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

Examining Face Recognition Technologies and Privacy: Ethical and Legal Choices

María Del Pilar Castro Arellano[1], María Del Pilar Quezada Castro[2], Eliana Maritza Barturen Mondragón[3], Martha Olga Marruffo Valdivieso[4], José Rolando Cárdenas Gonzáles[5], and Guillermo Alexander Quezada Castro[6*]

[1]Professor, Universidad Alas Peruanas, Perú. maripili_1728_19@hotmail.com, https://orcid.org/0000-0002-6661-9928

[2]Professor, Universidad Tecnológica Del Perú, Perú. c20853@utp.edu.pe, https://orcid.org/0000-0002-1012-570X

[3]Professor, Universidad Señor De Sipán, Perú. barturenm@uss.edu.pe, https://orcid.org/0000-0002-0458-1637

[4]Professor, Universidad Señor De Sipán, Perú. marrufovm@uss.edu.pe, https://orcid.org/0000-0001-6635-6454

[5]Professor, Universidad Señor De Sipán, Perú. cardenajose@uss.edu.pe, https://orcid.org/0000-0002-8141-9086

[6*]Professor, Universidad Tecnológica Del Perú, Perú. c21331@utp.edu.pe, https://orcid.org/0000-0002-4868-1664

Received: July 16, 2024; Revised: August 24, 2024; Accepted: September 26, 2024; Published: November 30, 2024

Abstract

Facial recognition technologies exist in society. When they were implemented, it was not considered that the use of this technology could lead to a breach of privacy of the individual. Not all countries have specific regulations and there is no standard to determine its international feasibility. This study presents the bibliometric and content analysis of scientific production in Scopus and Web of Science. A total of 169 documents published between 2000 and 2023 were identified. It was found that the most frequently used terms are privacy, facial recognition, surveillance, and security. It was concluded that there is legal and ethical debate because there is no clear protection of human rights for the misuse of this technology.

Keywords: Rights, Privacy, Technology, Surveillance.

1 Introduction

Facial recognition technology has experienced exponential growth in recent years. It is now feasible to be used in mobile devices and applications. Although the rationale for this is diverse, there is literature that accredits its integration with human and everyday activities (Kostka, et al., 2021). The boundary of their use is not unanimously defined because there is research that reflects fears about infringement of

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 360-376. DOI: *10.58346/JISIS.2024.I4.022*

*Corresponding author: Professor, Universidad Tecnológica Del Perú, Perú.

privacy or surveillance of enclosed spaces. Consent is not always sought for the voice and image of the person, a situation that generates debate (Brey, 2004; De Andrade et al., 2013).

Research is also recorded that encompasses the public's perception of facial recognition. User attitudes were analyzed and it was noted that there is a way to go, focusing on technical and ethical aspects (Alkishri et al., 2024). There is a need for trust and confidence at the technological level, which is possible through the protection of civil rights against the misuse of this innovation implemented in society (Kostka et al., 2023; Bradford et al., 2020; Ho et al., 2020; Shore, 2022).

In the literature review, few studies on the legal framework for the use of facial recognition are recognized. The innovation also leads to the existence of marginalized groups in this technology (Xiaoling & Zeming, 2024; Kumar et al., 2023). In this sense, it creates an environment conducive to the lack of privacy protection due to the use and a challenge to regulate behaviors that violate rights, respecting the culture of each country (Ringel & Reid, 2023; Espindola, 2023; Li et al., 2023; Gidaris, 2023).

In the same vein, it is mentioned that previous studies explored public attitudes. These changed as easy recognition was implemented in different demographic groups (Amraee & Koochari, 2014; Ghaforiyan & Emadi, 2016). However, little is known about the reasons or justification for accepting the evolution of this technology (Chen & Wang, 2023; Kostka, 2023).

The lack of regulation on facial recognition generates debate, especially if it may exist or vary from country to country. In this scenario, the need arises to identify the balance between the innovation produced by technology and the protection of the privacy of the individual. It is not advisable to be guided only by algorithms; it is necessary to assess the effects on populations to avoid the multiplicity of cases based on ignorance of the subject (Raposo, 2024).

In this order of ideas, the present study is based on the bibliometric and content analysis of facial recognition and its relationship with privacy (Ramos, 2020). This research is in the area of computer science, which is encompassed by the integration of computing with everyday environments. The purpose of this study is to encourage future research with a multidisciplinary approach.

2 Research Methodology

The aim of the research is to identify the scientific output of face recognition technologies and privacy in two databases in the period 2015-2023.

Bibliometric Analysis of Two Databases

This study considered the two most representative and multidisciplinary databases that bring together a diversity of high-impact journals: Scopus and Web of Science (WoS). The bibliometric analysis of facial recognition technology and privacy is based on the quantitative method and applies to the scientific production of the selected topic (Archambault et al., 2009).

Search Strategy

In Scopus: (TITLE-ABS-KEY ("Facial Recognition Technology" and privacy)). The initial result was 118 documents. In Wos: TOPIC ("Facial Recognition Technology" and privacy)). The initial result was 51 documents.

Inclusion and Exclusion Criteria

Table 1 details the inclusion and exclusion criteria for the 2 selected databases.

Table 1: Criteria

Criteria	Inclusion	Exclusion
Database	Scopus WoS (core collection)	Other databases
Document Type	Article, Conference Paper, Book Chapter, Review, Conference Review,	Book, Editorial, Note, Short Survey.
Publication Stage	Final	Article in Press
Source type	Journal, Conference proceeding	Book Series, Book, Trade Journal
Period	2000-2023	Another period

Tools for Data Analysis

Microsoft Excel and R-studio 4.1.0 software, the bibliometrix package, and the Biblioshiny interface were used for data analysis (Aria & Cuccurullo, 2017).

Bibliometric Indicators

Table 2 shows the bibliometric indicators used (Ardanuy, 2012).

