human rights framework provides a fundamental basis that can facilitate protections when employing efforts to exploit the enormous potential of AI, while preventing and mitigating its enormous implicit risks (Türk, 2023).

It is for all of the above that Artificial Intelligences must respond to human needs, properly speaking. It must be a tool to help, which must be a guarantor of human rights, and not, on the contrary, infringe upon them. Indeed, the use of these tools will always create new debates. However, the important thing about them is that, from their very development, the objective should be respect for rights and the harmonious existence of the community. A human rights perspective applied to the development and use of AI will have limited impact if it is not accompanied by adequate respect for human rights in the broader regulatory and institutional landscape (Türk, 2023).

Conclusion

The theoretical importance of human rights in the development of AIs lies in the need to seek respect for dignity, equity, and privacy in the use of these new technologies. Likewise, it aims to provide a starting point for states to base their regulations on, regarding the use, creation, and development of AIs. The advancement of intelligence cannot be restricted; however, it is necessary to regulate it in order to ensure



the responsible use of technologies and promote social harmony, non-discrimination, freedom, and respect for individual differences.

Disclaimer

The authors declare no potential conflict of interest related to the article. No artificial intelligence content generation tools were used in its preparation.

About the authors

Sergio Andrés López Zamora is a Lawyer and Legal Conciliator from Santo Tomás University. He holds a Postgraduate Degree in Virtual Education from the National University of Quilmes and a Postgraduate Degree in Legal Sciences with an emphasis on Criminal Law from the University of Buenos Aires; Specialist in Criminal Law and Criminal Procedure from Santo Tomás University and Candidate for a Specialization in Criminal Cassation from Gran Colombia University; Master's Degree in Criminal Law and Criminal Procedure from Santo Tomás University and Master's Degree in Human Rights from the Pedagogical and Technological University of Colombia; PhD in Public Law from Santo Tomás University and PhD candidate in Criminal Law at the University of Buenos Aires. He has 12 years of litigation experience in criminal law and human rights. He teaches undergraduate and postgraduate courses at Santo Tomás University (Bogotá and Tunja), Luis Amigó Catholic University (Medellín), and the Pedagogical and Technological University of Colombia (Tunja). Member of the Criminal Cassation Lawyers' Association.

<https://orcid.org/0000-0003-1350-6310> - sergio.lopezz@usantoto.edu.co

Valentina Hernández Chinome is a Lawyer graduated from Santo Tomás University, Tunja Branch.

<https://orcid.org/0009-0006-6468-1679> - valentina.hernandez@usantoto.edu.co

References

- Alexy, R. (2015). *Un concepto no positivista de derecho fundamental. Sobre la relación entre teoría de los principios, derechos fundamentales y mora sobre la relación entre teoría de los principios, derechos fundamentales y moral*. Fundación Manuel Giménez Abad.
- Bellman, R. E. (1978). *An Introduction to Artificial Intelligence: Can Computers Think?* Boyd & Fraser Publishing Company.
- Carnelutti, F. (2018). *Cómo nace el derecho*. Temis.
- Charniak, E. & McDermott, D. (1985). *Introducción a la Inteligencia Artificial*. Addison-Wesley.
- Dávila, J. (2014). Derechos Humanos en tanto derechos morales: dos concepciones. *Ius et Praxis*, 20(2), 495-524. <https://dx.doi.org/10.4067/S0718-00122014000200015>



- Durán, J. (2016). Derechos Humanos. Abstracción, homogeneización dominación. *Revista Electrónica Científica de Investigación Educativa*, 3(1), 75-81.
- Grigore, A (2022). Derechos humanos e inteligencia artificial. *Revistas Científicas*, 8(1), 165-175. <https://doi.org/10.12795/IESTSCIENTIA.2022.i01.10>
- Haugeland, J. (Ed.). (1985). *Artificial Intelligence: The Very Idea*. MIT Press.
- Kelsen, H. (2011). *Teoría pura del derecho, introducción a los problemas de las ciencias jurídicas*. Editorial Trotta.
- Kurzweil, R. (1990). *The Age of Intelligent Machines*. MIT Press.
- Morán Espinosa, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 15(48), 289-323. <https://doi.org/10.35487/rius.v15i48.2021.706>
- Nilsson, Nueva Jersey (1998). *Inteligencia artificial: una nueva síntesis*. Morgan Kaufmann.
- United Nations (2023). *La inteligencia artificial requiere una gobernanza basada en los derechos humanos*. <https://news.un.org/es/story/2023/11/1526062>
- United Nations (2024). *La Asamblea General adopta una resolución histórica sobre la IA*. <https://news.un.org/es/story/2024/03/1528511>
- Poole, D., Mackworth, A., & Goebel, R. (1998). *Inteligencia computacional: un enfoque lógico*. Oxford University Press.
- Rich, E. & Knight, K. (1991). *Artificial Intelligence*. McGraw-Hill.
- Russell, S. (2008). *Inteligencias Artificial Un Enforque Modernos*. Pearson.
- Torra, V. (2019). *Que es la inteligencia artificial*. Universitat Oberta de Catalunya.
- Türk, V. (2023). *La inteligencia artificial debe tomar como base los derechos humanos, declara el Alto Comisionado*. <https://tinyurl.com/48u9h4by>
- Unicef (2015). *¿Qué son los derechos humanos?* <https://tinyurl.com/ycptaysx>
- Visus, A. (2021). *Que es un Deep fakes, cómo se crean, cuáles fueron los primeros y su futuro*. <https://tinyurl.com/5xx8f86z>
- Von Ihering, R. (2015). *La lucha por el derecho*. Temis.
- Winston, P. (1992). *Inteligencia Artificial*. Addison-Wesley.



Brújula. Semilleros de Investigación

Volume 13, Number 25, January–June, pp. 4–15

Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.175>

DOSSIER

The AI dilemma: How does Artificial Intelligence affect Human Rights?

Sergio Andrés López Zamora 

Valentina Hernández Chinome 

Universidad Santo Tomas Seccional Tunja, Colombia

ABSTRACT

This article analyses the prevalence of human rights in the development of Artificial Intelligence (AI), approaching it from a historical and conceptual review of AI, evaluating its evolution and the impact it has had on society. It highlights how AI has advanced significantly and has been integrated into multiple aspects of human life, facilitating complex tasks and being efficient in various fields; however, it is essential to raise the challenges regarding how it impacts human rights, and the need to establish robust legal and ethical frameworks to regulate its accelerated development and use.

KEYWORDS:

automatic reasoning; globalization; human evolution; regulation; society; specialty; tools.

HOW TO CITE (APA):

López Zamora, S. A., & Hernández Chinome, V. (2025). The AI dilemma: How does Artificial Intelligence affect Human Rights? *Revista Brújula de Investigación*, 13(25), 4–15.

<https://doi.org/10.21830/23460628.175>

Received: April 15, 2025 **Accepted:** June 20, 2025

Contact: Valentina Hernández Chinome  valentina.hernandez@usantoto.edu.co



Introduction

During human evolution, humans have had to live in society to ensure their survival. Based on this end, each subject has been entrusted with different tasks, giving rise to work and specialization; however, this division of labor has intrinsically brought with it a solution to the need to meet social requirements, thereby guaranteeing harmonious coexistence and the survival of the species.

Through work, humans have dignified their existence and given it value, engaging in various activities, some of which are more complex than others. However, despite the above, each individual has sought ways to facilitate their work, making use of their instinct for creating tools, just as they have used to create their tools.

That advance is in line with collective activities and needs. The gadgets created have facilitated production and, with it, existence itself, reaching previously unthinkable points; so much so that today we have intangible tools that develop highly complex tasks, and their development continues to advance, as in the case of Artificial Intelligence.

The development of Artificial Intelligence (henceforth referred to as AI) has provided individuals with a tool for accessing the world in its entirety. This has also raised several ethical and legal questions, particularly regarding human rights. On the one hand, AIs offer the community considerable benefits in terms of convenience, speed of access to information, efficiency, and innovation. On the other hand, challenges arise that must be addressed to ensure respect and protection of users' fundamental rights.

In this sense, the question arises: What is the theoretical importance of human rights in the development of AIs? This question provides an analysis that will be developed under the following headings:

The age of Artificial Intelligence

AIs are not a creation of the 21st century; on the contrary, they have been developed since time immemorial. According to Vicenç Torra (2019), "The term artificial intelligence (AI) was adopted during the summer of 1956 in Dartmouth at a meeting that brought together researchers interested in the topics of intelligence, neural networks, and automata theory" (p.7). This circumstance makes it possible to establish that AI is not a recent phenomenon, but rather a thought and idea that has been evolving throughout the annals of history. It is only at a certain point in history, not very distant, that it is given a name of its own.

The rapid advance of AI has marked a new moment in human history. It gives rise to a new beginning in which humanity accesses information and technological tools



instantly, according to its needs. These new intelligences have experienced significant advances, mainly in recent years, resulting in access to sophisticated algorithms that offer substantial data processing capacity, as well as a vast array of information.

Despite the advances it has presented, it has been highly complex to define what an AI is objectively; however, “four approaches have been followed throughout history. As might be expected, there is a clash between human-centred and rationality-centred approaches” (Russell, 2008, p.30).

Among the early approaches to defining AIs, the first two focus on the human. A division is made between concepts, the first to analyse part of the system that thinks like a human: “the new and exciting endeavour to make computers think... machines with minds, in the broadest literal sense” (Haugeland, 1985). This is complemented by “the automation of activities that we link to human thought processes, activities such as decision making, problem solving, learning... (Bellman, 1978)”.

The second concept examines systems that behave like humans. It defines AI as “the art of developing machines capable of performing functions that when performed by humans require intelligence” (Kurzweil, 1990). It also states that it is “the study of how to get computers to perform tasks that, for the moment, humans do best” (Rich & Knight, 1991). This is how one can begin to think of AI as the need to bring some human intelligence to everyday tools.

It then becomes clear that the starting point of AI is the human being, their behavior, thinking, and acting; their whole being, intelligence analysis, and knowledge construction, the latter two points giving way to the next approach to the concept of AI.

The second approach to AI focuses on reasoning. Like the previous one, the concept focuses on two points: the first point is systems that reason. This is based on the definition that AI is “the study of mental faculties through the use of computational models” (Charniak & McDermott, 1985). This is made possible through the “study of computations that make it possible to perceive, reason, and act” (Winston, 1992). A concept that satisfies the claims of the need for information required by humans to fulfil their daily obligations but provided using a pre-coded algorithm.

The second point of reasoning lies in systems that act rationally. This item highlights the fact that AI is a creation that must focus on overcoming intelligence, specifically: “Computational Intelligence is the study of the design of intelligent agents” (Poole et al., 1998).

For researchers and authors interested in defining AI for this new era, an absolute concept has not yet emerged, as it depends on the starting point of analysis. However, even though the concepts are changing, some elements have remained con-



stant, such as thinking of AI as a system; the need for the system to take on human intelligence; the idea that these systems should serve as a tool for human beings but based on human reasoning and planning for it to work on its own, through a computer or technological element.

Thus, AI should be understood as a system created by human beings that possesses intelligence capable of rationalizing actions through algorithms specifically encoded with a function, and whose operation materialized through technological instruments. "AI... is related to intelligent behavior in artefacts" (Nilsson, 1998). It is worth noting that in the 21st century, access to technological artifacts has become common, resulting in widespread access to AI for the broader community.

Over the last decade, access to technological elements has increased, resulting in the fact that almost everyone has a computer, a mobile phone, a tablet, and internet access. As we have been saying, to access an AI, it is only necessary to have a computer. This means that technology itself represents AI: an artefact with intelligence capable of instant rationalization, and which is available to a large percentage of human beings around the world.

The fact that every human being can nowadays have access to AI has meant that it must have specific characteristics, which must be approved. The primary need for AI is intelligence, which must be equal to or superior to that of a human being. To determine if it can make decisions, it must be subjected to the Turing Test, proposed by Alan Turing (1950).

Alan Turing proposed that: "if a computer program could fool a set of human judges into thinking it was human, then that program must be intelligent" (Angeles, 2019). The Turing test states that the system must have several features:

- Natural language processing to enable him/her to communicate successfully in English.
- Knowledge representation to store what is known or felt.
- Automatic reasoning to use stored information to answer questions and draw new conclusions.
- Machine learning to adapt to new circumstances and to detect and extrapolate patterns (Russell, 2008, p.31).

In trying to resemble human intelligence, in order to fulfill the above capabilities, AI must learn as humans do. It is in this way that Machine Learning is incorporated, which is a "method of data analysis that learns from experience, allowing computers to find hidden information without being explicitly programmed" (Angeles, 2019). However, despite this and as is recognizable throughout this analysis, AI evolves and



its elements with it; in such a way that the union of Deep learning is realized. Deep learning is a concept that emerged in 2010:

It aims to mimic a human neural network through artificial intelligence, deep learning as it is also known, which is based on the design of individual layers of connections that maintain communication with other layers of information subject to an unlimited amount of data that is used first individually and then generally, for a specific task (just like a human neural network), is an aspect of machine learning that was designed to expand the contexts in which it was applied (Morán, 2020, p. 281-322.

This is centered on the fact that, in this technological era, artefacts are beginning to feature AI, endowing objects (such as cars, computers, appliances, tools, and even accessories) with the ability to serve humans. This is a result of the technological quest and the need to upgrade items to perform increasingly complex tasks that only human intelligence can perform.

Thus, for this era, it is established that AI systems are evolving and endowed with human intelligence, created to facilitate the existence of subjects. Due to globalization, they must be able to serve everyone, which is why they are constantly advancing; however, it should be noted that the use and access to intelligence by different subjects are beginning to generate an ethical and social debate.

Although they are great tools for this new technological era, adapted to the needs of subjects in general, they can be used in a counterproductive way against a third party. Some thinkers, such as Volker Türk, the United Nations High Commissioner for Human Rights, have established that AI is the future of humanity, a change that will lead to economic, social, political and cultural globalization; on the contrary, others, such as Yuval Noah Harari, author of "Sapiens" and "Homo Deus", have stated that AI can threaten the work of the community, provoke mass unemployment and economic inequality. This extends to affecting human rights, which are fundamental guarantees for every individual.

Challenges for the law in the face of artificial intelligence

As mentioned, the new era of AI brings about technological advances, but these advances also raise legal issues. AI is a human creation that seeks perfection, but throughout history, it has been shown that perfect is not a universal term but a personal one; the example of the Second World War and its implications.

Thus, it cannot be denied that personal biases of each user can be found within the algorithms that feed AI. Indeed, AI learns empirically about human behavior, but this is where one of the many concerns begins to emerge: human behavior is not always



the most appropriate, and this leads to the AI adopting discriminatory, immoral, or unlawful behavior, which in turn affects the social environment.

Algorithms can be biased if they are based on incomplete data or if different perspectives are not considered. It can already be affirmed that the main problem law faces is the lack of regulation for the development of ethical, but mainly legal, issues that come with these technologies. This is how the law, being “a set of rules that control the conduct of men” (Carnelutti, 2018, p. 3), must offer a limitation for the functioning of these AIs; as tools they are excellent, but as weapons they can be fatal, “their improper use, intentional or not, can also damage people’s rights” (Carnelutti, 2018, p. 3). Ethical and legal issues debate the allocation of responsibilities and obligations in situations involving intelligent systems (Grigore, 2022).

To establish a starting point, AI, as seen from the Turing concept (developed in the previous title), can potentially compromise individual rights, including privacy, intellectual property, equality, and labor rights, among others. Thus, the union of these rights gives rise to fundamental guarantees, which must be protected, as they are derived from the dignification of the human being through struggles and evolution itself.

Law cannot be taken merely as a limiting norm but must also address collective advancement; it must be appropriate to the context. Thus, “law is a social phenomenon, and society is a different object from nature because it comprises a completely different network of elements” (Kelsen, 2011, p. 41). In this sense, it becomes clear that the social phenomenon represents human behavior, which changes over time, and it is the duty of the latter to adapt to and protect from the same evolution what is, by nature, the property of man, such as his fundamental rights.

Thus, it is the duty of law to begin to protect human rights, for although many belong to man by nature, others have been the result of a struggle. “Every right in the world had to be acquired by struggle” (Von Ihering, 2015, p. 40-60). Moreover, for the protection of these, it is necessary to establish criteria that go beyond grammatical and interpretative systems, and contrary to these, limited conduct responds to personal freedoms. It regulates behaviors that have “objective meaning that is linked to the act, and the meaning it has” (Kelsen, 2011, p. 41). This is to set aside the mere narrativization of conduct and begin to truly protect rights, as Kelsen stated within the real utilities of law.

Therefore, the lack of regulation of AIs poses another challenge for the law, which is to address the potential human rights violations that may occur through their use. This is because, by not limiting the development of AIs and not regulating their ethical and legal use, there is no guarantee of transparency in their use; in other words,



Als acquire autonomy, which can lead to their algorithms violating rights, both consciously and unconsciously.

In order to understand the above, the case of Tay will be taken as an example:

Tay is a bot for Twitter developed by Microsoft (a bot is a program that executes tasks on the internet), capable of automatically interacting with users and learning from them. In a few hours, Tay learned racist, xenophobic, misogynistic, and fascist expressions and had to be blocked from the social network (Grigore, 2022, p. 165).

It is challenging to make use of AI when the value of these technologies is inclined to ignore respect for other users, not by creation, but by algorithmic data collection and the omission of transparent data collection models; a situation that has left a clear precedent for the use of AI and the vulnerability of users and their rights when it comes to their use. It is clear that the violation of these guarantees in many cases is unintentional, but their existence cannot be ignored.

There must be a sense of equality among developers and creators of intelligence. However, they must also create methods for selecting information, not radicalizing topics, but rather contexts. In other words, AI must be an impartial entity, in which respect for equality and diversity stand out; this is the way for systems to limit themselves to adopting the necessary information, but to discard the prejudices represented by the mass of the population.