Table 2: Identification of Problems, Objectives, and Indicators

Research Problem	Aims	Bibliometric Indicator
RQ1: What is the annual scientific output on face recognition technologies and privacy in the period 2000 to 2023?	To identify the annual scientific output on face recognition technologies and privacy in the period 2000 to 2023.	Production: Diachronic productivity and keywords.
RQ2: What are the most relevant sources of annual scientific output on face recognition technologies and privacy in the period 2000 to 2023?	To identify the most relevant sources of annual scientific output on face recognition technologies and privacy in the period 2000 to 2023.	Collaborative: Most prolific authors and most collaborative network
RQ3: What is the scientific output in countries on face recognition technologies and privacy in the period 2000 to 2023?	Identify the scientific production in countries on face recognition technologies and privacy in the period 2000 to 2023.	Visibility: Most productive journals on the topic and most productive countries.
RQ4: Which are the 10 institutions that stand out in scientific production on face recognition technologies and privacy in the period 2000 to 2023?	Identify the 10 institutions that stand out in the scientific production of face recognition technologies and privacy in the period 2000 to 2023.	Visibility: Most cited documents and keywords
RQ5: What are the 10 most cited papers on face recognition technologies and privacy in the period 2000 to 2023?	Identify the 10 most cited papers on face recognition technologies and privacy in the period 2000 to 2023.	Collaborative: Most prolific countries.
RQ6: What are the most commonly used words in the scientific output on face recognition technologies and privacy in the period 2000 to 2023?	Identify the most used words in the scientific production on face recognition technologies and privacy in the period 2000 to 2023.	Visibility: Most cited documents and keywords
RQ7: What is the collaborative network of authors publishing on face recognition technologies and privacy in the period 2000 to 2023?	Identify the collaborative network of authors publishing on face recognition technologies and privacy in the period 2000 to 2023.	Collaborative: Most prolific authors and most collaborative network
RQ8: What are the most prominent topics in the scientific output on face recognition technologies and privacy in the period 2000 to 2023?	Identify the topics that stand out in the scientific production on face recognition technologies and privacy in the period 2000 to 2023.	Collaborative: Most prolific authors and most collaborative network

In this sense, it can be seen that the credibility of the present study is supported by:

- The selection of the two most representative multidisciplinary databases.
- The clear and precise identification of the search formula.
- Use of specialized software - bibliometrix.
- Quantitative and qualitative analysis of the scientific production.

3 Results

Annual Scientific Production

Figure 1 a) shows the scientific production in Scopus and Figure 1 b) corresponds to the Web of Science. In the first case, the oldest article corresponds to 2000. In the second case, this has been the case since 2011. In the period 2016 to 2019, the production in the 2 selected databases was incipient. The analysis shows that there is a trend towards an increase from 2020. This result coincides with the period of the COVID-19 pandemic.

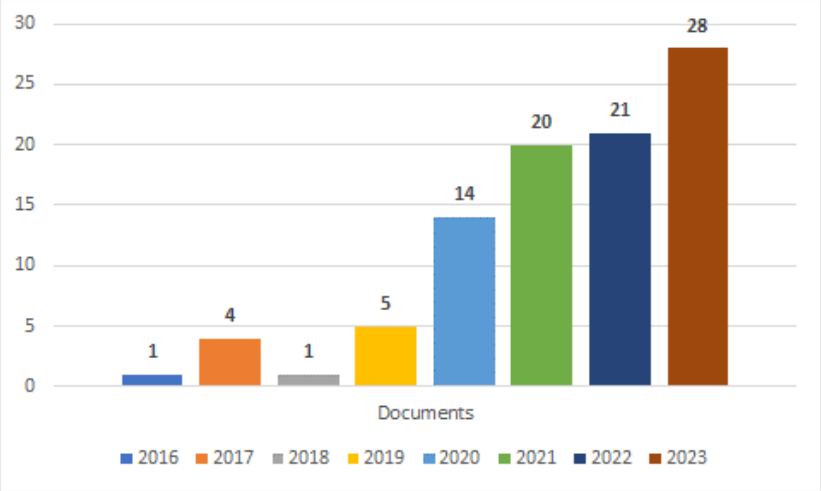

Figure 1: a) Scientific Production in Scopus

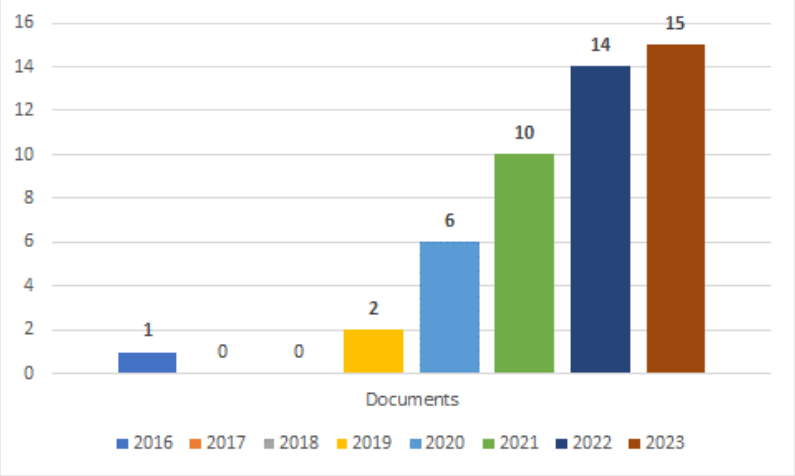

Figure 1: b) Scientific Production in WoS

Most Productive Sources

Table 3 shows that the journal Computer Law and Security Review has an H-index of 49, belongs to quartile 1, and has been registered in Scopus since 1985. The subject areas of the journal are Business, Management and Accounting, Computer Science, and Law. Likewise, the journal IFIP Advances in Information and Communication Technology has an H-index of 60, belongs to quartile 3, and has been registered in Scopus since 2000. The subject area of the journal is Computer Science and Decision Sciences. Similarly, the journal Government Information Quarterly has an H-index of 123, belongs to quartile 1 and has been registered in Scopus since 1984. The subject area of the journal is Social Sciences.

Table 4 shows that the journal Computer Law & Security Review has an Impact Factor of 2.9, belonging to quartile 1 in SSCI (Social Sciences Citation Index). The first record of the journal in this database was in 2014. Likewise, the journal Government Information Quarterly has a 7.8 Impact Factor, it belongs to quartile 1 in SSCI (Social Sciences Citation Index). The journal was first registered in 1997.

Table 3: Most Productive Sources in Scopus

N	Sources	Documents
1	Facial Recognition Technology: Best Practices, future uses and Privacy Concerns	9
2	Computer Law and Security Review	4
3	IFIP Advances in Information and Communication Technology	3
4	Privacy, Technology, and the Criminal Process	3
5	Acm International Conference Proceeding Series	2
6	Data and Policy	2
7	Government Information Quarterly	2
8	Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	2
9	Surveillance and Society	2
10	14th Cmi International Conference - Critical ICT Infrastructures and Platforms, Cmi 2021 - Proceedings	1

Table 4: Most Productive Sources in WoS

N	Sources	Documents
1	Computer Law & Security Review	4
2	Government Information Quarterly	2
3	Texas Law Review	2
4	Ai & Society	1
5	Air & Space Law	1
6	Alternative Law Journal	1
7	American Journal of Medical Genetics Part C-Seminars in Medical Genetics	1
8	Applied Sciences-Basel	1
9	Boston University Law Review	1
10	British Journal of Criminology	1

Country Scientific Production

Figure 2(a) shows the scientific output of the Scopus database. The United States stands out and occupies the first place. Australia, China, and India have the characteristics that they share second place. Canada is in third place. It can also be seen that South Africa, Portugal, Mexico, Ireland, France, Brazil, and Argentina are starting their interest in the topic of facial recognition technology and privacy.

Figure 2(b) shows the scientific output in the Web of Science. The United States is in first place. It can be seen that Australia, China, and Canada will increase their output in the coming years. In addition, Saudi Arabia, Mexico, Malaysia, France, and Denmark are starting to take an interest in the topic of facial recognition technology and privacy.

Figure 2: a) Country Scientific Production in Scopus

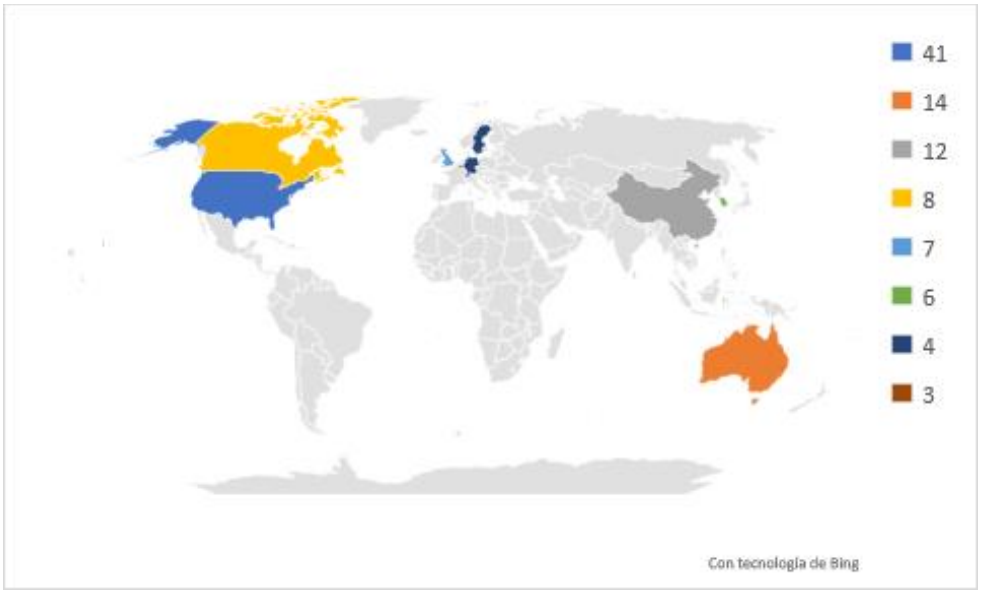

Figure 2: b) Country Scientific Production in WoS

Most Relevant Affiliations

Table 5 shows the 10 institutions that stand out for their scientific production on face recognition technology and privacy. It can be seen that Stanford University stands out in the two databases that were compared. In the case of WoS, there is a slight distance in the amount of scientific production. In the case of Scopus, this is not observed because the results between the institutions are very close.

Table 5: Comparison

Scopus		WoS	
Affiliation	**Documents**	**Affiliation**	**Documents**
University of Ontario Institute of Technology	8	Stanford University	10
University of Monastir	6	Monash University	4
Monash University	5	University California San Francisco	4
Ucsi University	5	University St Gallen	4
University of Toronto	5	Katholieke University Leuven	3
Hong Kong University of Science and Technology	4	Sun Yat Sen University	3
Huazhong University of Science and Technology	4	Sungkyunkwan University	3
University of California	4	University Gothenburg	3
University of Chicago	4	University Nevada	3
University of Gothenburg	4	Australian Natl University	2

Most Global Cited Documents

Table 6 lists the 10 most cited papers on facial recognition technology and privacy available in the Scopus database. The most cited is entitled Our Biometric Future: Facial Recognition Technology and the Culture of surveillance. Published in 2011, it argues that the incorporation of biometrics is a reality and that privacy will have to be adapted to security measures. This is necessary to avoid situations similar to the fateful event that occurred on 11 September in the United States with the attack on the Twin Towers (Turley, 2020).

Table 7 lists the 10 most cited papers on facial recognition technology and privacy that are available in the Web of Science database. The most cited is entitled Facial recognition technology can expose political orientation from naturalistic facial images Facial recognition technology can expose political orientation from naturalistic facial images. Published in 2021, it focuses on the identification of political orientation from facial recognition, an interaction that should not neglect privacy protection.