In this understanding, it is clear that the purpose of AI is not to offend anyone, much less to violate rights in general; on the contrary, it aims to facilitate human activity and existence in general, but "in order to fulfil this task, to behave like humans, to place people at the center of the development of new technologies, any solution, any regulation, must be based on respect for human rights" (Türk, 2023).

The law must adapt to the rapid evolution of Als; however, currently, only a limited number of countries have regulated this issue. By 2024, the United Nations (UN) General Assembly adopted a "historic solution on the promotion of 'safe and reliable' artificial intelligence (AI) systems that also benefit sustainable development for all" (UN, 2024).

However, even though the scope of AI is beginning to regulate, it is also necessary to understand that there will continue to be harm. One of these is the aspect of the right to privacy and data protection, as we must not lose sight of the fact that these intelligences work through the collection of algorithm information, a circumstance that, on the part of Als could undermine people's autonomy and freedom, as well as expose them to risks such as manipulation and discrimination.



Regarding the latter, it can be argued that discrimination is one of the primary violations that AIs exhibit. It is not against their development per se, but against the algorithm that prioritizes unfiltered adoption of data, thereby taking personal biases into account. This poses a significant challenge to justice and the protection of fairness and equality, presenting severe problems for the criminal justice system, fundamental guarantees, and access to employment, among others.

Work and economic acquisition are other challenges that the law will face. For it is no riddle that many of the AIs currently being developed are ultimately intended to replace human tasks. This situation would leave many workers or laborers both jobless and economically helpless. The industry will produce more goods and services with AI than with human labor; a point that, beyond technological advancement, results in a deterioration of human dignity.

Ultimately, to address the various challenges posed by AI, a comprehensive legal framework must be implemented, accompanied by clear context and a focus on the ethical use of AI. These rules should focus primarily on implementing transparent means for collecting algorithm data that respects diversity, equity, and privacy, among other values. However, the implementation of these technologies should be designed and regulated to benefit humans rather than harm them.

Human rights as an interpretative framework for AI

Human rights have various definitions; however, there is a meeting point in their conceptualization, and it is that "human rights are norms that recognize and protect the dignity of all human beings" (Unicef, 2015). In this understanding, it can also be understood that human rights are a set of rules and principles that lead to norms, which focus on guaranteeing the dignity, freedom and equality of all people "without distinction of any kind, such as race, sex, nationality, ethnic origin, language, religion or other status" (UN, 2023).

Human rights have five characteristics that articulate their existence: "they are rights, first, moral, second, universal, third, fundamental, fourth, abstract, and fifth, in terms of moral validity, they have priority over all other norms" (Alexy, 2015, p. 194). AIs must initially respond to the interpretation and guarantee of these universal mandates. Although their evolution has been beneficial for existence, it is also a reality that no limits have been placed on them, as stated in the previous title. These limits must be regulated in light of human rights, which serve as the basis for all regulation.

To talk about human rights, according to the High Commissioner for Human Rights, one must talk about:



Risks, with a focus on self-regulation and self-assessment by AI developers. Instead of adhering to detailed rules, risk-based regulation emphasizes identifying and mitigating risks to achieve results (Türk, 2023).

Thus, to regulate the application, operation, creation, and development of AI, one must begin to respect moral rights. This means that “moral rights represent more than individual will and could not exist if social life played no role” (Dávila, 2014, p. 20). Norms must address a broad social field, such as a population, but their application must be between autonomous individuals; disrespect for these mandates can break individual fundamental rights.

To complement the above, there is the case of deepfake or fake images, of which, in recent times, different women, especially those with a public image, have been victims. These are “videos in which false images are shown, usually of a person’s face, which appear to be real, and which have been produced using artificial intelligence” (Visus, 2021). Through this, content has been created mainly with sexual themes, which have had repercussions on the personal lives of those who falsely appear in the reproduction; thus, generating a violation of human rights and their moral themes.

On another point, the universality of human rights must be established, and this is where the responsibility of AI becomes necessary. AI “can create the basis for designing even more powerful tools for societal control, surveillance, and censorship” (Türk, 2023), which can be detrimental to states at war, in internal and external conflicts, with totalitarian and arbitrary rulers, and as the UN High Commissioner for Human Rights, Volker Türk, mentions: “can become vehicles for mass surveillance in our public spaces, ending any concept of privacy” (2023).

The aforementioned responds to the basis of human rights, materialized within states, i.e., fundamental rights. The fact that the use of AIs is not regulated also means that violations of fundamental rights will occur within each State; this is evident in the personal aura of each individual, as exemplified by the cases mentioned above, including discrimination, political participation, civil liberties, and access to public services.

Therefore, in terms of control and respect for fundamental rights, as a materialization of human rights within each State, it is necessary for:

All states must protect people from AI-induced human rights abuses, which means aligning their regulatory frameworks with their obligations under human rights law (UN, 2023).

Therefore, each State must legislate what is necessary for the protection of these rights, with the understanding that despite the existence of global measures, these have to be grounded in each specific territory, thus fulfilling the abstraction of



human rights, which occurs when “we idealize human beings, we assign them a series of adjectives and we define them as a desirable profile that should be attended to” (Durán, 2016, p. 75–81).

Nowadays, the majority of people worldwide have access to technological elements, including AI. Understanding that not all cultures are the same, it is necessary to regulate access to AI and its development according to the needs and management of these in each territory; it is not the same to generate a regulation in the United States, where its progress is abysmal, as in an African country where technology and internet progress is an innovation. “Existing regulations and protections must be applied, for example, regulatory frameworks on data protection, competition law, as well as sectoral regulations, including in the fields of healthcare, technology, or financial markets” (Türk, 2023).

Moreover, it is here that the last point for interpreting human rights must be addressed, as this is the priority that this regulation must have over the other rules. Thus, as a guarantee of human dignity, AI developers and creators must ensure that, in every algorithm, respect for human rights is paramount, thus avoiding transgressions based on race, gender, and other factors, in the words of Volker Türk:

The human rights framework provides a fundamental basis that can facilitate protections when employing efforts to exploit the enormous potential of AI, while preventing and mitigating its enormous implicit risks (Türk, 2023).

It is for all of the above that Artificial Intelligences must respond to human needs, properly speaking. It must be a tool to help, which must be a guarantor of human rights, and not, on the contrary, infringe upon them. Indeed, the use of these tools will always create new debates. However, the important thing about them is that, from their very development, the objective should be respect for rights and the harmonious existence of the community. A human rights perspective applied to the development and use of AI will have limited impact if it is not accompanied by adequate respect for human rights in the broader regulatory and institutional landscape (Türk, 2023).

Conclusion

The theoretical importance of human rights in the development of AIs lies in the need to seek respect for dignity, equity, and privacy in the use of these new technologies. Likewise, it aims to provide a starting point for states to base their regulations on, regarding the use, creation, and development of AIs. The advancement of intelligence cannot be restricted; however, it is necessary to regulate it in order to ensure



the responsible use of technologies and promote social harmony, non-discrimination, freedom, and respect for individual differences.

Disclaimer

The authors declare no potential conflict of interest related to the article. No artificial intelligence content generation tools were used in its preparation.

About the authors

Sergio Andrés López Zamora is a Lawyer and Legal Conciliator from Santo Tomás University. He holds a Postgraduate Degree in Virtual Education from the National University of Quilmes and a Postgraduate Degree in Legal Sciences with an emphasis on Criminal Law from the University of Buenos Aires; Specialist in Criminal Law and Criminal Procedure from Santo Tomás University and Candidate for a Specialization in Criminal Cassation from Gran Colombia University; Master's Degree in Criminal Law and Criminal Procedure from Santo Tomás University and Master's Degree in Human Rights from the Pedagogical and Technological University of Colombia; PhD in Public Law from Santo Tomás University and PhD candidate in Criminal Law at the University of Buenos Aires. He has 12 years of litigation experience in criminal law and human rights. He teaches undergraduate and postgraduate courses at Santo Tomás University (Bogotá and Tunja), Luis Amigó Catholic University (Medellín), and the Pedagogical and Technological University of Colombia (Tunja). Member of the Criminal Cassation Lawyers' Association.

<https://orcid.org/0000-0003-1350-6310> - sergio.lopezz@usantoto.edu.co

Valentina Hernández Chinome is a Lawyer graduated from Santo Tomás University, Tunja Branch.

<https://orcid.org/0009-0006-6468-1679> - valentina.hernandez@usantoto.edu.co

References

- Alexy, R. (2015). *Un concepto no positivista de derecho fundamental. Sobre la relación entre teoría de los principios, derechos fundamentales y mora sobre la relación entre teoría de los principios, derechos fundamentales y moral*. Fundación Manuel Giménez Abad.
- Bellman, R. E. (1978). *An Introduction to Artificial Intelligence: Can Computers Think?* Boyd & Fraser Publishing Company.
- Carnelutti, F. (2018). *Cómo nace el derecho*. Temis.
- Charniak, E. & McDermott, D. (1985). *Introducción a la Inteligencia Artificial*. Addison-Wesley.
- Dávila, J. (2014). Derechos Humanos en tanto derechos morales: dos concepciones. *Ius et Praxis*, 20(2), 495-524. <https://dx.doi.org/10.4067/S0718-00122014000200015>



- Durán, J. (2016). Derechos Humanos. Abstracción, homogeneización dominación. *Revista Electrónica Científica de Investigación Educativa*, 3(1), 75-81.
- Grigore, A (2022). Derechos humanos e inteligencia artificial. *Revistas Científicas*, 8(1), 165-175. <https://doi.org/10.12795/IESTSCIENTIA.2022.i01.10>
- Haugeland, J. (Ed.). (1985). *Artificial Intelligence: The Very Idea*. MIT Press.
- Kelsen, H. (2011). *Teoría pura del derecho, introducción a los problemas de las ciencias jurídicas*. Editorial Trotta.
- Kurzweil, R. (1990). *The Age of Intelligent Machines*. MIT Press.
- Morán Espinosa, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 15(48), 289-323. <https://doi.org/10.35487/rius.v15i48.2021.706>
- Nilsson, Nueva Jersey (1998). *Inteligencia artificial: una nueva síntesis*. Morgan Kaufmann.
- United Nations (2023). *La inteligencia artificial requiere una gobernanza basada en los derechos humanos*. <https://news.un.org/es/story/2023/11/1526062>
- United Nations (2024). *La Asamblea General adopta una resolución histórica sobre la IA*. <https://news.un.org/es/story/2024/03/1528511>
- Poole, D., Mackworth, A., & Goebel, R. (1998). *Inteligencia computacional: un enfoque lógico*. Oxford University Press.
- Rich, E. & Knight, K. (1991). *Artificial Intelligence*. McGraw-Hill.
- Russell, S. (2008). *Inteligencias Artificial Un Enforque Modernos*. Pearson.
- Torra, V. (2019). *Que es la inteligencia artificial*. Universitat Oberta de Catalunya.
- Türk, V. (2023). *La inteligencia artificial debe tomar como base los derechos humanos, declara el Alto Comisionado*. <https://tinyurl.com/48u9h4by>
- Unicef (2015). *¿Qué son los derechos humanos?* <https://tinyurl.com/ycptaysx>
- Visus, A. (2021). *Que es un Deep fakes, cómo se crean, cuáles fueron los primeros y su futuro*. <https://tinyurl.com/5xx8f86z>
- Von Ihering, R. (2015). *La lucha por el derecho*. Temis.
- Winston, P. (1992). *Inteligencia Artificial*. Addison-Wesley.



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, pp. 16-33


Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.174>

DOSIER

Inteligencia artificial y ciberdelincuencia: amenazas emergentes para la infancia y adolescencia en la era de los *deepfakes*?

Aldair Bueno Atencio 

Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad

RESUMEN

Este artículo analiza el impacto de herramientas basadas en IA, como los *deepfakes*, *deep nudes* y *deep voice*, en la generación de nuevas amenazas para menores de edad. A través de una revisión documental y el análisis de casos recientes, se identifican las principales conductas delictivas potenciadas por IA, así como los desafíos jurídicos y éticos que enfrenta el derecho penal para su persecución y sanción. Los resultados evidencian la creciente sofisticación de los ataques y la insuficiencia de los marcos normativos actuales, lo que subraya la necesidad de estrategias integrales de prevención, protección y actualización legislativa. Se concluye que la protección de los menores en entornos digitales exige un enfoque multidisciplinario y adaptativo.

PALABRAS CLAVE

adolescencia; ciberdelincuencia; derecho penal; falsificaciones profundas; infancia; inteligencia artificial

CITACIÓN APA

Bueno Atencio, A. (2025). Inteligencia artificial y ciberdelincuencia: amenazas emergentes para la infancia y adolescencia en la era de los *deepfakes*. *Revista Brújula de Investigación*, 13(25), 16-33.

<https://doi.org/10.21830/23460628.174>

Recibido: 15 de abril 2025 **Aceptado:** 20 de junio de 2025

Contacto: Aldair Bueno Atencio  info@ibdc.digital



Introducción

La revolución digital ha propiciado transformaciones profundas en la manera en que las sociedades interactúan, comunican y acceden a la información. Sin embargo, este avance tecnológico ha traído consigo desafíos inéditos, especialmente en el ámbito de la seguridad y la protección de los derechos fundamentales de los menores de edad. En los últimos años, la ciberdelincuencia ha evolucionado de manera vertiginosa, adoptando herramientas cada vez más sofisticadas, entre las que destaca la inteligencia artificial (IA) como catalizadora de nuevas formas de agresión y manipulación digital (Europol, 2022).

La infancia y la adolescencia constituyen grupos especialmente vulnerables en el entorno digital, no solo por su exposición temprana a las tecnologías de la información y la comunicación, sino también por la falta de madurez emocional y cognitiva para identificar y gestionar riesgos en línea (Livingstone & Stoilova, 2021). En este contexto, la aparición de los denominados *deepfakes*¹ —contenidos audiovisuales manipulados mediante IA para simular situaciones, voces o imágenes falsas con alto grado de realismo— ha inaugurado una nueva era de amenazas, donde la suplantación de identidad, la extorsión y la afectación de la reputación digital adquieren dimensiones inéditas (Chesney & Citron, 2019).

El fenómeno de los *deepfakes* y sus variantes, como los *deep nudes* y la *deepfake voice*, ha sido objeto de creciente preocupación en la literatura jurídica y tecnológica, debido a su potencial para vulnerar derechos fundamentales como la intimidad, la dignidad y la protección de datos personales de los menores (Maras & Alexandrou, 2019). Estas tecnologías permiten la creación y difusión de imágenes, videos o audios falsificados que pueden ser utilizados para acosar, extorsionar o manipular a niños y adolescentes, generando daños psicológicos, sociales y legales de difícil reparación.

A pesar de la gravedad del problema, los marcos normativos y las estrategias de prevención y persecución penal presentan importantes vacíos y limitaciones. El derecho penal, habitualmente reactivo y basado en la materialidad de la prueba, enfrenta el reto de adaptarse a un entorno donde la evidencia digital puede ser fácilmente manipulada y donde la autoría de los delitos se diluye en la complejidad de los algoritmos y el anonimato de la red (Brenner, 2010). Por ello, resulta imprescindible analizar no solo las conductas delictivas emergentes, sino también la capacidad de

1 El término *deepfake* se utiliza en este artículo para referirse a cualquier contenido audiovisual manipulado mediante inteligencia artificial —incluyendo imágenes, videos y audios— que simula situaciones o identidades falsas con alto grado de realismo.



respuesta del sistema jurídico y la necesidad de enfoques multidisciplinares que integren la tecnología, la educación y la protección social.

El presente artículo tiene como objetivo analizar el impacto de la inteligencia artificial en la ciberdelincuencia² dirigida contra la infancia y la adolescencia, con especial énfasis en el fenómeno de los *deepfakes*. Se parte de una revisión documental y el análisis de casos paradigmáticos para identificar las principales amenazas, los desafíos jurídicos y las posibles estrategias de prevención y protección. Se busca, así, contribuir a la comprensión integral de un fenómeno en constante evolución y a la formulación de propuestas que permitan fortalecer la protección de los menores en el entorno digital.

Marco teórico

La ciberdelincuencia, entendida como el conjunto de conductas ilícitas cometidas a través de medios informáticos o en el ciberespacio, ha experimentado una evolución significativa en las últimas décadas, impulsada por el desarrollo de nuevas tecnologías y la globalización de las comunicaciones digitales (Brenner, 2010). En este contexto, la inteligencia artificial (IA) se ha consolidado como un factor disruptivo, capaz de transformar tanto las estrategias de prevención y persecución del delito como las propias modalidades de comisión de conductas ilícitas³ (Europol, 2022).

Ciberdelincuencia y menores: un binomio de vulnerabilidad

La infancia y la adolescencia representan grupos especialmente expuestos a los riesgos del entorno digital. Diversos estudios han señalado que los menores, debido a su menor experiencia, madurez y capacidad crítica, son más susceptibles a ser víctimas de engaños, acoso, extorsión y manipulación en línea (Livingstone & Stoilova, 2021). La ciberdelincuencia dirigida contra menores abarca desde el ciberacoso y el *grooming* hasta la difusión no consentida de imágenes íntimas y la suplantación de identidad, fenómenos que se han visto agravados por la irrupción de la IA (UNICEF, 2021).

2 La ciberdelincuencia comprende todas aquellas conductas ilícitas que se cometen a través de medios informáticos o en el ciberespacio, afectando bienes jurídicos individuales o colectivos (Brenner, 2010).

3 La IA no solo ha potenciado la capacidad de los ciberdelincuentes, sino que también ha abierto nuevas posibilidades para la detección y prevención de delitos, lo que genera una carrera constante entre atacantes y defensores en el ciberespacio.



Inteligencia artificial: definición y aplicaciones en el ciberespacio

La IA puede definirse como el conjunto de sistemas o máquinas que, mediante algoritmos y grandes volúmenes de datos, son capaces de realizar tareas que normalmente requerían inteligencia humana, como el reconocimiento de patrones, la toma de decisiones o la generación de contenidos (Russell & Norvig, 2021). En el ámbito de la ciberseguridad, la IA se utiliza tanto para la detección y prevención de amenazas como para la automatización de ataques, la creación de *malware* adaptativo y la manipulación de información (Brundage et al., 2018).