The most productive author in the two selected databases is Genia Kotska. Her research includes the book Between Security and Convenience: Facial Recognition Technology in the eyes of citizens in China, Germany, The United Kingdom, and The United States, which has 38 citations in Scopus and 28 citations in WoS.

Table 6: Documents in Scopus

Titles	DOI	Total Citations
Our biometric future: Facial recognition technology and the culture of surveillance	NA	232
The Death of Privacy?	10.2307/1229519	205
Cancelable biometrics realization with multispace random projections	10.1109/TSMCB.2007.903538	135
Facial recognition technology can expose political orientation from naturalistic facial images	10.1038/s41598-020-79310-1	56
Urban surveillance and panopticism: Will we recognize the facial recognition society?	10.24908/ss.v1i3.3343	49
Privacy Preserving Face Recognition Utilizing Differential Privacy	10.1016/j.cose.2020.101951	46
Assisting Users in a World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications	10.1109/CVPRW.2017.181	46
The ethical application of biometric facial recognition technology	10.1007/s00146-021-01199-9	38
Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States	10.1177/09636625211001555	38
Ethical aspects of facial recognition systems in public places	10.1108/14779960480000246	37

Table 7: Documents in WoS

Titles	DOI	Total Citations
Facial recognition technology can expose political orientation from naturalistic facial images	10.1038/s41598-020-79310-1	44
The ethical application of biometric facial recognition technology	10.1007/s00146-021-01199-9	32
Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States	10.1177/09636625211001555	28
Surveillance Policy Making by Procurement	NA	28
"I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance	10.1002/asi.24342	23
Facial Recognition Technology: A Primer for Plastic Surgeons	10.1097/PRS.0000000000005673	20
Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police use of New Technology	10.1093/bjc/azaa032	18
Say cheese! Privacy and facial recognition	10.1016/j.clsr.2011.09.011	13
"All the Better to See You with, My Dear": Facial Recognition and Privacy in Online Social Networks	10.1109/MSP.2013.22	11
Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring	NA	9

Word Cloud

Figure 3 (a) shows the most frequently used words in the scientific production in Scopus. The use of the words privacy, facial recognition, surveillance, security, data protection, biometrics, policing, privacy concerns, human rights, law enforcement, personal data, and technology stands out (Dokmanović & Cvetićanin, 2023).

Figure 3(b) shows the most frequently used words in scientific production in the Web of Science. The use of the words facial recognition technology, privacy, surveillance, data protection, security, artificial intelligence, policing, human rights, civil law, criminal law and ethics, law, legitimacy, public opinion, smart cameras, technology, and trust stand out.

Figure 3: a) Word Cloud in Scopus

Figure 3: b) Word Cloud in WoS

Collaboration Network

Figure 4 a) shows the collaboration between authors who published their scientific output in Scopus. It can be seen that in the red cluster, the authors Liu J., Wang M. and Chen W. interact. In the blue cluster, authors Kostka G., Meckel M., and Steinacker I. interact. In the green cluster interact authors Kasturi R., Mohanty P., and Sarkar S.

Figure 4 b) shows the collaboration between authors who published their scientific output on the Web of Science. It can be seen that in the red cluster, the authors Kotska G., Meckel M., and Steinacker I. interact. In the green cluster interact authors Anderton J, Claes P, Cook-Deegan R, Doerr M, and Evans BJ. In the pink cluster interact authors Aboujaoude E, Boscardin WJ, Brown JEH, and Hallgrímsson B. In the grey cluster interact authors Bragias A, Fleet R, and Hine K.

Figure 4: a) Authors in Scopus

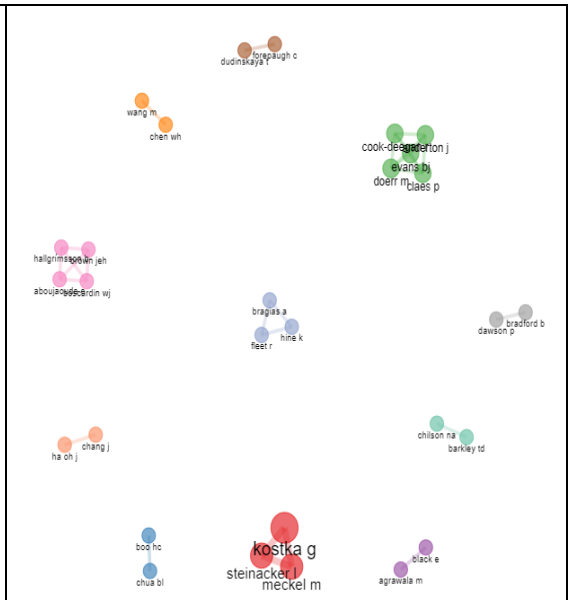

Figure 4: b) Authors in WoS

Identification of the topics according to the scientific production of the 2 selected databases. Table 8 contains the classification of the themes according to the scientific production of Scopus and Web of Science. Authors related to the common themes are recognized. This information will allow us to go deeper into the topic of facial recognition technology and privacy. It will also help to identify future lines of research.

Table 8: Common Themes

Subject	Authors
Police and surveillance use	(Dauvergne, 2022; Hutchins & Andrejevic, 2021; Eneman et al., 2022; Murphy & Estcourt, 2020; Daly, 2017).
Ethical and privacy concerns	(Palmiotto & Gonzalez, 2023; Santos & Rapp, 2019; Nam, 2020; De Vries & Schinkel, 2019; Faraldo Cabana, 2023).
Legal regulation and policy frameworks	(Sarabdeen, 2022; Chan, 2021; Wilkinson, 2020; Froomkin, 2000; Teoh & Yuang, 2007).
Public attitudes and perceptions	(Bragias et al., 2021; Katsanis et al., 2021; Yang et al., 2021; Shaikh & Moran, 2024; Duckworth & Krieger, 2021).
Commercial and retail uses	(Wang et al., 2023; Pantano et al., 2023; Feng & Xie, 2019).
Justice and guaranteeing rights	(Das et al, 2017; Shao et al., 2021).

Table 9 shows the authors' opinions on the use of facial recognition technologies and human rights. These opinions help to identify the relevance of the topic and the ethical and legal concerns regarding the regulatory gaps in different countries.

Table 9: Authors' Opinions

Country	Opinions	Authors
China	High public acceptance. Less privacy concerns. Learn-by-doing regulatory approach.	(Kostka et al., 2023; Shi et al., 2024)
European Union	Strict regulatory approach. Strong protection of personal data. Tendency to restrict the use of facial recognition technology.	(Montasari, 2024; Kavoliūnaitė-Ragauskienė, 2024)
United States	Self-regulatory approach. Concern for privacy and civil rights. Regulation in public and private sectors.	(Kiotska et al., 2023; Chen & Wong, 2023)
United Kingdom	Middle ground on public acceptance. Balance between security and privacy.	(Kostka et al., 2023)
Germany	Low public acceptance. Strong emphasis on privacy protection.	(Kostka et al., 2023)
Saudi Arabia	Adoption for public services and surveillance. Less concern for privacy than in the West.	(Alqarni et al. 2023)
South Korea	Increasing use of recognition technology. Need to improve data protection legislation.	(Kim et al., 2023)
Ukraine	Use of facial recognition technology in the context of war. New ethical and privacy challenges.	(Espindola, 2023)

4 Discussion

About the surveillance factor, there is research that identifies the potential danger of using facial recognition technologies for surveillance. It is argued that there is a tendency towards discriminatory practice and infringement of civil rights. It is also reported that biometric surveillance has been implemented in stadiums and that this generates controversy in terms of respecting the privacy of each

individual. In the same vein, it is mentioned that there is a need to standardize legislation to preserve the balance between security and privacy protection (Raposo, 2024; Dauvergne, 2022; Daly, 2017; Stark et al., 2020).

From the literature review, these authors are recognized because their arguments represent the starting point for the regulation of the use of facial recognition technologies. Understandably, the authorities implement guidelines to protect the community from various crimes; however, it is necessary to remember that every action has limits. In this case, the main limit is privacy, which should not be violated by the misuse of this technology (Kosinski, 2021; Smith & Miller, 2022).

The European Court of Human Rights has ruled that the use of facial recognition technologies is incompatible with human rights. Likewise, there is research that specifies that images are a latent risk to people's privacy. In light of this, authors argue that the use of technologies should not promote the denaturalization of the presumption of innocence (Palmiotto & Gonzalez, 2023; Faraldo Cabana, 2023).

In this respect, a new concern arises among the authors about the presumption of innocence. It is important to recognize that society requires peace and tranquillity, but this must be in balance with the fundamental rights and constitutional guarantees that each country recognizes in the face of charges for the alleged commission of a crime. To hold otherwise could affect the dignity of the person (Haider AbdAlkreem et al., 2024).

In this vein, research has identified that current laws are not adequate to regulate and sanction cases arising from facial recognition technologies. Laws and biometrics do not strike a balance between security and privacy. This is because there are no internal policies in countries to identify the risks and benefits for society. It is advisable to disseminate the advantages and disadvantages of the use of this technology to the population. Only in this way will it be possible to act against the violation of rights (Li et al., 2023; Sarabdeen, 2022; Chan, 2021; Froomkin, 2000; Teoh & Yuang, 2007; Kim et al., 2023).

Public perception regarding the implementation of facial recognition technologies is important to consider to build trust and transparent use for the benefit of the community. In the health sector, the patient must be aware of the benefits derived from this technology. The media can contribute to the dissemination of the limits of its use (Kostka et al., 2021; Bragias et al., 2021; Katsanis et al., 2021; Yang et al., 2021; Shaikh & Moran, 2024).

From a commercial perspective, it is important to note that there is research that considers it essential to incorporate a method for the use of facial recognition technologies. Also, it is up to the user to decide on his or her protection against possible privacy violations (Kostka et al., 2023; Wang et al., 2023; Pantano et al., 2023; Feng & Xie, 2019; Zuo et al., 2019; Buckley & Hunter, 2011; Boo & Chua, 2022; Andrejevic & Volcic, 2021).

The rise of facial recognition technologies is notorious. This gives rise to due attention to cybersecurity and criminal justice protection from attacks by criminals. It is important to ensure that there is an effective state response to rights violations in the country (Ringel & Reid, 2023; Das et al., 2017; Shao et al., 2021; Greiffenhagen et al., 2023; Yang et al., 2023).

From the literature review, it is clear that several countries are in legal and ethical disputes over the issue of facial recognition technology and human rights.

In the United States, there is an ongoing debate about the effectiveness of facial recognition technology and the protection of civil rights, which is why there is a need for stricter regulation in order to protect the privacy of citizens (Chen & Wang, 2023; Kostka et al., 2023).

In the European Union, there is also strict regulation related to privacy protection. There is an ongoing debate between the use of facial recognition technology and respect for human rights (Montasari, 2024; Kavoliūnaitė-Ragauskienė, 2024).

In the UK, an intermediate position emerges and the debate includes the identification of ethical and legal boundaries in the use of facial recognition technologies (Kostka et al., 2023).

China is characterized by the widespread use of facial recognition technologies for surveillance. This situation raises international concerns about the protection of human rights (Kostka et al., 2023; Shi et al., 2024; Weber et al., 2020).

In Ukraine, the use of facial recognition technology in the context of war can be seen, as a situation that gives rise to new conflicts about the international protection of human rights (Espindola, 2023).

In South Korea, there is a need to improve legislation to establish a balance between the use of facial recognition technologies and human rights (Kim et al., 2023).

In relation to developing countries, it is recorded that legislations are not consolidated for the implementation of the use of facial recognition technologies, so there is a likelihood of cases of human rights violations (Dauvergne, 2022).