***Deepfakes* y variantes: tecnologías emergentes de manipulación digital**

El término *deepfake* hace referencia a contenidos audiovisuales —principalmente videos, imágenes y audios— generados o alterados mediante técnicas de aprendizaje profundo (*deep learning*), que permiten simular con gran realismo la apariencia, voz o acciones de una persona (Chesney & Citron, 2019). Estas tecnologías han evolucionado rápidamente, dando lugar a variantes como los *deep nudes* (imágenes íntimas falsas generadas por IA) y la *deepfake voice* (imitación de voces humanas con fines de suplantación o extorsión) (Maras & Alexandrou, 2019).

La facilidad de acceso a herramientas de creación de *deepfakes* y la dificultad para detectar su falsedad han incrementado su uso en conductas delictivas, especialmente aquellas dirigidas a menores, como la difusión de imágenes íntimas falsas, el chantaje y la manipulación emocional (UNICEF, 2021; Europol, 2022).

Desafíos jurídicos y éticos en la protección de menores

El uso de IA en la ciberdelincuencia plantea retos significativos para el derecho penal y la protección de los derechos de los menores. Por un lado, la identificación y persecución de los responsables se complica debido al anonimato y la descentralización de las redes digitales. Por otro, la manipulación de pruebas digitales mediante *deepfakes* dificulta la labor probatoria y puede afectar la presunción de inocencia y el debido proceso (Maras & Alexandrou, 2019). Además, surgen dilemas éticos relacionados con la privacidad, la protección de datos y el consentimiento informado, especialmente en el caso de menores de edad (Livingstone & Stoilova, 2021).

Métodos

El presente artículo se fundamenta en una revisión documental de literatura científica, informes institucionales y casos paradigmáticos reportados en los últimos cinco años. Se emplea un enfoque cualitativo, orientado a identificar patrones, ten-



dencias y vacíos normativos en la protección de menores frente a la ciberdelincuencia potenciada por IA. Asimismo, se analizan las respuestas jurídicas y las propuestas de política pública formuladas a nivel internacional y regional.

La naturaleza compleja y multifacética del fenómeno estudiado —la intersección de la inteligencia artificial (IA), la ciberdelincuencia y la vulnerabilidad de la infancia— exige un enfoque metodológico que trascienda la mera cuantificación para adentrarse en la comprensión profunda de los procesos, significados y contextos. Por ello, esta investigación se fundamenta en un paradigma cualitativo-interpretativo, diseñado para explorar en detalle la naturaleza de las amenazas emergentes, los vacíos normativos y las implicaciones sociales de la ciberdelincuencia potenciada por IA. El diseño metodológico se articuló en tres fases principales, secuenciales y complementarias: una revisión documental sistemática, un estudio de casos múltiples y un análisis jurídico-doctrinal, culminando en una síntesis integradora.

Paradigma y enfoque metodológico

Se adoptó un paradigma cualitativo-interpretativo, ya que el objetivo principal no era medir la prevalencia estadística del fenómeno —una tarea casi imposible dada la “cifra oscura” del delito—, sino comprender su “cómo” y su “porqué”. Este enfoque permite explorar la riqueza y la complejidad de las interacciones entre tecnología, comportamiento delictivo y respuesta social, interpretando los datos dentro de su contexto sociolegal. El diseño específico es el de una investigación documental y de estudio de casos múltiples, una combinación que permite, por un lado, obtener una visión panorámica y fundamentada del estado del arte (a través de la revisión documental) y, por otro, aterrizar los conceptos abstractos en realidades concretas y analizables (a través de los casos).

Fase 1: Revisión documental sistemática

Esta fase inicial constituyó el pilar sobre el que se construyó toda la investigación. Su propósito fue doble: establecer un marco teórico robusto y mapear el conocimiento existente para identificar tanto las certezas consolidadas como las lagunas de investigación.

Estrategia de búsqueda y fuentes de información

Se diseñó una estrategia de búsqueda exhaustiva para minimizar el riesgo de omitir literatura relevante. La búsqueda se realizó entre enero y marzo de 2024, para incluir un periodo de publicación de los últimos cinco años (2019-2024) y así asegurar la máxima actualidad en un campo tecnológico de evolución vertiginosa. Las fuentes consultadas se dividieron en tres categorías:



- Bases de datos académicas: se realizaron búsquedas sistemáticas en Scopus, Web of Science, Google Scholar, IEEE Xplore y ACM Digital Library para la literatura científica y técnica. Para la literatura jurídica y de ciencias sociales, se consultaron bases como Westlaw, LexisNexis, HeinOnline y ProQuest.
- Repositorios institucionales y de "literatura gris": se llevó a cabo una búsqueda manual en los portales web de organizaciones intergubernamentales y no gubernamentales clave, como Europol, Interpol, UNICEF, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Unión Internacional de Telecomunicaciones (ITU), y ONG especializadas como ECPAT International y Thorn. Esta "literatura gris" (informes, evaluaciones, guías) es fundamental, ya que a menudo contiene los datos más actualizados y prácticos sobre tendencias delictivas.
- Fuentes gubernamentales: se revisaron portales legislativos y de agencias de ciberseguridad de diversas jurisdicciones (p. ej., ENISA en la UE, CISA en EE. UU.) para identificar informes y alertas relevantes.

La ecuación de búsqueda se construyó combinando descriptores clave mediante operadores booleanos (AND, OR) y truncamientos (). *Una cadena de búsqueda representativa fue: ("inteligencia artificial" OR "IA" OR "deepfake" OR "machine learning") AND ("ciberdelincuencia" OR "ciberacoso" OR "grooming" OR "sextorsión") AND ("menor*" OR "niño*" OR "infancia" OR "adolescenc*") AND ("derecho penal" OR "legislación" OR "protección").*

Criterios de inclusión y exclusión

Para garantizar la calidad y pertinencia del corpus documental, se aplicaron criterios estrictos:

- Criterios de inclusión: se incluyeron artículos científicos revisados por pares, libros y capítulos de libro, informes institucionales, legislación y jurisprudencia relevante, y tesis doctorales que abordaran directamente la intersección de los tres ejes temáticos. Se priorizaron los documentos en español e inglés.
- Criterios de exclusión: se excluyeron artículos de opinión sin fundamento empírico o teórico, noticias de prensa no verificadas o de medios no especializados, blogs, foros de internet y literatura puramente técnica sobre algoritmos de IA que no abordaran sus implicaciones sociales, éticas o legales.



El proceso de cribado se realizó en dos etapas: primero, una revisión de títulos y resúmenes para descartar los documentos claramente irrelevantes; segundo, una lectura completa de los documentos preseleccionados para confirmar su adecuación final.

Fase 2: Estudio de casos múltiples

Mientras la revisión documental proporcionó la amplitud, el estudio de casos aportó la profundidad necesaria para comprender cómo se manifiestan estas amenazas en la práctica.

Justificación y selección de casos

Se optó por un diseño de estudio de casos múltiples para permitir la comparación entre ellos, identificar patrones comunes y diferencias significativas, y aumentar la robustez de las conclusiones. Los casos no se seleccionaron con el fin de una generalización estadística, sino por su valor paradigmático, es decir, su capacidad para ilustrar de manera clara y potente las dinámicas del fenómeno estudiado. Los criterios para la selección de casos fueron:

- **Riqueza informativa:** casos que estuvieran suficientemente documentados en fuentes confiables (informes policiales desclasificados, sentencias judiciales, reportajes de investigación periodística de medios reconocidos) para permitir un análisis detallado.
- **Relevancia paradigmática:** casos que ejemplificaran claramente el uso de una tecnología de IA específica (*deepfake*, clonación de voz, etc.) en la comisión de un delito contra un menor.
- **Diversidad tipológica y geográfica:** se buscó una muestra de casos que reflejaran diferentes tipos de delitos (acoso, extorsión, abuso sexual), diferentes plataformas digitales implicadas y diferentes contextos jurisdiccionales para observar variaciones en la respuesta legal.

Protocolo de análisis de caso

Para asegurar la consistencia y el rigor en el análisis, se desarrolló un protocolo estandarizado que se aplicó a cada caso. Este protocolo funcionó como una plantilla para la extracción y organización de la información, cubriendo las siguientes dimensiones:

Descripción fáctica: narrativa detallada de los hechos.

- **Actores involucrados:** perfil anonimizado de la víctima (edad, género) y del agresor (individuo, grupo, motivaciones).



- Componente tecnológico: identificación de la herramienta o técnica de IA específica utilizada y su rol en el delito.
- Vector de ataque: plataforma o medio digital a través del cual se perpetró el ataque (redes sociales, aplicaciones de mensajería, etc.).
- Impacto documentado: consecuencias para la víctima (psicológicas, sociales, académicas) según lo reportado.
- Respuesta institucional: acciones tomadas por las fuerzas de seguridad, fiscales y tribunales.
- Desenlace y lecciones aprendidas: resultado del proceso legal (si lo hubo) y reflexiones clave extraídas del caso.

Fase 3: Análisis jurídico-doctrinal

Esta fase se centra en evaluar la capacidad de respuesta del ordenamiento jurídico frente a los desafíos identificados. El análisis se dividió en dos vertientes:

- Análisis normativo (*lex lata*): un examen del derecho vigente. Se revisaron instrumentos internacionales (p. ej., Convenio de Budapest sobre la Ciberdelincuencia, Convención sobre los Derechos del Niño), legislación regional (p. ej., Directiva de la UE sobre la lucha contra el abuso sexual de los niños, Ley de Servicios Digitales) y legislaciones nacionales de jurisdicciones seleccionadas. El objetivo era identificar qué figuras delictivas existentes podrían aplicarse y dónde residían los principales vacíos o ambigüedades legales.
- Análisis doctrinal (*lex ferenda*): un estudio de las propuestas y debates académicos sobre cómo debería evolucionar el derecho. Se analizaron artículos en revistas jurídicas especializadas y monografías que discutían problemas de tipificación, cuestiones probatorias (la admisibilidad y valoración de la evidencia digital manipulable) y la atribución de responsabilidad penal en entornos complejos mediados por algoritmos.

Integración de datos y síntesis

La fase final consistió en un proceso de triangulación metodológica, donde los hallazgos de cada una de las tres fases se pusieron en diálogo para construir una comprensión holística. Los patrones identificados en la revisión documental fueron ilustrados y validados con los datos de los casos de estudio, y ambos fueron interpretados a la luz de los desafíos y posibilidades reveladas por el análisis jurídico-doctrinal. Esta síntesis integradora es la que forma el núcleo de las secciones de Resultados y Discusión de este artículo.



Discusión

Los resultados presentados en la sección anterior dibujan un panorama inquietante y complejo. La convergencia entre la inteligencia artificial (IA) y la ciberdelincuencia ha dejado de ser una hipótesis futurista para convertirse en una realidad tangible que impacta de manera desproporcionada a uno de los colectivos más vulnerables de la sociedad: la infancia y la adolescencia. La presente discusión se propone desentrañar las múltiples capas de este fenómeno, interpretando los hallazgos en un contexto más amplio, dialogando críticamente con la literatura existente, reconociendo las limitaciones del estudio y, finalmente, proyectando las implicaciones de estos hallazgos hacia el futuro del derecho, la tecnología y la protección de menores.

Interpretación integral de los resultados: la sinergia entre IA y vulnerabilidad infantil

Los hallazgos de esta investigación no deben interpretarse como un simple listado de nuevas herramientas en el arsenal de los ciberdelincuentes. Lo que se evidencia es una transformación cualitativa de la amenaza. La IA no solo facilita la comisión de delitos ya conocidos, como el ciberacoso o la extorsión, sino que redefine su naturaleza, escala e impacto.

De la herramienta a la amenaza sistémica: la escalabilidad y personalización del daño

Tradicionalmente, delitos como la difamación o la creación de material pornográfico falso requerían un esfuerzo técnico y temporal considerable. La IA, a través de los *deepfakes*, ha demolido estas barreras. La capacidad de generar contenido falso de alta calidad de manera automatizada y a gran escala representa un cambio de paradigma (Brundage et al., 2018). Un agresor ya no necesita habilidades de edición de video; solo requiere acceso a un *software*, a menudo disponible gratuitamente o a bajo costo, y una imagen de la víctima obtenida de una red social. Esta “democratización” de la capacidad de generar desinformación y contenido malicioso es, quizás, el aspecto más alarmante.

Además, la IA permite una personalización del ataque sin precedentes. Los algoritmos pueden analizar los perfiles en línea de los menores para adaptar los mensajes de *grooming* o las tácticas de extorsión a sus intereses, miedos e inseguridades específicas, aumentando la probabilidad de éxito del delincuente (Europol, 2022). Esta personalización convierte cada ataque en una experiencia singularmente traumática, diseñada para explotar las vulnerabilidades psicológicas del individuo. El delito deja de ser genérico para convertirse en un ataque “quirúrgico” a la psique del menor.



El impacto psicosocial amplificado: la erosión de la identidad y la confianza

El daño causado por estas nuevas formas de ciberdelincuencia trasciende lo meramente reputacional. Para un adolescente, cuya identidad está en pleno proceso de construcción y es altamente dependiente de la validación social, la difusión de un *deep nude* o un video humillante puede ser devastadora (Livingstone & Stoilova, 2021). La víctima no solo se enfrenta a la vergüenza y al ostracismo, sino también a una profunda crisis de identidad. La imagen digital, que es una extensión de su yo, ha sido secuestrada, violada y redefinida sin su consentimiento. Este fenómeno puede generar secuelas psicológicas graves y duraderas, como trastorno de estrés postraumático, ansiedad social, depresión e ideación suicida (UNICEF, 2021).

Más allá del impacto individual, los *deepfakes* erosionan un pilar fundamental de la interacción social: la confianza en la evidencia sensorial. Como señalan Chesney y Citron (2019), nos adentramos en una era donde “ver ya no es creer”. Esta devaluación de la prueba audiovisual tiene consecuencias profundas. Un menor víctima de un *deepfake* no solo debe lidiar con el contenido falso, sino también con la dificultad de demostrar su inocencia. A la inversa, un agresor real podría alegar que el video que lo incrimina es un *deepfake*, explotando lo que se ha denominado el “dividendo del mentiroso”. Esta incertidumbre epistémica genera un entorno de sospecha generalizada que puede paralizar la capacidad de respuesta de las familias, los centros educativos y las propias autoridades.

El desafío a la realidad y la evidencia digital: implicaciones para el sistema judicial

El sistema de justicia penal se fundamenta en la capacidad de establecer hechos a través de pruebas confiables. La irrupción de los *deepfakes* representa un desafío existencial para este principio. Como advierten Maras y Alexandrou (2019), la autenticación de la evidencia digital se convierte en un campo de batalla técnico y forense de alta complejidad. ¿Cómo puede un juez o un jurado, sin formación técnica especializada, valorar la autenticidad de un video o un audio? La carga de la prueba podría invertirse *de facto*, obligando a la víctima a demostrar que un contenido es falso, en lugar de que el acusador demuestre que es real.

Esto plantea la necesidad urgente de desarrollar nuevos estándares forenses y protocolos de autenticación de evidencia digital. Sin embargo, nos encontramos en una carrera armamentística asimétrica: mientras las tecnologías de generación de *deepfakes* avanzan a un ritmo exponencial, las herramientas de detección siempre irán un paso por detrás. Cualquier método de detección basado en artefactos visuales o inconsistencias puede ser, eventualmente, superado por algoritmos de gene-



ración más avanzados. Esta realidad obliga a repensar la centralidad de la prueba audiovisual en los procesos judiciales y a buscar formas de corroboración a través de otros medios probatorios.

Diálogo con la literatura existente, conflictos y hallazgos inesperados

Los resultados de esta investigación no surgen en el vacío, sino que dialogan, confirman y, en ocasiones, matizan las predicciones y análisis de la literatura académica e institucional previa.

Confirmación y expansión de las tesis previas

El análisis confirma las advertencias tempranas de autores como Brundage et al. (2018) sobre el potencial uso malicioso de la IA. Lo que en 2018 era una previsión, hoy es una realidad documentada en los informes de agencias como Europol (2022). De igual manera, la conceptualización del “dividendo del mentiroso” de Chesney y Citron (2019) se ve reflejada en la práctica, donde la mera posibilidad de que una prueba sea un *deepfake* ya introduce una duda razonable que puede ser explotada procesalmente.

Nuestra investigación expande estas tesis al enfocarse específicamente en la población infanto-juvenil. Mientras gran parte de la discusión inicial sobre *deepfakes* se centra en la desinformación política o la seguridad nacional, nuestros hallazgos subrayan que uno de los campos de batalla más cruentos y con víctimas más vulnerables es el de la violencia interpersonal y la delincuencia sexual contra menores. La combinación de la vulnerabilidad inherente a la etapa del desarrollo y la potencia de la tecnología crea una “tormenta perfecta” con consecuencias devastadoras.

La brecha entre la predicción teórica y la realidad práctica: el rol de las plataformas

Un hallazgo que merece una reflexión profunda es la brecha entre la conciencia del problema a nivel teórico y la lentitud de la respuesta práctica, especialmente por parte de las plataformas tecnológicas. Si bien empresas como Meta, Google o TikTok han implementado políticas contra la desinformación y el contenido manipulado, su aplicación es a menudo inconsistente y reactiva. La moderación de contenido a escala masiva es un desafío hercúleo, pero la falta de transparencia sobre la eficacia de sus algoritmos de detección y la reticencia a compartir datos con investigadores independientes dificultan una evaluación objetiva del problema y de las soluciones.