Thus, it can be seen that the common denominator in the countries mentioned in Table 9 is the protection of human rights in the use of facial recognition technologies; however, there are new challenges related to national security, freedom of expression, and the abuse of technology by governments. It is important to take this into account to strengthen democracy in society.

5 Conclusion

It was found that scientific production on facial recognition technologies and privacy has increased since 2020 and that they are found in books or articles in high-impact journals.

The United States leads in scientific production in the Scopus and Web of Science databases. Stanford University is the most prominent institution. The most cited document is the book entitled Our biometric future: Facial recognition technology and the culture of surveillance, published in 2011. Genia Kotska is the most cited author in the 2 selected databases.

The most used words in the 2 selected databases are privacy, surveillance, data protection, security, policing, and technology. The collaborative network between authors in Scopus is formed by Liu J., Wang M. and Chen W; Kostka G., Meckel M. and Steinacker I.and Kasturi R., Mohanty P. and Sarkar S. For Web of Science it is Anderton J, Claes P, Cook-Deegan R, Doerr M and Evans BJ; Aboujaoude E, Boscardin WJ, Brown JEH and Hallgrímsson B and Bragias A, Fleet R and Hine K.

The themes of scientific output in the 2 selected databases were identified as surveillance, ethics and privacy, legal regulation, public perceptions, commercial use, and justice and the guarantee of rights.

The implementation of facial recognition technologies is optimal. Research supports their presence because they provide surveillance of the population. However, there is still a legal and ethical debate as the protection of human rights is not standardized. Privacy is a right that could be affected by the misuse of this technology.

The effectiveness of facial recognition technologies at the contractual level is proposed as a future line of research. There is a need to understand their application for staff working and being productive from home or remotely.

References

[1] Alkishri, W., Widyarto, S., & Yousif, J. H. (2024). Evaluating the Effectiveness of a Gan Fingerprint Removal Approach in Fooling Deepfake Face Detection. *Journal of Internet Services and Information Security (JISIS)*, *14*(1), 85-103. https://doi.org/10.58346/JISIS.2024.I1.006

[2] Alqarni, A. M., Timko, D., & Rahman, M. L. (2023, August). Saudi Arabian perspective of security, privacy, and attitude of using facial recognition technology. In *2023 20th Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1-12). IEEE. https://doi.org/10.1109/PST58708.2023.10320185

[3] Amraee, M., & Koochari, A. (2014). Face recognition using a training sample from each individual. *International Academic Journal of Innovative Research, 1*(2), 6–13.

[4] Andrejevic, M., & Volcic, Z. (2021). "Smart" cameras and the operational enclosure. *Television & New Media*, *22*(4), 343-359. https://doi.org/10.1177/1527476419890456

[5] Archambault, É., Campbell, D., Gingras, Y., & Larivière, V. (2009). Comparing bibliometric statistics obtained from the Web of Science and Scopus. *Journal of the American society for information science and technology*, *60*(7), 1320-1326. https://doi.org/10.1002/asi.21062

[6] Ardanuy, J. (2012). Brief introduction to bibliometrics. *The scopus database and other CBUES e-resources as a tool for managing research activity; 1*.

[7] Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics*, *11*(4), 959-975. https://doi.org/10.1016/j.joi.2017.08.007

[8] Boo, H. C., & Chua, B. L. (2022). An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore. *International Journal of Contemporary Hospitality Management*, *34*(11), 4052-4079. https://doi.org/10.1108/IJCHM-12-2021-1471

[9] Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, *60*(6), 1502-1522. https://doi.org/10.1093/bjc/azaa032

[10] Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research*, *22*(6), 1637-1654. https://doi.org/10.1080/15614263.2021.1942873

[11] Brey, P. (2004). Ethical aspects of facial recognition systems in public places. *Journal of information, communication and ethics in society*, *2*(2), 97-109. https://doi.org/10.1108/14779960480000246

[12] Buckley, B., & Hunter, M. (2011). Say cheese! Privacy and facial recognition. *Computer Law & Security Review*, *27*(6), 637-640. https://doi.org/10.1016/j.clsr.2011.09.011

[13] Chan, G. K. (2021). Towards a calibrated trust-based approach to the use of facial recognition technology. *International Journal of Law and Information Technology*, *29*(4), 305-331. https://doi.org/10.1093/ijlit/eaab011

[14] Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

[15] Daly, A. (2017). Privacy in automation: An appraisal of the emerging Australian approach. *Computer Law & Security Review*, *33*(6), 836-846. https://doi.org/10.1016/j.clsr.2017.05.009

[16] Das, A., Degeling, M., Wang, X., Wang, J., Sadeh, N., & Satyanarayanan, M. (2017, July). Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (pp. 1387-1396). IEEE. https://doi.org/10.1109/CVPRW.2017.181

[17] Dauvergne, P. (2022). Facial recognition technology for policing and surveillance in the Global South: a call for bans. *Third World Quarterly*, *43*(9), 2325-2335. https://doi.org/10.1080/01436597.2022.2080654

[18] De Andrade, N. N. G., Martin, A., & Monteleone, S. (2013). " All the better to see you with, my dear": Facial recognition and privacy in online social networks. *IEEE security & privacy*, *11*(3), 21-28. https://doi.org/10.1109/MSP.2013.22

[19] De Vries, P., & Schinkel, W. (2019). Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms. *Big Data & Society*, *6*(1), 2053951719851532. https://doi.org/10.1177/2053951719851532

[20] Dokmanović, M., & Cvetićanin, N. (2023). Regulation of the use of facial recognition technology–limitations and challenges from a human rights perspective. *Teorija in praksa*, (3), 548-564. https://doi.org/10.51936/tip.60.3.548

[21] Duckworth, A., & Krieger, J. (2021). 'The world will be watching and so will NSA!': A History of Technology and Security at the Olympic Games. *The International Journal of the History of Sport*, *38*(2-3), 264-281. https://doi.org/10.1080/09523367.2021.1909574