Este estudio sugiere que el modelo de autorregulación, preferido por la industria tecnológica, se muestra insuficiente para proteger eficazmente a los menores. La lógica comercial, que prioriza el *engagement* y el crecimiento, puede entrar en con-



flicto directo con la necesidad de crear entornos digitales más seguros. Esto apunta hacia la necesidad de una regulación externa más robusta, que establezca obligaciones claras de diligencia debida, transparencia y rendición de cuentas para las plataformas, en línea con propuestas como la Ley de Servicios Digitales (DSA) de la Unión Europea.

El silencio de las víctimas: un hallazgo por omisión y la cifra oscura del delito

Una de las principales limitaciones de este estudio —la dependencia de fuentes secundarias y casos reportados— es en sí misma un hallazgo significativo. Revela la existencia de una vasta “cifra oscura” de la ciberdelincuencia con IA. Por cada caso que llega a los medios de comunicación o a los tribunales, es probable que existan cientos o miles que permanezcan ocultos. El estigma, la vergüenza, el miedo a la revictimización o la creencia de que no se puede hacer nada llevan a muchos menores y a sus familias a no denunciar (UNICEF, 2021).

Este silencio no es solo una limitación metodológica; es una dimensión central del problema. La invisibilidad de la mayoría de los casos impide dimensionar la verdadera escala de la epidemia, dificulta la asignación de recursos para la prevención y el apoyo a las víctimas, y perpetúa un ciclo de impunidad para los agresores. Cualquier estrategia de política pública debe, por tanto, incluir medidas activas para fomentar la denuncia, creando canales seguros, confidenciales y adaptados a la sensibilidad de los menores.

Implicaciones para el futuro: hacia un nuevo contrato social digital

Los desafíos descritos no pueden ser abordados con soluciones parciales o anacrónicas. Se requiere una reevaluación profunda de nuestras estrategias legales, educativas y tecnológicas.

Implicaciones para el derecho penal y la política criminal

El derecho penal se enfrenta a un triple desafío: tipificación, investigación y jurisdicción.

- Tipificación: muchos ordenamientos jurídicos carecen de tipos penales específicos que sancionen la creación y difusión de *deepfakes* maliciosos. Depender de figuras genéricas como la injuria, la calumnia o los delitos contra la integridad moral puede ser insuficiente para capturar la gravedad y la especificidad del daño. Se hace necesario debatir la creación de nuevos delitos, como el de “violencia digital por suplantación” o “agresión sexual mediante imagen generada por IA”, que reconozcan la naturaleza única de estas conductas.



- Investigación: las fuerzas y cuerpos de seguridad necesitan una capacitación y dotación de recursos sin precedentes. La investigación de estos delitos requiere unidades especializadas en ciberdelincuencia con peritos forenses capaces de analizar evidencia digital compleja. Además, la cooperación internacional es indispensable, ya que los agresores, las víctimas y las plataformas suelen encontrarse en jurisdicciones diferentes. Mecanismos como el Convenio de Budapest sobre la Ciberdelincuencia deben ser fortalecidos y universalizados.
- Jurisdicción: el carácter transnacional del ciberespacio pone en jaque los principios tradicionales de territorialidad del derecho penal. Se necesitan marcos de cooperación judicial ágiles que permitan la obtención de pruebas y la persecución de delincuentes más allá de las fronteras nacionales.

Implicaciones para la educación y la alfabetización digital crítica

La prevención más eficaz es la educación. Sin embargo, la alfabetización digital no puede limitarse a enseñar a usar herramientas informáticas. Debe evolucionar hacia una “alfabetización digital crítica” (Livingstone & Stoilova, 2021). Esto implica dotar a los menores de las habilidades para:

- Evaluar críticamente la información: enseñarles a dudar, a contrastar fuentes y a identificar indicios de manipulación.
- Gestionar su identidad y privacidad digital: concienciar sobre la importancia de configurar la privacidad en redes sociales y sobre las consecuencias de compartir información personal.
- Desarrollar resiliencia emocional: prepararlos para enfrentar situaciones de acoso o exposición a contenido dañino, y enseñarles a quién acudir en busca de ayuda.

Esta educación debe ser un pilar transversal en el currículo escolar e involucrar activamente a las familias, proporcionándoles también a ellas las herramientas y el conocimiento necesarios para acompañar a sus hijos en el entorno digital.

Implicaciones para la industria tecnológica: hacia una ética por diseño

La industria tecnológica no puede seguir siendo un actor pasivo. Debe asumir una responsabilidad proactiva, integrando la seguridad y la ética desde la fase de diseño de sus productos y algoritmos (*ethics by design*). Esto implica:

- Desarrollar y mejorar las herramientas de detección: invertir en investigación para crear sistemas más eficaces para identificar y etiquetar contenido generado por IA.



- Implementar “cortafuegos” éticos: establecer límites en sus propias tecnologías de IA para impedir su uso en la generación de contenido dañino, como los *deep nudes*.
- Facilitar la denuncia y el apoyo: crear mecanismos de denuncia sencillos, rápidos y efectivos, y colaborar con organizaciones de apoyo a víctimas para ofrecer recursos a los usuarios afectados.

En última instancia, la lucha contra la ciberdelincuencia potenciada por IA es una responsabilidad compartida. Requiere un nuevo contrato social digital en el que gobiernos, empresas, educadores, familias y los propios menores trabajen de manera coordinada para construir un ciberespacio más seguro, justo y respetuoso con los derechos humanos. La inacción o la respuesta tardía no solo dejarán a una generación de jóvenes expuesta a daños irreparables, sino que socavarán los cimientos de confianza sobre los que se construye nuestra sociedad digital.

Conclusión

Al término de este análisis, la respuesta a la pregunta que ha guiado esta investigación se presenta con una claridad tan contundente como alarmante. El impacto de la inteligencia artificial (IA) en la ciberdelincuencia dirigida contra la infancia y la adolescencia no es una mera evolución incremental de las amenazas existentes; representa un cambio de paradigma fundamental, una ruptura cualitativa que desafía los cimientos de nuestra comprensión sobre la seguridad, la identidad y la justicia en la era digital. Los hallazgos de este estudio convergen en una tesis central: la sinergia entre la escalabilidad y el realismo de las tecnologías de IA, como los *deepfakes*, y la vulnerabilidad psicosocial inherente a las etapas formativas de la vida ha dado lugar a una nueva y formidable arquitectura de la agresión. Esta conclusión no es una especulación futurista, sino la constatación de una realidad emergente, documentada en los informes de agencias de seguridad (Europol, 2022) y analizada en profundidad por la academia (Chesney & Citron, 2019).

La integración de los resultados revela que el daño perpetrado a través de estas herramientas trasciende la concepción tradicional del delito informático. No estamos simplemente ante un fraude, una lesión o una suplantación de identidad en el sentido clásico. La creación y difusión de un *deep nude* de un menor, por ejemplo, no es solo una falsificación; es un acto de violencia ontológica. Es un ataque directo al ser, a la construcción de la identidad personal y sexual en un momento crítico del desarrollo. La tecnología permite secuestrar la imagen de una persona —la represen-



tación digital de su yo— para profanarla, recontextualizarla y convertirla en un arma de humillación y control. Este tipo de agresión deja cicatrices que no son meramente digitales; son heridas profundas en la psique de la víctima, capaces de generar traumas duraderos, ansiedad, depresión y un profundo sentimiento de despersonalización (UNICEF, 2021). El cuerpo digital, para las generaciones nativas digitales, es una extensión inseparable del cuerpo físico, y su violación debe ser entendida con una gravedad equivalente.

Asimismo, este estudio concluye que el fenómeno de los *deepfakes* genera una segunda capa de daño, de naturaleza epistémica y social. Como advirtieron Maras y Alexandrou (2019), nos enfrentamos a una “crisis de la evidencia”. La mera posibilidad de que cualquier contenido audiovisual pueda ser una falsificación sofisticada introduce una “hemorragia de confianza” en el ecosistema informativo y, de manera crucial, en el sistema de justicia. Este fenómeno, conocido como el “dividendo del mentiroso”, crea un entorno de incertidumbre donde las víctimas luchan por demostrar la falsedad de los ataques que sufren, mientras que los culpables pueden desacreditar pruebas genuinas alegando que son manipulaciones. Para un menor que intenta defender su honor y su verdad, este es un obstáculo casi insuperable que agrava su victimización, sumiéndolo en la impotencia. Esta erosión de la confianza en la prueba no es un problema técnico para peritos forenses; es una amenaza directa al derecho a la tutela judicial efectiva y al principio de justicia material.

Frente a esta amenaza multidimensional, la capacidad de respuesta de nuestros sistemas de protección se revela, en el mejor de los casos, como insuficiente y, en el peor, como anacrónica. El análisis jurídico-doctrinal ha demostrado que el derecho penal, con su estructura dogmática y sus tipos delictivos concebidos en una era predigital, se esfuerza por encajar estas nuevas realidades en categorías que no les hacen justicia. Figuras como la injuria, la calumnia o los delitos contra la integridad moral fueron diseñadas para un mundo donde la difusión de la falsedad era limitada y su impacto, aunque grave, no poseía la permanencia, la viralidad y el realismo visceral que la IA permite hoy. La ley, como ha señalado Brenner (2010) en el contexto más amplio de la ciberdelincuencia, a menudo va por detrás de la tecnología, dejando a las víctimas en un limbo de desprotección. Los desafíos en materia de tipificación, atribución de responsabilidad —especialmente cuando los agresores utilizan plataformas descentralizadas o anónimas— y jurisdicción transnacional conforman un paradigma en ruinas que necesita ser reconstruido, no simplemente parcheado.

De igual modo, este estudio concluye que el modelo de autorregulación de las plataformas digitales, que ha sido la norma durante las últimas dos décadas, ha demos-



trado ser inadecuado para proteger eficazmente a los menores. Las plataformas, atrapadas en un modelo de negocio que prioriza el *engagement* y la recolección de datos, a menudo implementan medidas de seguridad de manera reactiva, solo después de que el daño ya se ha producido y ha escalado a un escándalo público. Sus sistemas de moderación, aunque tecnológicamente avanzados, son fácilmente superados por la escala y la velocidad de la creación de contenido malicioso, y su falta de transparencia impide una evaluación independiente de su verdadera eficacia. La protección de la infancia no puede ser una externalidad negativa en el balance de una corporación; debe ser una obligación legal, verificable y sancionable.

Por tanto, la conclusión de este trabajo no es un llamado al pánico tecnológico ni a la tecnofobia, sino un llamado urgente a la acción, a la responsabilidad y a la construcción de un nuevo paradigma de protección integral. Este paradigma debe articularse sobre tres pilares fundamentales e interconectados: la resiliencia educativa, la innovación jurídica y la responsabilidad tecnológica por diseño.

En primer lugar, la resiliencia educativa debe ir más allá de la simple alfabetización digital. No basta con enseñar a los niños a usar un *software* o configurar una contraseña. Es imperativo cultivar una “alfabetización digital crítica”, como proponen Livingstone y Stoilova (2021), que dote a los menores de las herramientas cognitivas y emocionales para navegar en un entorno de información inherentemente incierto. Esto significa enseñarles a dudar, a verificar, a comprender los mecanismos de la manipulación, a gestionar su huella digital de manera consciente y, sobre todo, a desarrollar la resiliencia emocional para saber cómo y a quién pedir ayuda cuando se enfrentan a una agresión. Esta educación debe ser una competencia básica del siglo XXI, integrada de manera transversal en el currículo escolar y reforzada en el ámbito familiar.

En segundo lugar, la innovación jurídica es ineludible. Se necesita una nueva generación de leyes que reconozcan la especificidad de la violencia digital. Esto implica la creación de tipos penales que sancionen explícitamente la creación y difusión de contenido hiperrealista falso con fines maliciosos, especialmente contra menores. Requiere, además, agilizar los mecanismos de cooperación judicial internacional para superar las barreras jurisdiccionales y asegurar que los agresores no encuentren refugio en la impunidad que ofrece el ciberespacio global. Asimismo, es crucial desarrollar nuevos estándares procesales para la valoración de la prueba digital, capacitando a jueces, fiscales y abogados para enfrentar los desafíos de la era del *deepfake*.

Finalmente, y quizás lo más importante, es necesario exigir una responsabilidad tecnológica por diseño (seguridad y ética por diseño). La seguridad de los menores



no puede ser un añadido posterior, una opción de configuración oculta en un menú. Debe ser un principio rector integrado en el núcleo mismo del diseño de plataformas, algoritmos y aplicaciones. Esto significa que las empresas tecnológicas tienen la obligación de evaluar proactivamente los riesgos de abuso de sus tecnologías, implementar salvaguardas para prevenir la generación de contenido dañino y crear canales de denuncia y retirada de contenido que sean rápidos, accesibles y efectivos. La carga de la prueba debe invertirse: las empresas deben demostrar que sus productos son seguros para los menores antes de lanzarlos al mercado, no esperar a que las víctimas demuestren que son peligrosos.

En síntesis, la era de la inocencia digital, si alguna vez existió, ha terminado. La inteligencia artificial ha desatado fuerzas que pueden ser utilizadas tanto para el progreso como para la depredación. Proteger a la infancia y a la adolescencia de esta nueva frontera de la ciberdelincuencia no es una opción, sino un imperativo ético y una condición necesaria para la salud de nuestras futuras sociedades democráticas. La inacción o la respuesta tibia no solo condenará a innumerables jóvenes a sufrir daños profundos y evitables, sino que también significará nuestra claudicación colectiva ante un futuro donde la verdad es maleable, la identidad es vulnerable y la dignidad es un bien negociable. La tarea es monumental, pero la alternativa es impensable.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo. Los puntos de vista y los resultados de este artículo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes. No se emplearon herramientas de generación de contenido por inteligencia artificial (IA) para su elaboración.

Sobre el autor

Aldair Bueno Atencio. Magíster en Derechos Humanos y Derecho Internacional de los Conflictos Armados. Especialista en Derecho Penal y en Crimen Organizado, Corrupción y Terrorismo. Abogado. Miembro Fundador del Instituto Iberoamericano de Derecho Digital y la ciberseguridad. Investigador, Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad.

<https://orcid.org/0000-0001-9477-2826> – Contacto: info@ibdc.digital



Referencias

- Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B.,... & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. <https://arxiv.org/abs/1802.07228>
- Chesney, R., & Citron, D. K. (2019). Deepfakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. <https://doi.org/10.2139/ssrn.3213954>
- Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA) 2022*. <https://www.europol.europa.eu/>
- Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying online risk to children* (CO:RE, Key Topics Brief Reports Series, n.º 3). <https://doi.org/10.21241/ssor.71817>
- Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255-262. <https://doi.org/10.1177/1365712718807226>
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4.ª ed.). Pearson.
- UNICEF. (2021). *The state of the world's children 2021: On my mind: Promoting, protecting and caring for children's mental health*. <https://www.unicef.org/reports/state-worlds-children-2021>



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, pp. 34-42

Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.172>

DOSIER

Control+Alt+Delito: reflexiones jurídicas sobre la cibercriminalidad en Colombia

Angela Rosa Mejía Corrales 

Fundación Universitaria del Área Andina, Valledupar, Cesar

RESUMEN

Este artículo analiza, desde una mirada crítica y jurídica, los desafíos que enfrenta el país frente al auge de delitos informáticos. Si bien Colombia ha dado pasos importantes en la construcción de un marco normativo —como la *Cartilla metodológica de atención a delitos informáticos*, de la Fiscalía General de la Nación, la cual pretende ser una guía para abordar este tipo de crímenes estableciendo protocolos de acción para las autoridades y rutas de atención a usuarios y víctimas—, es necesario cuestionar su aplicabilidad práctica y si requiere una actualización profunda para ser verdaderamente efectiva.

PALABRAS CLAVE

datos personales; delitos informáticos; denuncia; derecho a la información; derecho a la privacidad; derecho del ciberespacio

CITACIÓN APA

Mejía Corrales, A. R. (2025). Control+Alt+Delito: reflexiones jurídicas sobre la cibercriminalidad en Colombia. *Revista Brújula de Investigación*, 13(25), 34-42.

<https://doi.org/10.21830/23460628.172>

Recibido: 15 de abril 2025 **Aceptado:** 20 de junio de 2025

Contacto: Angela Rosa Mejía Corrales ✉ amejia90@estudiantes.areandina.edu.co



Introducción

Vivimos en una era donde el acceso a la información, la hiperconectividad y la digitalización de servicios han transformado la forma en que nos comunicamos, trabajamos y vivimos. Sin embargo, este avance también ha traído consigo nuevas formas de criminalidad que desafían los límites del derecho tradicional. En este contexto, surge un fenómeno creciente y complejo: la cibercriminalidad, la cual plantea retos técnicos, normativos y éticos para los operadores jurídicos, las instituciones del Estado y la ciudadanía en general.

El objetivo de este artículo es analizar críticamente el marco jurídico colombiano frente a los delitos informáticos, especialmente a la luz de la *Cartilla metodológica de atención para los delitos informáticos*, de la Fiscalía General de la Nación (FGN), diseñada para guiar a operadores judiciales y técnicos en el abordaje de esta problemática. Se abordarán las categorías delictivas más frecuentes, los retos probatorios asociados a la evidencia digital y la cooperación internacional como mecanismo indispensable en la lucha contra el cibercrimen.

Desde una perspectiva teórico-jurídica y práctica, se expondrán los principales avances normativos, así como las limitaciones operativas y conceptuales que enfrenta el Estado frente a un fenómeno transnacional, dinámico y técnicamente sofisticado. La cibercriminalidad no solo desafía al derecho penal clásico en sus categorías tradicionales de tipicidad, antijuridicidad y culpabilidad, sino que exige una constante actualización de capacidades institucionales, normativas y periciales.

Este análisis se propone contribuir al debate académico sobre los alcances reales de la legislación vigente y su aplicabilidad, proponiendo además una mirada crítica sobre la eficiencia de las herramientas disponibles para el control social y penal en entornos digitales. Busca responder a la pregunta problema: ¿es efectiva la respuesta jurídica del Estado colombiano frente a la cibercriminalidad, particularmente a través de la Ley 1273 de 2009 y la *Cartilla metodológica de atención a delitos informáticos*, de la Fiscalía General de la Nación? La importancia de este trabajo radica en que permite comprender cómo se está protegiendo —o dejando de proteger— uno de los activos más valiosos de nuestra sociedad: la información.