[22] Eneman, M., Ljungberg, J., Raviola, E., & Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities 1. *Information Polity*, *27*(2), 219-232. https://doi.org/10.3233/IP-211538

[23] Espindola, J. (2023). Facial recognition in war contexts: Mass surveillance and mass atrocity. *Ethics & International Affairs*, *37*(2), 177-192. https://doi.org/10.1017/S0892679423000151

[24] Faraldo Cabana, P. (2023). Technical and legal challenges of the use of automated facial recognition technologies for law enforcement and forensic purposes. In *Artificial Intelligence, social harms and human rights* (pp. 35-54). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-19149-7_2

[25] Feng, Y., & Xie, Q. (2019). Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps. *Journal of Interactive Advertising*, *19*(1), 43-57. https://doi.org/10.1080/15252019.2018.1521317

[26] Froomkin, A. M. (2000). The death of privacy? *Stanford Law Review*, *52*, 1461-1543.

[27] Ghaforiyan, H., & Emadi, M. (2016). Human face recognition under pose variation with fusion geometric methods. *International Academic Journal of Science and Engineering*, *3*(1), 214–223.

[28] Gidaris, C. (2023). The Problem with Regulating Facial Recognition Technology in a Digital Culture of Visibility. *Canadian Journal of Communication*, *48*(1), 124-141. https://doi.org/10.3138/cjc.2022-0030

[29] Greiffenhagen, C., Xu, X., & Reeves, S. (2023). The Work to Make Facial Recognition Work. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW1), 1-30. https://doi.org/10.1145/3579531

[30] Haider AbdAlkreem, M., Sadoon Salman, R., & Khiled Al-Jibory, F. (2024). Detect People's Faces and Protect Them by Providing High Privacy Based on Deep Learning. *Tehnički glasnik*, *18*(1), 92-99. https://doi.org/10.31803/tg-20231210183347

[31] Ho, D. E., Black, E., Agrawala, M., & Fei-Fei, L. (2020). Evaluating facial recognition technology: a protocol for performance assessment in new domains. *Denv. L. Rev.*, *98*, 753-773.

[32] Hutchins, B., & Andrejevic, M. (2021). Olympian surveillance: Sports stadiums and the normalization of biometric monitoring. *International Journal of Communication*, *15*, 363-382.

[33] Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J., ... & Wagner, J. K. (2021). A survey of US public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PloS one*, *16*(10), e0257923. https://doi.org/10.1371/journal.pone.0257923

[34] Kavoliūnaitė-Ragauskienė, E. (2024). Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union. *Journal of Human Rights Practice*, *16*(2), 658-674. https://doi.org/10.1093/jhuman/huad065

[35] Kim, M. W., Kim, I. H., Kim, J., Oh, J. H., Chang, J., & Park, S. (2023). A study on the protection of biometric information against facial recognition technology. *KSII Transactions on Internet and Information Systems (TIIS)*, *17*(8), 2124-2139. https://doi.org/10.3837/tiis.2023.08.009

[36] Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific reports*, *11*(1), 100. https://doi.org/10.1038/s41598-020-79310-1

[37] Kostka, G. (2023). Digital doubters in different political and cultural contexts: Comparing citizen attitudes across three major digital technologies. *Data & Policy*, *5*, e27. https://doi.org/10.1017/dap.2023.25

[38] Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671-690. https://doi.org/10.1177/09636625211001555

[39] Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

[40] Kumar, A., Joshi, P., Bala, A., Sudhakar Patil, P., Jang Bahadur Saini, D. K., & Joshi, K. (2023). Smart Transaction through an ATM Machine using Face Recognition. *Indian Journal of Information Sources and Services*, *13*(2), 7-13.

[41] Li, Z., Guo, Y., Yarime, M., & Wu, X. (2023). Policy designs for adaptive governance of disruptive technologies: The case of facial recognition technology (FRT) in China. *Policy Design and Practice*, *6*(1), 27-40. https://doi.org/10.1080/25741292.2022.2162248

[42] Montasari, R. (2024). The Impact of Facial Recognition Technology on the Fundamental Right to Privacy and Associated Recommendations. In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses* (pp. 259-270). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-50454-9_13

[43] Murphy, J. R., & Estcourt, D. (2020). Surveillance and the state: body-worn cameras, privacy and democratic policing. *Current Issues in Criminal Justice*, *32*(3), 368-378. https://doi.org/10.1080/10345329.2020.1813383

[44] Nam, S. (2020). Bend and Snap: Adding Flexibility to the Carpenter Inquiry. *Colum. JL & Soc. Probs.*, *54*, 131-167.

[45] Palmiotto, F., & González, N. M. (2023). Facial recognition technology, democracy and human rights. *Computer Law & Security Review*, *50*, 105857. https://doi.org/10.1016/j.clsr.2023.105857

[46] Pantano, E., Vannucci, V., & Marikyan, D. (2023). Gratifications in change of privacy? The response of four consumers' generational cohorts toward facial recognition technology in retail settings. *Journal of Consumer Behaviour*, *22*(2), 288-299. https://doi.org/10.1002/cb.2124

[47] Ramos, L. F. M. (2020, September). Evaluating privacy during the COVID-19 public health emergency: the case of facial recognition technologies. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 176-179). https://doi.org/10.1145/3428502.3428526

[48] Raposo, V. L. (2024). 'Look at the camera and say cheese': the existing European legal framework for facial recognition technology in criminal investigations. *Information & Communications Technology Law*, *33*(1), 1-20. https://doi.org/10.1080/13600834.2023.2239621

[49] Ringel, E., & Reid, A. (2023). Regulating Facial Recognition Technology: A Taxonomy of Regulatory Schemata and First Amendment Challenges. *Communication Law and Policy*, *28*(1), 3-46. https://doi.org/10.1080/10811680.2023.2180271

[50] Santos, C., & Rapp, L. (2019). Satellite imagery, very high-resolution and processing-intensive image analysis: Potential risks under the GDPR. *Air and Space Law*, *44*(3), 275-295. https://doi.org/10.54648/aila2019018

[51] Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3). https://doi.org/10.1016/j.heliyon.2022.e09086

[52] Shaikh, S. J., & Moran, R. E. (2024). Recognize the bias? News media partisanship shapes the coverage of facial recognition technology in the United States. *New Media & Society*, *26*(5), 2829-2850. https://doi.org/10.1177/14614448221090916

[53] Shao, X. F., Li, Y., Suseno, Y., Li, R. Y. M., Gouliamos, K., Yue, X. G., & Luo, Y. (2021). How does facial recognition as an urban safety technology affect firm performance? The moderating role of the home country's government subsidies. *Safety science*, *143*, 105434. https://doi.org/10.1016/j.ssci.2021.105434

[54] Shi, J., Hu, X., & Guo, X. (2024). The lesser of two evils: Assessing the public acceptance of AI thermal facial recognition during the COVID-19 crisis. *Risk Analysis*, *44*(4), 958-971. https://doi.org/10.1111/risa.14198

[55] Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

[56] Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, *37*(1), 167-175. https://doi.org/10.1007/s00146-021-01199-9

[57] Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "i don't want someone to watch me while i'm working": Gendered views of facial recognition technology in workplace surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1074-1088. https://doi.org/10.1002/asi.24342

[58] Teoh, A. B. J., & Yuang, C. T. (2007). Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *37*(5), 1096-1106. https://doi.org/10.1109/TSMCB.2007.903538

[59] Turley, J. (2020). Anonymity, obscurity, and technology: Reconsidering privacy in the age of biometrics. *Boston University Law Review*, *100*, 2179-2261.

[60] Wang, M., Qin, Y., Liu, J., & Li, W. (2023). Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks. *Humanities and Social Sciences Communications*, *10*(1), 1-15. https://doi.org/10.1057/s41599-023-01673-3

[61] Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, *20*, 565-587. https://doi.org/10.1007/s10660-020-09422-3

[62] Wilkinson, S. (2020). Artificial intelligence, facial recognition technology and data privacy. *Journal of Data Protection & Privacy*, *3*(2), 186-198.

[63] Xiaoling, X., & Zeming, F. (2024). Multi-Modal Emotional Understanding in AI Virtual Characters: Integrating Micro-Expression-Driven Feedback within Context-Aware Facial Micro-Expression Processing Systems. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *15*(3), 474-500. http://doi.org/10.58346/JOWUA.2024.I3.031

[64] Yang, X., Mei, H., & Zheng, Y. (2023). Understanding the antecedents of privacy fatigue in facial recognition-based m-Gov services: An empirical study from China. *Government Information Quarterly*, *40*(3), 101827. https://doi.org/10.1016/j.giq.2023.101827

[65] Yang, Y., Yin, D., Easa, S. M., & Liu, J. (2021). Attitudes toward Applying Facial Recognition Technology for Red-Light Running by E-Bikers: A Case Study in Fuzhou, China. *Applied Sciences*, *12*(1), 211. https://doi.org/10.3390/app12010211

[66] Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial recognition technology: a primer for plastic surgeons. *Plastic and reconstructive surgery*, *143*(6), 1298e-1306e. https://doi.org/10.1097/PRS.0000000000005673

Authors Biography

María Del Pilar Castro Arellano, is a Social Worker, Lawyer, and Degree in Tourism, Hotel Management and Gastronomy. She holds a Master's in Civil Law and a Doctorate in Law. She teaches at the Universidad Alas Peruanas and Universidad Tecnológica del Perú. She has experience in writing scientific articles in different journals. She has experience as a thesis advisor. She is a specialist in Family Law. She is a researcher recognized by CONCYTEC - Peru and is a level V.

María Del Pilar Quezada Castro, is a lawyer, Master's in Civil Law and Doctor in Education. She studied Tourism, Hotel Management, and Gastronomy at the Universidad de Huánuco. Arbitrator with Register N° 884. Extrajudicial Conciliator with Register N° 49392. She is the Professional School of Law academic coordinator at the Universidad Tecnológica del Perú. She has experience in writing scientific articles. She teaches courses on Family Law, Personal Law, and Introduction to Law. She is a researcher recognized by CONCYTEC - Peru and holds level V.

Eliana Maritza Barturen Mondragón, is a full-time professor at the Universidad Señor de Sipán and a part-time professor at the Universidad Tecnológica del Perú. She holds a doctorate in education. She has a master's degree in economic sciences with a mention in taxation, and graduated from the Universidad Nacional de Trujillo. She is a candidate for a master's degree in constitutional law. She is a lawyer and has a bachelor's degree in accounting. She is currently working as a lawyer for the law firm Mondragón Jimenez. She belongs to the NGO Sunqu Sinchi. She is a researcher recognized by CONCYTEC - Peru and holds level VI.

Martha Olga Marruffo Valdivieso, Lawyer, Master in Public Management. University lecturer. Research Coordinator of the Professional School of Law of the Universidad Señor de Sipán, Peru.

José Rolando Cárdenas Gonzáles, Lawyer, Master in Parliamentary Law, Elections and Legislative Studies at the Complutense University of Madrid and Master in Constitutional Law at the University of Castilla La Mancha. Specialist in Human Rights and Constitutional Justice, Interpretation and Application of the Constitution from the University of Castilla La Mancha. Director of Chornancap Revista Jurídica del Ilustre Colegio de Abogados de Lambayeque. Full-time lecturer at the Postgraduate School of the Universidad Señor de Sipán, Peru.

Guillermo Alexander Quezada Castro, Lawyer, Master in Civil Law, and PhD student in Legal Research. He has experience in writing scientific articles. He has experience as a leader of research groups and research workshops. He teaches at the Universidad Tecnológica del Perú and Universidad Alas Peruanas. He has experience as a thesis advisor. He is a researcher recognized by CONCYTEC-Peru and is a level IV.