Marco teórico

En el VI Congreso Internacional de Derecho Penal, organizado por la Universidad de los Andes en 2012, Fernando Miró, docente español, detalló el concepto de *cibercriminalidad*. Este término puede parecer un concepto legal, pero en realidad es criminológico, ya que hace referencia al contexto en el que se produce la infracción. Señaló que los seres humanos convivimos en dos espacios simultáneamente: un espacio físico o



material, donde se cometen delitos físicos —los cuales encontramos ya desarrollados en la Ley 599 de 2000, por la cual se dicta el Código Penal colombiano— y otro, denominado *ciberespacio*, donde se perpetran ciberdelitos o delitos informáticos mediante el uso de las tecnologías de la información y la comunicación (TIC).

Los cibercrímenes han sido objeto de estudio por juristas y ordenamientos jurídicos nacionales e internacionales. Para definir el término *cibercriminalidad*, el Convenio de Budapest sobre Ciberdelincuencia de 2001 establece que son aquellas infracciones “contra la confidencialidad, la integridad y la disponibilidad de la información, de los datos y de los sistemas informáticos”. En Colombia, por su parte, se expidió la Ley 1273 de 2009, donde se crea el bien jurídicamente tutelado de la información, los datos y los sistemas de información, y, tipificando conductas asociadas a la afectación de este bien, se crearon los siguientes tipos penales: Capítulo I, “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”. En este capítulo podemos encontrar conductas penales como: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de *software* malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales. Capítulo II, “De los atentados informáticos y otras infracciones”; este capítulo tipifica el hurto por medios informáticos y semejantes, así como la transferencia no consentida de activos.

Los antes anotados tipos penales se encuentran determinados a partir del artículo 269A de la Ley 1273 de 2009, que añadió estas conductas al Código Penal colombiano (Ley 599 de 2000), donde se establece el tipo *acceso abusivo a un sistema informático*. En este tipo penal se sanciona a quien, sin autorización, accede a un sistema informático protegido o no. Es la base para tipificar la intrusión no consentida a redes o servidores, muy común en *hackeos*. Se sanciona con pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La Sentencia SP592-2022 del 2 de marzo de 2022, proferida por la Corte Suprema de Justicia, se refirió por primera vez sobre los elementos del ciberdelito en los siguientes términos:

- i) Sujeto activo no calificado, por no necesitar de una condición especial para quien realiza los verbos rectores; ii) Sujeto pasivo, persona natural o jurídica titular del sistema informático; iii) Lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad. En ese sentido, ha sido reconocido como un tipo penal pluriofensivo; iv) Solo admite el dolo en el actuar del ciberdelincuente; v) Es un delito de mera conducta, por cuanto, la sola intromisión en una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado; vi) Contempla dos verbos rectores, acceder o mantener; vii) Como ingrediente normativo, exige que



el sujeto activo de la acción acceda en el sistema informático sin autorización, o, aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas.

Otro de los artículos de la misma ley es el 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación*, el cual penaliza la interferencia con el funcionamiento de un sistema informático o red de telecomunicación o la eliminación, alteración o supresión de datos, lo cual puede paralizar servicios esenciales. También está consagrado el artículo 269C: *Interceptación de datos informáticos*. Este delito castiga a quien intercepte sin autorización datos transmitidos entre sistemas, incluso si no los modifica. Se puede visibilizar en casos de espionaje digital. Artículo 269D: *Daño informático*. Tipifica la conducta de quien, sin autorización, dañe, deteriore, altere o suprima información contenida en un sistema informático. Este incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Además, del artículo 269E: *Uso de software malicioso*. Establece la pena para quien incurra en la creación, distribución o uso de programas diseñados para causar daño informático, como virus, troyanos o *ransomware* (*malware* que secuestra o retiene datos dentro de un sistema operativo a cambio de un rescate para remover esta restricción). O el artículo 269F: *Violación de datos personales*, donde se sanciona el acceso, uso o divulgación no autorizada de datos personales almacenados en sistemas informáticos, conectando con el derecho fundamental al *habeas data*, establecido en el artículo 15 de nuestra Constitución Política. Así como unos muy comunes actualmente, como el artículo 269G: *Suplantación de sitios web para capturar datos personales*. Con este se penaliza la creación o manipulación de páginas web falsas con el fin de capturar datos de los usuarios para usos ilícitos.

Y, por supuesto, los artículos 269I y 269J, donde se determinan respectivamente el *hurto por medios informáticos y semejantes* y la *transferencia no consentida de activos*. El primero establece como delito el apoderamiento de bienes (como dinero), es decir, adueñarse de estos bienes ajenos mediante manipulación informática, simulaciones digitales o fraudes electrónicos. Mientras que el segundo aborda el uso no autorizado de sistemas para mover activos (como fondos electrónicos), sin necesidad de vulnerar la seguridad del sistema, pero sí de aprovecharlo para un beneficio económico.

Todos estos delitos informáticos también se encuentran incluidos en la cartilla metodológica expedida por la Fiscalía General de la Nación, además de una descripción detallada de las rutas de atención, roles de los actores institucionales y canales disponibles para la recepción de denuncias, tanto en entornos presenciales como



virtuales. Su enfoque parte de una clara diferenciación entre usuario y víctima, y delimita funciones específicas para fiscales, policías judiciales y peritos forenses.

Métodos

Como aspecto metodológico de la investigación sobre la efectividad de la respuesta jurídica colombiana frente a la cibercriminalidad, es pertinente mencionar que se ha requerido de una revisión bibliográfica con un método de investigación hermenéutico, puesto que es necesaria la recopilación, análisis y síntesis de información proveniente de diversas fuentes documentales, orientado a la comprensión crítica de esos textos normativos, doctrinales y técnicos relevantes en el ámbito jurídico y forense digital.

Esta perspectiva hermenéutica ha facilitado el estudio del contenido legal de la Ley 1273 de 2009, su utilidad en la esfera penal, además de los componentes operativos y procedimientos presentes en la *Cartilla metodológica de atención para los delitos informáticos* emitida por la Fiscalía General de la Nación. Esta revisión no solo analiza las reglas y directrices, sino también su contexto, amplitud, restricciones y vínculo con los fenómenos actuales de delincuencia digital.

Este método nos ayudará tanto a explicar el fenómeno de la cibercriminalidad como a evaluar la capacidad del Estado para enfrentarlo, llevándonos hacia una explicación más detallada del porqué mediante diferentes técnicas que se caracterizan por su contextualización, como un análisis normativo y jurisprudencial de la Ley 1273 de 2009, una revisión crítica de la cartilla metodológica y algunas entrevistas semiestructuradas a fiscales de la ciudad de Valledupar, miembros de la división de delitos informáticos y policías judiciales, para que nos informen sobre la utilidad de esta cartilla, indicando si es eficiente o si ha tenido dificultades para su aplicación.

Resultados

En la anterior indagación, se analizó la Ley 1273 de 2009 y la *Cartilla metodológica de atención de delitos informáticos*, expedida por la Fiscalía General de la Nación, en la que se destacan tanto sus fortalezas como sus debilidades. Se pudieron identificar algunos desafíos legales en la persecución de delitos informáticos:

Vacíos normativos: impunidad y falta de sanción

Si bien la cartilla se sustenta en un marco legal robusto (incluyendo la Constitución, el Código Penal y el Convenio de Budapest), su aplicabilidad en la realidad colombiana es un punto de debate. A pesar de la existencia de leyes como la Ley 1273 de 2009,



que tipifica los delitos informáticos, el crecimiento exponencial de nuevas formas de criminalidad digital como el *ransomware* o el *cyberbullying*, los cuales no están bien determinados en la norma, genera que los delincuentes puedan eludir el castigo. Si las leyes no han sido actualizadas o no se han desarrollado normas específicas para ciertos tipos de delitos, quienes cometen estos actos pueden quedar impunes, ya que no hay un marco legal claro que los defina como ilegales. Estos vacíos normativos en los delitos informáticos también generan dificultades para los jueces y las autoridades, pues limita su deber legal de administrar justicia al no lograr una interpretación clara de la norma que defina si las conductas que encuentran en los diferentes casos se ajustan o no a un tipo penal.

Colaboración internacional en la lucha contra el cibercrimen

Se menciona la importancia de tratados internacionales como el Convenio de Budapest y los acuerdos con Europol y Ameripol. Sin embargo, en la práctica, la cooperación internacional de los delitos informáticos enfrenta obstáculos significativos. Según el *Módulo 7: Cooperación internacional contra los delitos cibernéticos* de la UNODC (Oficina de las Naciones Unidas contra la Droga y el Delito), la colaboración internacional se promueve mediante acuerdos bilaterales, regionales y multilaterales sobre delitos cibernéticos, siempre que haya una doble sanción (es decir, una estipulación en los acuerdos que requiera que el comportamiento denunciado sea visto como ilegal en los países colaboradores). Sin la doble penalización y sin normativas equilibradas, se generan refugios seguros para los crímenes cibernéticos donde no se puede juzgar a los responsables. La lucha contra el cibercrimen requiere la cooperación de diferentes países debido a varios factores, como la globalización de internet y que los delitos informáticos pueden involucrar actores y víctimas de diferentes países.

Rol de los actores y canales de denuncia/atención

El rol de los actores clave en la investigación de delitos informáticos (fiscales, policías judiciales y peritos forenses) está claramente definido en la cartilla. Sin embargo, una de las críticas recurrentes a la efectividad de la justicia en estos casos es la falta de formación especializada y de herramientas tecnológicas avanzadas. Sin un equipo capacitado y con acceso a *software* de análisis forense de última generación, la lucha contra el crimen informático se ve severamente limitada. A pesar de que el documento presenta distintos canales de denuncia (presencial, virtual, telefónica y escrita), la realidad es que a nivel local (Valledupar) muchas de las personas afectadas y usuarios no pueden acceder a ellos en el instante que los necesitan.



Discusión

Los resultados previstos en este estudio permiten una respuesta afirmativa, aunque con algunos matices, a la cuestión planteada: ¿es eficaz la reacción legal del Estado colombiano ante la cibercriminalidad mediante la Ley 1273 de 2009 y la cartilla metodológica? El estudio de este marco normativo muestra que su instauración representó un importante hito regulatorio en Colombia, al categorizar por primera vez comportamientos vinculados a crímenes informáticos. Sin embargo, la rápida transformación tecnológica ha dejado ciertas lagunas frente a nuevas modalidades de delincuencia como el *ransomware*, el *phishing* basado en inteligencia artificial o la explotación de vulnerabilidades en la nube.

Respecto de la cartilla metodológica de la FGN, se aprecia positivamente su contribución como herramienta de guía operativa para la gestión de cibercrímenes, al establecer de manera precisa los participantes, sus roles y las rutas de atención. No obstante, su eficacia se encuentra restringida por elementos estructurales: escasez de personal especializado, escasa formación en informática forense, ausencia de coordinación institucional y problemas en el acceso de los ciudadanos a los medios de denuncia. Estos componentes influyen de manera negativa en la ejecución práctica de las directrices de la cartilla.

Probablemente, un descubrimiento significativo será la tensión entre la presencia de un marco legal jurídicamente integral y su escasa aplicación práctica, fenómeno que ha sido ampliamente debatido en investigaciones anteriores del derecho penal en Colombia. Otra posible interpretación es que la cibercriminalidad no solo demanda una reacción legal, sino también un cambio cultural e institucional para que los actores legales, expertos y ciudadanos puedan abordarla de manera holística.

Dentro de las restricciones del estudio se encuentra la imposibilidad de acceder a detalles de investigaciones reservadas de la FGN, además de la limitación de conseguir un número limitado de declaraciones de especialistas si no se consiguen las entrevistas previstas. Sin embargo, la orientación documental del estudio garantiza un enfoque adecuado para las multas sugeridas.

Conclusión

La *Cartilla metodológica de atención de los delitos informáticos*, de la Fiscalía General de la Nación, no aborda de manera profunda los mecanismos de apoyo y reparación a las víctimas, más allá del proceso judicial, y su efectividad se ve afectada por la falta de actualización frente a nuevas modalidades de delito, la insuficiencia



de recursos tecnológicos y humanos, y las dificultades en la cooperación internacional. Sin embargo, no podemos desmeritar la gran iniciativa que representa este documento, pues es un instrumento importante para estandarizar los procesos de investigación. Para hacer frente a los desafíos del cibercrimen moderno, es indispensable que la FGN fortalezca la capacitación del personal, implemente herramientas de inteligencia artificial en la investigación y optimice los mecanismos de denuncia y atención a víctimas. Así como la ciudadanía debe mantenerse informada sobre las modalidades para cometer ciberdelitos y prevenir estas vulneraciones de derechos, la meta es estar y sentirnos seguros en el ciberespacio.

Declaración de divulgación

La autora declara que no existe ningún potencial conflicto de interés relacionado con el artículo. Los puntos de vista y los resultados de este artículo pertenecen a la autora y no reflejan necesariamente los de las instituciones participantes. No se emplearon herramientas de generación de contenido por inteligencia artificial (IA) para su elaboración.

Sobre la autora

Angela Rosa Mejía Corrales. Estudiante de la Facultad de Derecho, Fundación Universitaria del Área Andina, sede Valledupar. Integrante del grupo de investigación Verbaiuris, Semillero Derecho Procesal y Probatorio a cargo de la Dra. Margarita Martínez.

<https://orcid.org/0009-0007-3018-4364>

Contacto: amejia90@estudiantes.areandina.edu.co

Referencias

- Ámbito Jurídico. (2012, 10 de septiembre). Cibercriminalidad: la delincuencia en “el otro espacio”. *Ámbito Jurídico*. <https://www.ambitojuridico.com/noticias/penal/penal/cibercriminalidad-la-delincuencia-en-el-otro-espacio>
- Corte Suprema de Justicia. (2022). *Sentencia SP592-2022* (Radicación 50621). [enlace sospechoso eliminado]
- Fiscalía General de la Nación. (s. f.). *Cartilla metodológica de atención de los delitos informáticos*. <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Methodologica-de-Atencion-de-Delitos-Informaticos.pdf>
- Fiscalía General de la Nación. (2024, 6 de noviembre). *¿Qué es el ciberdelito?* <https://www.fiscalia.gov.co/colombia/judiccionario/que-es-el-ciberdelito/>



Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Enero 5 de 2009. DO. N.º 47.223.

Madariaga Pérez, X. C. (s. f.). *La Corte Suprema de Justicia aclaró elementos normativos del acceso abusivo a un sistema informático*. Blog Opiniones del Instituto Colombiano de Derecho Penal. <https://icdp.org.co/la-corte-suprema-de-justicia-aclaro-elementos-normativos-del-acceso-abusivo-a-un-sistema-informatico/>

Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2019, junio). *Módulo 7: Cooperación internacional contra los delitos cibernéticos*. <https://www.unodc.org/e4j/es/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html>



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, pp. 43-64


Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.171>

DOSIER

Escuela Militar de Cadetes “General José María Córdova”: optimización del proceso de contratación del personal docente

Ricardo Andrés Bernal Vallarino 

Esteban Dario Maigual Maigual

Cristian Horacio Pérez Navarro

Escuela Militar de Cadetes “General José María Córdova”

RESUMEN

Este artículo propone solucionar la problemática de contratación docente de la Escuela Militar de Cadetes “General José María Córdova”, para lo cual desarrolla un diseño metodológico basado en un enfoque mixto que muestra por qué es necesario el cuerpo docente y su vinculación y contratación. Posteriormente, analiza la percepción y problemáticas de dicho proceso, donde, finalmente, con el diseño de una herramienta tecnológica (*software*), pueda optimizarse la celeridad y agilidad de la contratación para los docentes hora cátedra de la ESMIC. Lo anterior permite mejorar ostensiblemente la gestión del talento humano, brindando bienestar y evolución en esta IES.

PALABRAS CLAVE

contratación; docentes; instrumento; *software*; tecnología

CITACIÓN APA

Bernal Vallarino, R. A., Maigual Maigual, E. D., & Pérez Navarro, C. H. (2025). Escuela Militar de Cadetes “General José María Córdova”: optimización del proceso de contratación del personal docente. *Revista Brújula de Investigación*, 13(25), 43-64.

<https://doi.org/10.21830/23460628.171>

Recibido: 15 de abril 2025 **Aceptado:** 20 de junio de 2025

Contacto: Ricardo Andrés Bernal Vallarino  ricardo.bernal@esmic.edu.co



Introducción

La tecnología ha permitido a los seres humanos tener una mayor facilidad en el desarrollo y ejecución de procesos. Prueba de ello es cómo las empresas, conforme a la globalización, van evolucionando y teniendo una mejora continua, con el fin de ser más competitivas y optimizar sus procedimientos en el campo empresarial y la administración del talento humano.

En este contexto, la ciencia, en relación con los cambios de la tecnología, propicia la integración de los conocimientos científicos desde varias aristas y de manera integral permite dar un mejor tratamiento a los complejos fenómenos de la realidad social. Lo anterior induce el surgimiento de nuevas ciencias integradas y la conformación de equipos interdisciplinarios y multidisciplinarios con una profunda orientación humanista, con el fin de resolver los problemas sociales que existen y agobian al mundo. Álvarez (2021) señala:

El desempeño del talento humano docente es un aspecto básico de la gestión de recursos humanos en las instituciones educativas. Es una prioridad para emprender acciones que estimulen la permanencia y resultado en las actividades académicas, investigativas y sus relaciones con la sociedad (p. 151).

La Escuela Militar de Cadetes “General José María Córdova” (ESMIC) forma a los futuros oficiales del Ejército Nacional, que salen a los diferentes territorios del Estado colombiano con el fin de brindar seguridad y apoyo a los ciudadanos del país. Por tal razón, es necesario que sean formados en conocimientos de la ciencia militar y carreras complementarias que aporten a la toma de decisiones y les den un valor agregado para contribuir al desarrollo del país.

De acuerdo con lo anterior, es vital el cuerpo docente, orientador y difusor de buenas prácticas para el desarrollo de la ciencia militar, plasmando en el futuro oficial los conocimientos necesarios para el ejercicio del quehacer castrense. Esto amerita, dentro de la administración del talento humano, un proceso de selección y contratación que ayude a la ESMIC a focalizar los perfiles más adecuados que formarán a los futuros oficiales, toda vez que esta IES es diferencial. Chaveco (2020) indica:

En el logro de los propósitos antes mencionados juega un papel esencial la labor educativa de nuestros docentes, si entendemos a la misma como el proceso en el cual se corresponden los objetivos y tareas de la sociedad y en cuyos resultados se pueden contemplar la formación de la personalidad del alumno (p. 65).

Por tal razón, en la administración del talento humano se debe optimizar un procedimiento que coadyuve a la selección de los docentes y a su vez sea práctico, con el fin de que se agilice y se eviten demoras. Es aquí donde juega un papel importante la tecnología, la cual permite optimizar tiempo y brindar bienestar al futuro cuerpo docente en la diligencia de los requisitos para su selección.



En cuanto a la metodología empleada para el presente trabajo, se recurrió a un enfoque mixto, donde se podrá evidenciar una medición de datos por medio del instrumento de Google Forms, el cual, mediante gráficos estadísticos, mostrará una perspectiva de la problemática en diferentes categorías o variables; de igual forma, se verá plasmada una percepción del fenómeno.

Así mismo, el alcance de la presente investigación será descriptivo, toda vez que se reflejará su proceso, las falencias del tema por abordar y sus posibles soluciones. Para obtener las variables o categorías, se contará con una población de docentes de la ESMIC en Bogotá, cuya muestra será recopilada de las facultades de Ciencias Militares y Administración Logística. También es fundamental considerar las fases del proyecto como: recopilación de la información, decantación del material no vital en el presente tema, organización y tabulación de la información, análisis de resultados, y conclusiones y recomendaciones. Finalmente, el análisis e interpretación de los datos será conforme a los datos arrojados por el instrumento mencionado, el cual brindará los insumos necesarios para determinar las categorías y variables relevantes dentro del presente tema.

Proceso de contratación docente

Previo a establecer el proceso de contratación, es pertinente justificar por qué un oficial del Ejército Nacional debe tener una preparación. Prueba de ello lo manifiesta la historia. Todo tipo de disciplina o carrera profesional necesita personal idóneo que disemine el conocimiento a las generaciones futuras, logrando de esta manera generar experticia en el desempeño de una profesión; en este caso, generar la pericia y capacidad en la ciencia militar. La base de la formación en la carrera militar se refleja en las diferentes misiones militares que aportaron en la evolución, diseño curricular y cultura militar del soldado colombiano. Lo anterior se debe a la necesidad de una reforma militar y a la visión que tuvo el general Rafael Reyes al asumir su presidencia en 1904. Las misiones militares contratadas para la actualización y cambio del Ejército colombiano fueron las siguientes:

- Misión chilena (1907-1915): por las buenas relaciones que existían en el momento en los gobiernos, fue más sencillo y viable la gestión de traer una comisión que estructurara la formación y contenidos temáticos de la carrera militar. Se tuvo en cuenta dicho país porque para la época era considerado en la parte militar como el mejor Ejército latinoamericano.
- Misión suiza (1924-1927): la percepción en su momento por parte del Gobierno nacional era que, por tener similitudes con el terreno colombiano, era pertinente y asertivo traer una comisión de dicho país para otra actualiza-



ción y estructura del futuro oficial del Ejército colombiano. El Ejército suizo también poseía en su ADN formación prusiana, lo cual determinaba que era compatible en el caso de la continuidad de los planes de instrucción y cátedra académica.

- Misión alemana (1929-1934): catalogado como el mejor Ejército a nivel mundial.

Tener una intervención e interés en la formación de los futuros oficiales del Ejército permite evidenciar que no solo están formados para la guerra; también tienen un valor agregado en otras disciplinas y materias, que permiten a este comprometido servidor de la nación emplear un conocimiento adicional para la toma de decisiones y ayuda al pueblo colombiano. Por lo anterior, en el plan de estudios de 1930, que se encuentra en el libro *Evolución histórica de la ESMIC* (tomo 1), se muestran materias relacionadas con la formación y preparación de un oficial del Ejército Nacional.

Plan de estudios para 1930

Materias	Cursos Generales		Curso Militar	
	1er. año	2º año	3er. año	4º año
Religión	1			
Castellano	4			
Literatura		2		
Historia universal	3	3		
Historia de Colombia	2	3	2	
Geografía	3			
Álgebra	3			
Geometría	4	2	2	
Geometría descriptiva		2		
Geometría analítica		2		
Dibujo		2		
Física		3	2	2
Química		3	3	
Historia natural	3	3	2	
Francés	3			
Inglés		3	3	
Táctica			3	3
Topografía			2	2
Fortificaciones			2	3
Conocimiento de armas			2	3
Códigos y constitución				4
Conocimiento de reglamentos				3
TOTAL HORAS SEMANALES	26	26	23	23

El Curso Militar tenía, dos veces a la semana, instrucción de fortificaciones y de táctica en el terreno.

Figura 1. Plan de estudios de 1930 para la formación de oficiales de la ESMIC.

Nota: El plan de estudios plasma materias de ámbito militar y particular que ven los cadetes en la ESMIC, reflejando una preparación integral.

Fuente: Rodríguez(2007).



Así las cosas, y retomando el Decreto 434 del 13 de abril de 1907, se logra establecer que en los artículos 7 y 9 se fundamentan las razones de un cuerpo docente para la preparación y formación de los futuros oficiales del Ejército.

- Artículo 7. El número de profesores civiles y militares se fijará de acuerdo con las necesidades del plan de estudios que se adopte, y los nombramientos se harán por el Ministerio de Guerra, a propuesta de la dirección de la Escuela.
- Artículo 9. El plan de estudios que deba seguirse definitivamente será propuesto por la Dirección de la Escuela al Ministerio de Guerra durante el curso del presente año.

En definitiva, se debe tener una selección óptima y apropiada de los docentes de la ESMIC con características diferenciales y esenciales para una persona con formación castrense.

La ESMIC es una institución de educación superior (IES) con acreditación en alta calidad y diferentes programas académicos. Como valor agregado, es una IES diferencial y, como institución castrense, ofrece que los futuros oficiales del Ejército Nacional tengan la posibilidad de tener una doble titulación. De acuerdo con esto, es pertinente mencionar con qué programas académicos cuenta tan prestigiosa IES:

- Como programa pilar y fundamental en la formación de los subtenientes del Ejército, está la carrera de Ciencias Militares. Dicho programa es la esencia de la carrera militar y brinda las competencias para el desarrollo de los procesos y procedimientos de la ciencia militar. De igual forma, con su componente homologable, permite en aquellas materias o saberes transversales a las diferentes disciplinas que se pueda tener la viabilidad de poder desarrollar una profesión complementaria, que dé un valor agregado a los futuros oficiales del Ejército para que sea puesta en práctica conforme a las necesidades y futuras soluciones del ciudadano colombiano en las zonas más complejas del territorio nacional. El proyecto educativo del programa del 27 de enero del 2022 de la Facultad de Ciencias Militares plasma lo siguiente:

Estructura curricular por áreas de formación, módulos multidisciplinarios de saberes afines y componente homologables entre programas. La homologación de créditos académicos en el plan de estudio permite que los estudiantes se formen como profesional en Ciencias Militares, centro de la formación militar, y paralelamente en otra carrera vinculada a la formación. (ESMIC, 2022, p. 55)

- Administración Logística. Genera los conocimientos para la administración de los diferentes recursos de defensa, en la esencia logística, personal y material, con el fin de potencializar un aspecto que permite planear y prever el



sostenimiento de las Operaciones Terrestres Unificadas (OTU) en el área de operaciones.

- Relaciones Internacionales. Brinda herramientas para el análisis y comprensión del sistema internacional contemporáneo, siendo la geopolítica una de las principales herramientas que permite enlazar el Estado con la política exterior y del propio territorio.
- Educación Física Militar. Proyecta a los futuros educadores físicos para promover las buenas prácticas en el desempeño físico de los funcionarios de la institución, fortaleciendo de esta manera las capacidades para sortear los obstáculos e inclemencias de las OTU.
- Derecho. La cual, dentro del marco constitucional y doctrinal, orienta la buena toma de decisiones jurídicas para las problemáticas y adversidades que puedan presentarse en el ejercicio de la ciencia militar en el territorio colombiano.
- Ingeniería Civil. Donde por medio de sus capacidades y especialidades, promueve el progreso, crecimiento institucional y, en el caso de la población civil, cuando sea requerido, contribuye al desarrollo económico y estructural del país.

Descripción del proceso de contratación

El proceso de selección en la contratación docente en la ESMIC se lleva a cabo de la siguiente manera:

1. De acuerdo con las materias o saberes donde se presenten necesidades en las facultades, dicha dependencia estructura el perfil y requisitos necesarios, los cuales deben ser acordes a la materia de la facultad.
2. Las facultades envían la información del perfil y saber a la dependencia de Comunicaciones Estratégicas, donde crean el *brochure* para ser publicado en la página web de la ESMIC y abrir la convocatoria docente.
3. Los posibles candidatos deben enviar lo requerido a un correo emitido por las facultades en el tiempo estipulado por la convocatoria.
4. Los participantes que acudieron al llamado de la convocatoria son consolidados y llevados a consejo de facultad para ser avalados en comité y seleccionados, según el puntaje conforme a la información suministrada.
5. Posterior a la selección de las facultades, los docentes que sean escogidos son notificados vía correo electrónico, en donde, como etapa final, efectúan una entrevista psicológica, un examen de conocimientos y una entrevista con el decano de la facultad.



6. Finalmente, al culminar los últimos tres pasos, son notificados quienes hayan pasado la convocatoria para ser contratados.

La documentación para la contratación consta de los siguientes 24 ítems (Figura 2):

LISTA DE VERIFICACIÓN HORA CATEDRA B1 - DOCENTES ANTIGUOS		
NO.	DOCUMENTACIÓN	COMPLETA
1	Acta de escalafón docente completa	
2	Evaluación docente (segundo semestre 2023)	
3	Formato solicitud de empleo con fecha actual de acuerdo a formato ordenado.	
4	Hoja de vida personal con fotografía a color formato (curriculum vitae).	
5	Una (01) copia cedula de ciudadanía 150 %	
6	Copia del registro civil de nacimiento.	
7	Validación situación militar definida (Ley 1861 página de reclutamiento).	
8	Una (1) fotografía 7X8 y tres (3) fotografías de 3X4 fondo color blanco o azul, pegadas en hoja tamaño carta.	
9	Concepto de idoneidad profesional con firma y fecha actual (Facultad).	
10	Entrevista psicológica con firma, fecha actual Facultad	
11	Constancias de estudios: Diplomas, Actas de Grado y Tarjeta Profesional (Título Profesional de pregrado, Especializaciones, Maestrías y Doctorados) (Los mismos que fueron analizados y valorados en el escalafón docente y que están relacionados en la respectiva acta).	
12	Certificados de experiencia laboral relacionados en el acta de escalafón.	
13	Certificados de experiencia docente relacionados en el acta de escalafón.	
14	Concepto de confiabilidad con firma, fecha actual (B2).	
15	Antecedentes disciplinarios de la Procuraduría General de la Nación (www.procuraduria.gov.co) con vigencia no mayor a 30 días de expedido.	
16	Antecedentes de la Policía (www.policianacional.gov.co) y certificado de medios (https://svrncpc.policia.gov.co/PSC/frm_cnp_consulta.aspx) con vigencia no mayor a 30 días de expedido.	
17	Boletín de Responsable Fiscales de la Contraloría General de la Nación (www.contraloriagen.gov.co) con vigencia no mayor a 30 días de expedido.	
18	Dos (2) recomendaciones personales.	
19	Formato único declaración juramentada de bienes y rentas y actividad económica personal natural, por el departamento administrativo de la función pública debidamente diligenciado y firmado, con fecha actualizada (http://www.dafp.gov.co/listar_seccion_completa.asp?idpublicacion=95&iddependencia) con firma y fecha actual.	
20	Formulario de novedades afiliación de la E.P.S. diligenciado y copia del documento de identidad. En caso de ser militar en uso de buen retiro, certificación actualizada de afiliación expedido por la Dirección General de Sanidad Militar (https://saludsis.mil.co/)	
21	Certificación de afiliación al Fondo de Pensiones, en caso de ser pensionado anexar copia de resolución de pensión.	
22	Certificación bancaria necesaria para realizar la consignación del salario mensual con vigencia no mayor a 30 días de expedido.	
23	Afiliación ARL (B1-ESMIC)	
24	Afiliación Caja de Compensación Familiar (B1-ESMIC)	

CADA FACULTAD DEBE ENTREGAR TODA LA DOCUMENTACIÓN ORGANIZADA DE ACUERDO A LISTA DE VERIFICACIÓN EN UNA CARPETA 4 ALETAS, POR CADA DOCENTE Y MARCADA CON EL NOMBRE DEL DOCENTE Y LA FACULTAD, DE ACUERDO A DIRECTIVA PERMANENTE NO. 01016 DEL 2016 "ANEKO J".

Elabora: AA12 Lady Vanegas
Auxiliar Apoyo Contratación Docente Cátedra

Revisó: PB Sandra Seva
Asesora Contratación Hora cátedra

Vo. B. TC. Ernesto Santamaría
Jefe de Proceso ESMIC

Fecha actualización: 30/10/2023.

Figura 2. Listado de la documentación requerida para la contratación.

Nota: Cantidad de documentos y su denominación para la contratación docente en la ESMIC.

Fuente: Facultad de Ciencias Militares, ESMIC (s. f.).

Oportunidades de mejora en el proceso de contratación

La ESMIC maneja un proceso de contratación minucioso y riguroso. Muestra de ello es que la selección para el año siguiente está terminada previo a la vigencia en ejecución, demostrando un grato planeamiento y celeridad administrativa en cada una de las facultades de la ESMIC.



Los docentes que hacen parte de tan estimada institución son personal plenamente preparado y capacitado; además, como conocimiento diferencial, deben poseer criterios e idoneidad en seguridad y defensa, doctrina de la ciencia militar, carreras complementarias, experticia y experiencia en el campo empresarial y laboral.

En consecuencia de lo anterior y siguiendo las directrices del Proyecto Educativo de la Fuerza Pública (PEFUP, 2021), este nos manifiesta lo siguiente:

Consecuente con este gran propósito contamos con un gran sistema educativo, pues es propósito del Estado colombiano que nuestros hombres y mujeres estén inmersos en escenarios que les permitan desarrollar al máximo sus capacidades, vivan un espíritu de superación permanente y se preparen con programas de alta calidad para enfrentar con éxito sus propias vidas y los retos de la seguridad y la defensa del país. (p. 4)

Esto quiere decir que los docentes poseen capacidades y conocimientos en las diferentes carreras que promoció la ESMIC, como también en la ciencia militar, donde es una mezcla armoniosa entre lo holístico y lo militar.

De acuerdo con lo anterior, es imperativo tener un cuerpo docente selecto y, por tal razón, se puede observar que la contratación de este personal es exigente. El comité de representantes de la institución educativa se rige por la Ley 115 de 1994, que establece que la selección y la contratación de docentes deben ser avaladas por los representantes de la institución, la comunidad educativa y el Ministerio de Educación Nacional, evidenciándose contratos a término fijo (máximo diez meses) o indefinido, consultando plenamente la normativa específica para cada caso particular.

A nivel general, la contratación es muy buena y puede optimizarse más mediante la tecnología que actualmente está a la vanguardia de todos los procesos. Otros autores manifiestan:

Seleccionar y contratar de manera eficaz a los candidatos a la profesión docente y asignar el profesorado de calidad de manera equitativa es un aspecto vital para mejorar el aprendizaje del alumnado. Un profesorado eficaz puede representar el más importante factor interno a la escuela a la hora de mejorar el rendimiento del alumnado (Bruns & Luque, 2014; Bruns et al., 2019; OECD, 2018a). Según la investigación llevada a cabo para el *Global Monitoring Report* de la UNESCO, un análisis de los resultados en 45 países del *Trends in International Mathematics and Science Study 2011* para cuarto grado arrojó la conclusión de que, a mayor calidad del profesorado, más descendía la incidencia del aprovechamiento deficiente (Global Education Monitoring Report Team, 2014, p. 233).

Por tal razón, se hace necesario un instrumento tecnológico que optimice y coadyuve en el proceso de contratación y documental para ahorrar tiempo y ser más ágil. El instrumento fue diseñado con las siguientes preguntas: 1) ¿Qué tipo de cone



trato tiene actualmente? 2) ¿Cuánto tiempo lleva usted en la ESMIC? 3) ¿Cuánto tiempo (días) demanda la elaboración y entrega de su carpeta para su contratación? 4) ¿Cuál ha sido la mayor problemática al entregar la documentación para su contratación? 5) Clasifique usted cómo considera la idea de incluir una herramienta tecnológica para el proceso documental en la contratación.

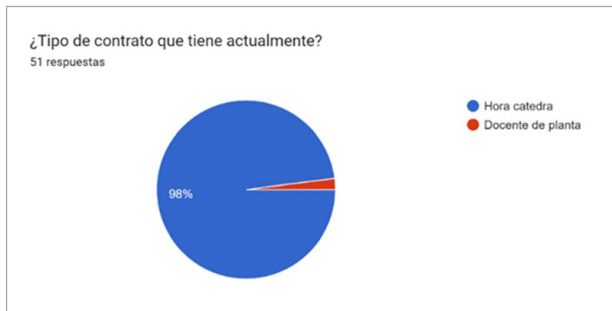


Figura 3. Porcentaje en la denominación docente en la contratación de la ESMIC.

Nota: Porcentaje en la denominación docente en la contratación de la ESMIC.

Fuente: Elaboración propia.

Se observa que el 98 % de los docentes es hora cátedra (horas dictadas por materia o saber). Estos manifiestan que cada año se debe realizar nuevamente el proceso de una manera impresa y física, comprometiendo tiempo en dicho trámite. Es aquí donde se ve como mejora continua implementar la herramienta tecnológica que propenderá por optimizar y dar un valor agregado mayor al proceso de entrega.

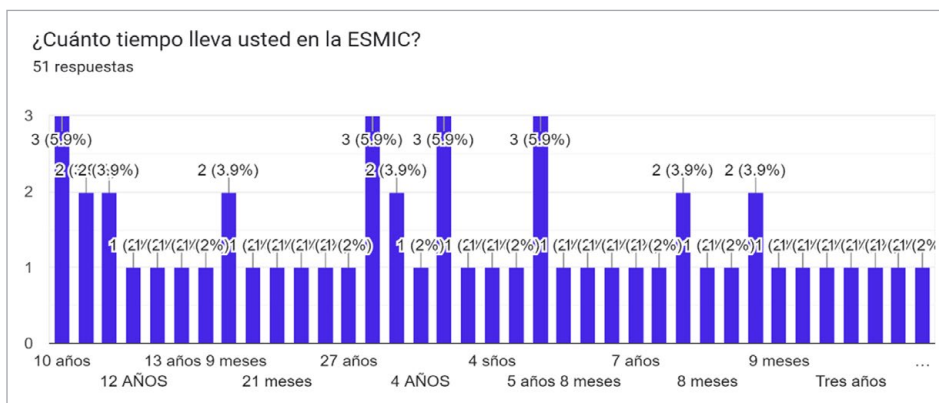


Figura 4. Permanencia en la ESMIC como docente.

Nota: Periodos de duración de los docentes ESMIC.

Fuente: Elaboración propia.



Podemos deducir que el docente que más años lleva trabajando en la ESMIC tiene 27 años y el que menos lleva tiene ocho meses. Por tal razón, se logra identificar que tienen un tiempo importante en la institución; esto permite una objetividad en la percepción del manejo de los procedimientos en las facultades. El proceso de contratación, según los docentes, ha mejorado con el paso del tiempo en la selección y entrega de documentos a las facultades. Ahora, y con Respecto de las nuevas tecnologías, es una gran oportunidad de mejora la implementación de la tecnología en la parte administrativa.

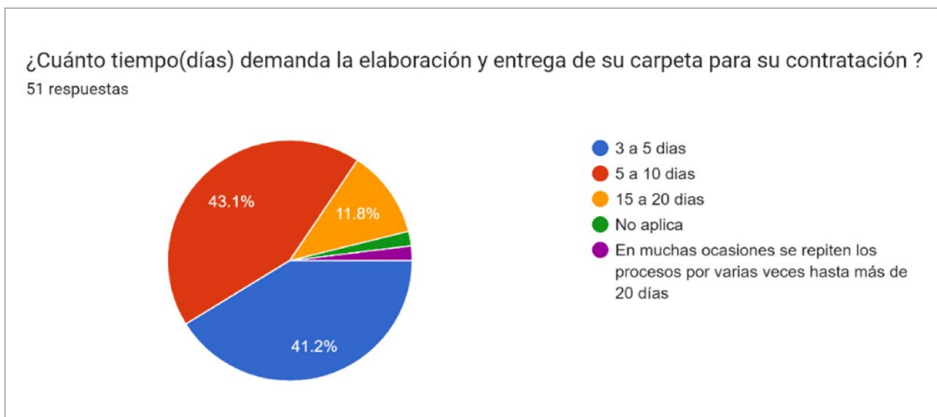


Figura 5. Cantidad en días para el proceso de contratación.

Nota: Porcentaje de entrega y duración en tiempo de la documentación que debe rendirse para la contratación.

Fuente: Elaboración propia.

Los datos recolectados evidencian la oportunidad de mejora que puede presentarse conforme a la problemática actual y la necesidad de una plataforma que brinde agilidad y seguridad. Los resultados reflejados conforme al tiempo son: el 43,1 % de los encuestados afirmó que la recepción de la documentación tarda entre cinco y diez días, mientras que el 41,2 % indicó un periodo de tres a cinco días. Por último, 11,8 % señaló demoras de entre 15 y 20 días. Por esta razón, implementar una herramienta tecnológica es una solución viable y oportuna para optimizar el tiempo y la celeridad del proceso. De igual forma, emplear tecnología en el proceso de contratación permite actualizar los procesos y procedimientos en cada una de las facultades, brindando aún más bienestar y celeridad en la contratación para los docentes.

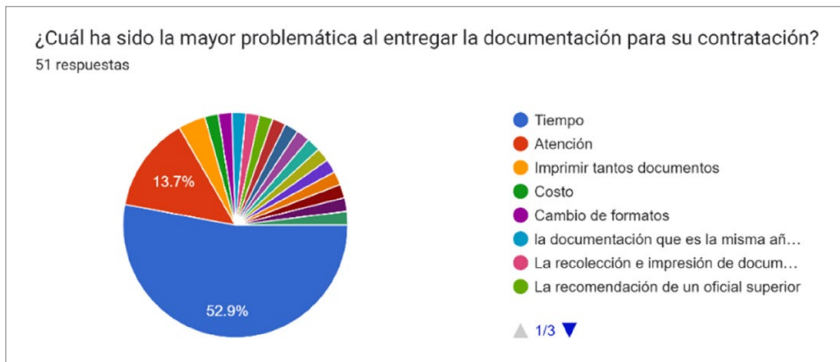


Figura 6. Variables de problemática en la entrega de documentación en la contratación.

Nota: Categorías predominantes en la esencia del problema de contratación.

Fuente: Elaboración propia.

Al observar la Figura 6, es preciso señalar que el indicador fundamental y vital para los medios tecnológicos en la optimización de un proceso tiene que ver con el tiempo de respuesta y la agilidad. Muestra de lo anterior es el dato imperante que se mencionó. Por tal razón, un componente tecnológico ayuda a subsanar este aspecto y de la misma forma contribuye a las facultades en la consolidación y objetividad en la recopilación y selección de la información para la contratación. Aranda (2021) dice lo siguiente: “Es claro que la tecnología acerca, de alguna manera, a los que se encuentran lejos. Esto beneficia la celebración masiva de contratos, puesto que suprime las distancias en que se encuentran las partes y permite disminuir los gastos de contratación” (p. 10).



Figura 7. Opinión sobre el implemento de una herramienta tecnológica.

Nota: Tipo de aceptación que tendría el implementar o proponer una herramienta tecnológica que permita optimizar el proceso de contratación docente.

Fuente: Elaboración propia.



Finalmente, la propuesta de solución cuenta con una gran aprobación, dado que el 86,3 % de la población encuestada afirmó aceptar la idea de incluir una herramienta tecnológica en el proceso de contratación. Esto otorga una claridad específica a nuestra propuesta. Lo anterior demuestra que la tecnología es un aspecto fundamental en todas las organizaciones y la mejora continua de los procesos institucionales. Ariza (2022) afirma que:

Hablar de “nuevas tecnologías” resulta ambiguo y, a su vez, complejo en la actualidad, en la medida en que el sentido de novedad cada vez es más relativo para el ser humano y para la industria. Sin embargo, a través de ese concepto, pretendemos hacer referencia a aquellas nuevas técnicas o medios que tienen el potencial de crear una nueva industria o de transformar una existente y que, de acuerdo con González et al. (1996), citado por Prendes (1997, p. 35), han sido definidas como el “conjunto de procesos y productos derivados de las nuevas herramientas (*hardware* y *software*), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de información” (p. 4).

Instrumento tecnológico para la optimización de la contratación docente

EduDocente Connect

Objetivo general

Desarrollar un prototipo de una aplicación web de gestión docente y postulación, denominada EduDocente Connect, diseñada para simplificar y agilizar los procesos administrativos y de postulación en el ámbito educativo, proporcionando a los docentes y a la institución una plataforma intuitiva y eficiente.

Descripción

En nuestro compromiso por ofrecer una solución eficiente y accesible, hemos optado por utilizar WordPress como la base para el desarrollo de este prototipo. WordPress nos brinda la flexibilidad y la robustez necesarias para crear una plataforma intuitiva y totalmente funcional que se adapte a las necesidades específicas del sector educativo. Entre las características principales de nuestra aplicación web de gestión docente y postulación se incluyen:

- Gestión de datos docentes: Los docentes podrán gestionar y actualizar fácilmente su información personal, académica y laboral, garantizando que sus perfiles estén siempre actualizados y completos.
- Compartir documentos importantes: La plataforma permitirá a los usuarios compartir documentos relevantes, como certificados académicos, *curricu-*



lum vitae y cartas de presentación, entre otros, de manera segura y rápida.

- Sistema de postulación simplificado: Facilitaremos el proceso de postulación a nuevas oportunidades docentes mediante un sistema intuitivo y fácil de usar. Los docentes podrán buscar y aplicar a puestos vacantes de manera eficiente, optimizando así su búsqueda de empleo.
- Notificaciones y alertas: Implementaremos un sistema de notificaciones y alertas que mantendrá a los usuarios informados sobre actualizaciones importantes, fechas límite de postulación y cambios en el estado de sus aplicaciones, entre otros.
- Diseño *responsive* y amigable: Nuestra plataforma estará diseñada para ser totalmente *responsive*, lo que garantizará una experiencia de usuario óptima en dispositivos móviles y de escritorio. Además, nos aseguraremos de que el diseño sea intuitivo y fácil de navegar para usuarios de todos los niveles de habilidad tecnológica.

En el siguiente ítem se visualizarán las historias de usuarios que se tendrán para la creación del *software*:

Historia de usuario para docente

Yo como: Docente. Quiero: Iniciar sesión o registrarme en la plataforma para acceder a las funcionalidades personalizadas y gestionar mi información de manera segura.

Descripción

Como docente, necesito tener la capacidad de iniciar sesión en la plataforma si ya tengo una cuenta o registrarme si soy nuevo usuario. Esto me permitirá acceder a las funciones específicas destinadas a los docentes y gestionar mi información personal, académica y laboral de manera segura.

Requerimiento funcional

- La plataforma debe contar con un sistema de autenticación que permita a los docentes iniciar sesión con sus credenciales o registrarse si aún no tienen una cuenta.
- Debe existir un formulario de registro que solicite la información necesaria para crear una cuenta de docente, como nombre, correo electrónico, contraseña, etc.
- Una vez autenticado, el docente debe tener acceso a un panel de control personalizado donde pueda ver y editar su información.



Criterios de aceptación

- Los docentes deben poder iniciar sesión correctamente utilizando sus credenciales existentes.
- Los nuevos docentes deben poder registrarse satisfactoriamente en la plataforma.
- Después de iniciar sesión, los docentes deben ser redirigidos a un panel de control donde puedan ver y editar su información personal.

Requerimientos no funcionales

- Seguridad: el sistema de autenticación debe ser seguro y proteger la información confidencial de los docentes.
- Usabilidad: el proceso de inicio de sesión y registro debe ser intuitivo y fácil de entender para los usuarios.

Historia de usuario para postulante

Yo como: Postulante. Quiero: Iniciar sesión o registrarme en la plataforma para explorar oportunidades de docencia y realizar postulaciones de manera eficiente.

Descripción

Como postulante interesado en oportunidades de docencia, necesito tener la capacidad de iniciar sesión en la plataforma si ya tengo una cuenta o registrarme si soy un nuevo usuario. Esto me permitirá explorar las oportunidades de docencia disponibles y realizar postulaciones de manera eficiente.

Requerimiento funcional

- La plataforma debe contar con un sistema de autenticación que permita a los postulantes iniciar sesión con sus credenciales o registrarse si aún no tienen una cuenta.
- Debe haber una sección dedicada para que los postulantes exploren las oportunidades de docencia disponibles, con descripciones detalladas de los puestos.
- Debe existir un proceso simplificado de postulación que permita a los postulantes enviar sus datos y adjuntar los documentos necesarios.

Criterios de aceptación

- Los postulantes deben poder iniciar sesión correctamente utilizando sus credenciales existentes.



- Los nuevos postulantes deben poder registrarse satisfactoriamente en la plataforma.
- Los postulantes deben poder explorar las oportunidades de docencia disponibles y acceder a descripciones detalladas de los puestos.
- Los postulantes deben poder completar el proceso de postulación, enviando sus datos y adjuntando los documentos necesarios.

Requerimientos no funcionales

- El sistema de autenticación y la transmisión de datos deben ser seguros para proteger la información personal de los postulantes.
- Eficiencia: El proceso de registro y postulación debe ser rápido y fácil de usar para los postulantes.

Historia de usuario para administrador

Yo como: Administrador. Quiero: Iniciar sesión para gestionar las postulaciones y la información de los docentes para revisar y gestionar eficientemente las postulaciones y mantener actualizada la información de los docentes.

Descripción

Como administrador de la plataforma, necesito tener la capacidad de iniciar sesión para acceder a las funcionalidades destinadas a la gestión de postulaciones y la información de los docentes. Esto me permitirá revisar, aprobar o rechazar las postulaciones, así como mantener actualizada la información de los docentes pertenecientes a la institución.

Requerimiento funcional

- La plataforma debe contar con un sistema de autenticación que permita al administrador iniciar sesión con credenciales específicas.
- Debe haber una sección dedicada para que el administrador acceda a una vista completa de las postulaciones registradas en la institución.
- Debe existir la capacidad de revisar, aprobar o rechazar las postulaciones, así como gestionar la información de los docentes.

Criterios de aceptación

- El administrador debe poder iniciar sesión correctamente utilizando sus credenciales específicas.
- El administrador debe poder acceder a una vista completa de las postulaciones registradas.



- El administrador debe poder revisar, aprobar o rechazar las postulaciones de manera eficiente.
- El administrador debe poder gestionar la información de los docentes pertenecientes a la institución.

Requerimientos no funcionales

- Seguridad: El sistema de autenticación y la gestión de datos deben ser seguros para proteger la información confidencial de los docentes y postulantes.
- Eficiencia: La interfaz de usuario para la gestión de postulaciones y la información de los docentes debe ser fácil de usar y eficiente.

Se realizan los *mockups*: inicio de sesión de los usuarios.

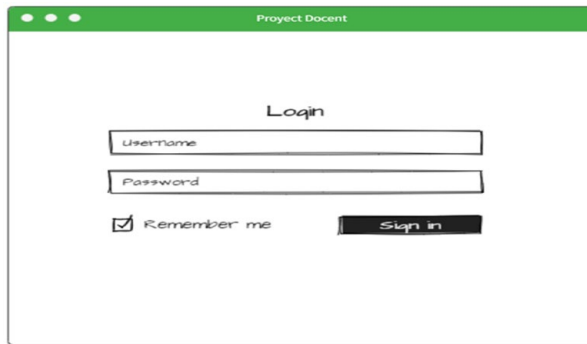


Figura 8. Imagen representativa del modelo de la plataforma.

Nota: Los *mockups* son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.

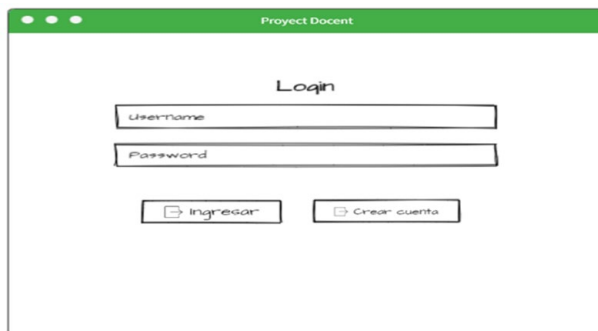
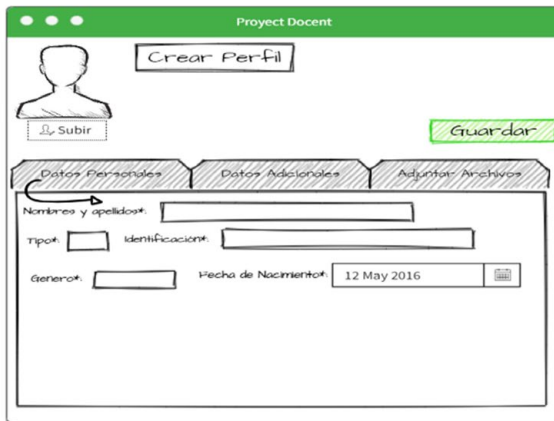


Figura 9. Imagen representativa del modelo de la plataforma.

Nota: Los *mockups* son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.



Estas pantallas consisten en crear el perfil del Docente candidato, digitando los datos personales, datos adicionales, soportes como cedula, experiencias, diplomas.

Figura 10. Imagen representativa del modelo de la plataforma.

Nota: Los *mockups* son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.

Perfil de un docente que se está inscribiendo y perfil de un docente para subir documentación para actualizar datos:

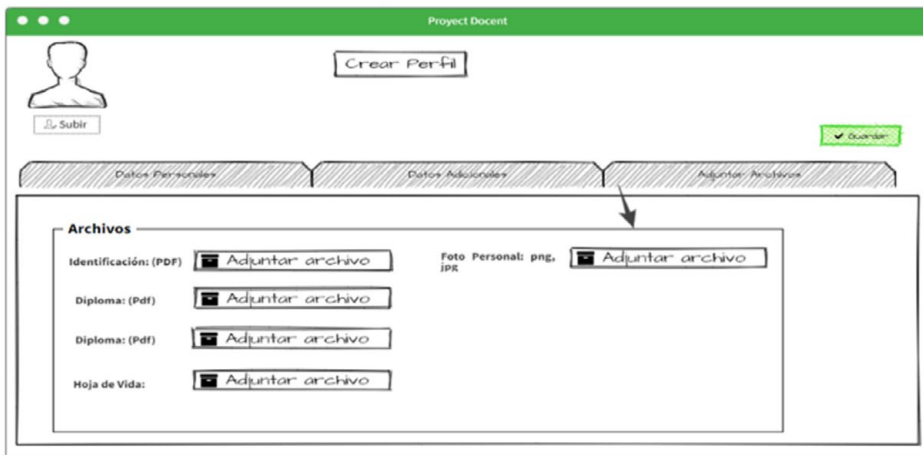


Figura 11. Imagen representativa del modelo de la plataforma.

Nota: Los *mockups* son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.



Rol administrador

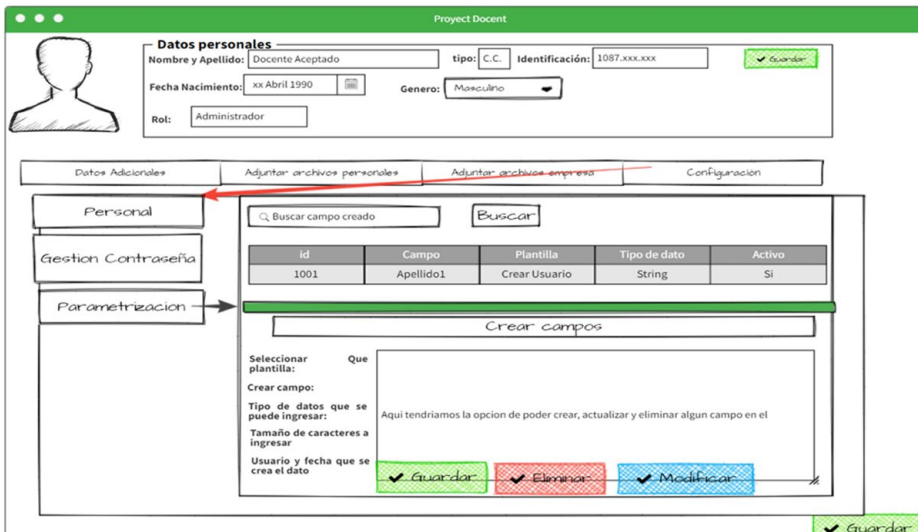


Figura 12. Imagen representativa del modelo de la plataforma.

Nota: Los mockups son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.

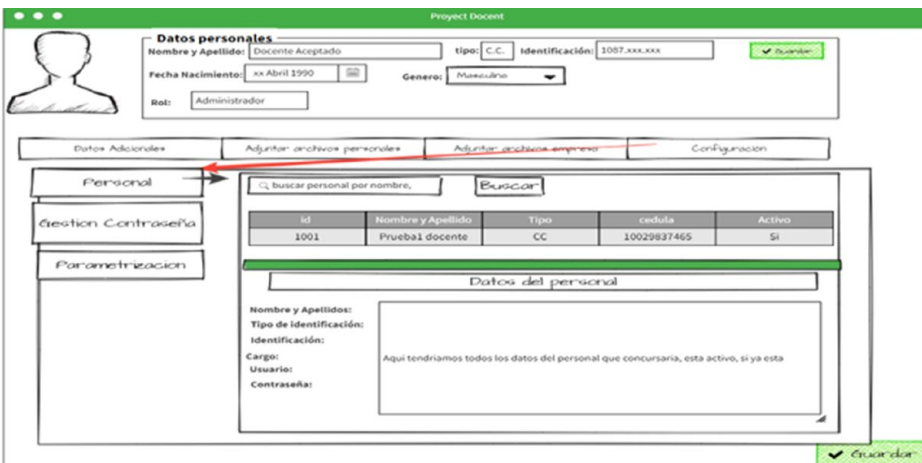


Figura 13. Imagen representativa del modelo de la plataforma.

Nota: Los mockups son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.



Figura 14. Imagen representativa del modelo de la plataforma.

Nota: Los mockups son un modelo que se utiliza para representar de forma rápida el resultado final de un diseño. En este caso, vemos reflejado el resultado de la plataforma por proponer.

Fuente: Elaboración propia.

El administrador podrá modificar, crear o quitar campos que sean pertinentes o no al momento de las postulaciones de los docentes.

Glosario

Mockups: representaciones visuales aproximadas de un producto, generalmente utilizadas en las etapas iniciales del diseño para demostrar el diseño, la funcionalidad y el flujo de una interfaz de usuario o un objeto físico. Pueden crearse utilizando diversas herramientas, desde simples bocetos en papel hasta *software* de diseño digital sofisticado. Los *mockups* ayudan a diseñadores, desarrolladores y partes interesadas a visualizar y refinar el concepto antes de invertir tiempo y recursos en un desarrollo detallado.

WordPress: popular sistema de gestión de contenidos (CMS) de código abierto que permite a los usuarios crear y gestionar sitios web y blogs. Lanzado inicialmente como una plataforma de blogs en 2003, WordPress ha evolucionado hacia una herramienta versátil que



impulsa una parte significativa de la web. Proporciona una interfaz fácil de usar, amplias opciones de personalización a través de temas y complementos, y un sólido soporte comunitario. WordPress se utiliza para diversos fines, incluyendo blogs personales, sitios web empresariales, tiendas de comercio electrónico, portafolios y más.

Administrador: el usuario administrador podrá cambiar los permisos de los módulos que requiera modificar, así como añadir campos que necesite que el docente postulante pueda visualizar cuando ingrese con su perfil.

Credenciales

existentes: el docente postulante debe comenzar por completar sus datos personales iniciales y luego crear su usuario como postulante. Una vez registrado, será dirigido a una página de inicio de sesión, donde podrá ingresar su cédula y contraseña para acceder a la plataforma y cargar todos los documentos pertinentes.

Conclusiones

- El proceso de contratación debe ser conforme a unos perfiles que se adapten al entorno castrense y que tengan formación en otras disciplinas.
- Es vital optimizar el proceso de contratación docente, ya que la ESMIC inicia primero que otros institutos de educación superior.
- Al poseer un diseño de herramienta tecnológica, se busca que el proceso de contratación evolucione y ofrezca una prospectiva para ser empleado en el futuro.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. Los puntos de vista y los resultados de este artículo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes. No se emplearon herramientas de generación de contenido por inteligencia artificial (IA) para su elaboración.

Sobre los autores

Ricardo Andrés Bernal Vallarino. Teniente Coronel (R) del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacional. Especialista en Administra-



ción de Recursos para la Defensa. Profesional en Ciencias Militares, administrador de empresas. Docente investigador, ESMIC.

Orcid: <https://orcid.org/0000-0003-3160-6518>

Contacto: ricardo.bernal@esmic.edu.co

Esteban Dario Maigual Maigual. Alférez de la Escuela Militar de Cadetes "General José María Córdova".

Contacto: esteban.maigual@esmic.edu.co

Cristian Horacio Pérez Navarro. Alférez de la Escuela Militar de Cadetes "General José María Córdova".

Contacto: cristhian.perez@esmic.edu.co

Referencias

- Álvarez Enríquez, G. F. (2021). El enfoque ciencia-tecnología-sociedad en la gestión del talento humano docente. *Revista Universidad y Sociedad*, 13(1), 150-158.
- Ángeles, M. (13 de noviembre de 2023). *Propuesta de implementación de software para la mejora del proceso de reclutamiento y selección de docentes en una empresa de capacitaciones del rubro de transporte y telecomunicaciones en Lima Metropolitana*. Universidad Peruana de Ciencias Aplicadas.
- Ariza Vesga, R. A. (2022). Nuevas perspectivas del uso de la tecnología en el ámbito del contrato de seguro. *Revista Ibero-Latinoamericana de Seguros*, 31(57), 13-48. <https://doi.org/10.11144/Javeriana.ris57.nput>
- Cazau, P. (2006). *Introducción a la investigación en ciencias sociales*. <https://bit.ly/4b82d3m>
- Chaveco Castillo, A. (2020, 18 de diciembre). Labor educativa del docente militar: sus contradicciones sociales. *Revista de Investigación, Formación y Desarrollo: Generando Productividad Institucional*, 8(3).
- Escuela Militar de Cadetes "General José María Córdova". (2007). *Evolución histórica de la Escuela Militar de Cadetes* (Tomo 1). Imprenta Nacional de Colombia.
- Escuela Militar de Cadetes "General José María Córdova". (s. f.). *Programa de Ingeniería Civil*. <https://esmic.edu.co/academia/programa-de-ingenieria-civil/72>
- Escuela Militar de Cadetes "General José María Córdova", Facultad de Ciencias Militares. (2022, 27 de enero). *Proyecto educativo del programa*.
- Figuroa, M. J., García, S., Maldonado, D., Rodríguez, C., & Saavedra, A. M. (2018, mayo). *La profesión docente en Colombia: normatividad, formación, selección y evaluación*. Universidad de los Andes, Escuela de Gobierno Alberto Lleras Camargo.
- Hernández Sampieri, R., & Mendoza, C. P. (2008). *La investigación mixta: una estrategia*. <https://bit.ly/4b6vQ9r>
- Madrigal, D. (2024). *Diferencia generacional en la educación militar*. Sello Editorial ESMIC.
- Ministerio de Defensa Nacional. (2021). *Política de educación para la Fuerza Pública (PEFuP) 2021-2026: hacia una educación diferencial y de calidad*.
- Ministerio de Educación Nacional. (s. f.). *Contratación de docentes*. <https://bit.ly/3wK8VfJ>



- Mirón, M. (2019). La guerra irregular, insurgencias y cómo contrarrestarlas. *Revista Científica General José María Córdova*, 17(27), 457-480. <https://doi.org/10.21830/19006586.497>
- Ospina, H. T. (2012, 18 de junio). *Modelo de sistema experto para la selección de personal docente universitario*. Instituto Tecnológico Metropolitano.
- Sánchez, J. (2013). *El método de proyectos en la investigación tecnológica*. <http://bit.ly/3xZ1tS3>
- Sanromán Aranda, R., & Ruiz Reynoso, A. M. (2021). La contratación en la época contemporánea y la tecnología. *Revista de Derecho Privado*, (20), 107-128. <https://doi.org/10.22201/ijj.24487902e.2021.20.18670>
- UNESCO. (2025, 1 de junio). *La selección, contratación y asignación del profesorado*. Instituto Internacional de Planeamiento de la Educación de la UNESCO. <https://learningportal.iiep.unesco.org/es/fichas-praticas/mejorar-el-aprendizaje/la-seleccion-contratacion-y-asignacion-del-profesorado>
- Valderrama, B. (2019, 12 de abril). *Transformación digital y organizaciones ágiles*. Universidad Tecnológica Intercontinental.
- Zikmund, W. (2007). *Essentials of marketing research*. South-Western College Pub.



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, pp. 65-68


Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.170>

DOSIER

Reseña de libro: El derecho internacional humanitario y Juego de tronos

Juan Fernando Gil Osorio 

Escuela Militar de Cadetes "General José María Córdova"

RESUMEN

Este artículo realiza un análisis del libro *El derecho internacional humanitario y Juego de Tronos*, en el cual se plantea una metodología innovadora para la enseñanza del derecho internacional humanitario (DIH). La obra, compuesta por trece capítulos interdisciplinarios, establece un puente entre los sucesos narrativos de la saga *Game of Thrones* y las normas que regulan los conflictos armados. Se abordan temas clave como ética de la guerra, perfidia, trato a prisioneros, tácticas bélicas y rol de las mujeres en escenarios de violencia. Este análisis destaca cómo la ficción puede convertirse en una herramienta pedagógica rigurosa para reflexionar sobre la evolución, legitimidad y desafíos contemporáneos del DIH en la docencia y la investigación.

PALABRAS CLAVE

conflicto armado; Derecho Internacional Humanitario; enseñanza jurídica; *Game of Thrones*

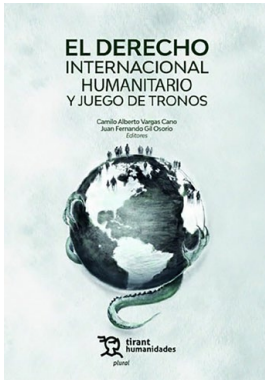
CITACIÓN APA

Gil Osorio, J. F. (2025). Reseña de libro: *El derecho internacional humanitario y Juego de tronos*. *Revista Brújula de Investigación*, 13(25), 65-68.

<https://doi.org/10.21830/23460628.170>

Recibido: 15 de abril 2025 **Aceptado:** 20 de junio de 2025

Contacto: Juan Fernando Gil Osorio  juan.gil@esmic.edu.co



Libro: ***El derecho internacional humanitario y Juego de tronos***

Editores del libro: **Camilo Alberto Vargas Cano - Juan Fernando Gil Osorio**

Editorial: Tirant Humanidades

Año: 2025

ISBN impreso: 978-84-1081-134-8

Páginas: 372

En tiempos en que la enseñanza del derecho internacional humanitario (DIH) enfrenta el reto de conectar con nuevas generaciones, hablar de él, desde un camino alternativo e innovador, como es el paralelismo entre escenarios ficticios y reales, se posiciona como una estrategia clave para la comprensión de los fenómenos complejos como el conflicto armado. Al respecto, la obra académica *Derecho internacional y Juego de tronos*, publicada por el sello editorial Tirant Humanidades, en colaboración con la Academia Colombiana de Derecho Internacional (Accoldi), se ubica como una apuesta metodológica valiosa en la literatura jurídica contemporánea, donde se crea un puente entre el universo ficticio de Westeros y los principios normativos que rigen los conflictos armados en el mundo real.

Este libro surge como un ejercicio colectivo de producción académica realizado por expertos de múltiples disciplinas, con un claro interés y pasión por esta saga, que se propusieron explorar las complejas interrelaciones entre la realidad y la narrativa literaria desde un plano jurídico. Se compone de trece capítulos donde se aborda el DIH a través de un análisis detallado de eventos emblemáticos de la serie *Game of Thrones (GOT)*, tales como “La boda roja”, y distintos personajes creados por George R. R. Martin, quienes se vieron envueltos en los acontecimientos vividos en Westeros. Entre estos personajes, se encuentran Eddard Stark, Jaime Lannister, Sansa Stark, Cersei Lannister y Daenerys Targaryen.

Es así como desde el primer capítulo, “Reflexiones sobre derecho internacional humanitario en Game of Thrones”, hasta el último, “El rol de las mujeres líderes en la serie de Game of Thrones”, se analizan las acciones, decisiones y estrategias desarrolladas por cada uno de estos personajes, evaluando su ajuste con las normas internacionales establecidas para humanizar los conflictos armados. Se estudian aspectos como la ética de la guerra, la perfidia, las masacres, las capturas, las tácticas bélicas, estrategias, métodos y técnicas de guerra, como también las obligaciones de las par-



tes beligerantes, los derechos de los prisioneros en el marco de conflicto y la transición de las formas de combate en cada época; todo ello, desde una analogía con las dinámicas reales que han marcado la historia del conflicto armado.

Ahora bien, uno de los aspectos más destacados de esta obra es su enfoque multidimensional, que no solo ofrece un estudio profundo de los derechos humanos en contextos de conflicto armado, sino que también incorpora una perspectiva de género que permite entender cómo estas realidades han estado atravesadas por expresiones de desigualdad y violencia de género. Esto abre nuevas líneas de investigación y reflexión respecto de las violaciones al DIH y la aplicación de sus principios en contextos ficticios y reales.

Adicionalmente, esta obra cuestiona la idea de que los principios del DIH son exclusivamente producto de la modernidad, pues se remonta a las tradiciones filosóficas y normativas anteriores al modelo westfaliano, aportando una mayor profundidad al estudio jurídico y debate contemporáneo sobre la evolución y legitimidad del derecho internacional.

En términos metodológicos, este libro combina un análisis descriptivo y comparativo que permite evaluar de manera rigurosa los eventos narrativos de la serie *Game of Thrones* desde una mirada jurídica que ahonda sobre los eventos, estrategias y decisiones que marcaron el accionar de los personajes bajo el marco normativo del DIH. Esto demuestra cómo las narrativas de ficción pueden servir como herramientas útiles de aprendizaje y enseñanza de los principios jurídicos, como también de su aplicación en contextos complejos y hostiles como el conflicto armado, estimulando la reflexión sobre los dilemas morales que se presentan alrededor de estos.

Es necesario enfatizar que este libro fue sometido a un proceso de evaluación riguroso que asegura su calidad y relevancia académica, y le permite posicionarse como una contribución significativa e innovadora para el estudio y enseñanza del derecho internacional humanitario, ya que es un instrumento interesante para docentes, estudiantes y estudiosos del derecho internacional.

En conclusión, el libro *El derecho internacional humanitario y Juego de tronos* demuestra que la intersección entre el derecho internacional y la producción cultural contemporánea no solo es viable como sucede en este caso con la saga *Game of Thrones*, sino que es intelectualmente productiva al utilizar el escenario fantástico como un marco de análisis y crítica a la normatividad aplicable en contextos bélicos, lo que no solo enriquece el conocimiento popular para aquellos aficionados de la saga, sino que además invita a una reflexión sobre los desafíos alrededor de la aplicación del DIH. De ahí que se considere que es una contribución original para el campo del derecho internacional humanitario, que trasciende las fronteras disciplinarias tradicionales y redefine la forma como se aprende el derecho en la actualidad.



Sobre el autor

Juan Fernando Gil Osorio. Doctor en Derecho, Universidad Externado de Colombia. Magíster en Derechos Humanos y Democratización, Universidad Externado de Colombia y Universidad Carlos III de Madrid. Abogado. Exdecano de la Facultad de Derecho, Escuela Militar de Cadetes "General José María Córdova". Investigador Junior reconocido y categorizado por MinCiencias. Docente investigador, ESMIC.

<https://orcid.org/0000-0002-6605-6846>

Contacto: juan.gil@esmic.edu.co



Accede a toda la producción académica de la Escuela Militar de Cadetes "General José María Córdova" mediante este código QR o ingresando a la página www.brujuladesemilleros.com

