Personal Data Protection in the Era of Digital Surveillance: A Bibliometric Analysis of Scientific Production (2014–2024)

Vidnay Noel Valero-Ancco*
Universidad Nacional del Altiplano, Peru

Yolanda Lujano-Ortega
Universidad Nacional del Altiplano, Peru.

Katty Maribel Calderon-Quino
Universidad Nacional del Altiplano, Peru.

Fredy Sosa Gutierrez
Universidad Nacional del Altiplano, Peru.

Miryam Pari-Orihuela
Universidad Nacional del Altiplano, Peru.

Sonia Bustinza-Choquehuanca
Universidad Nacional del Altiplano, Peru.

Valero-Ancco, Vidnay Noel et al. Personal Data Protection in the Era of Digital Surveillance: A Bibliometric Analysis of Scientific Production (2014–2024). *Revista Electrónica de Ciencia Penal y Criminología*. 2025, núm. 27-01, pp. 1-18.

Abstract: In today's digital era, the protection of personal data has become a pressing challenge in the face of emerging surveillance technologies that threaten fundamental rights and citizens' informational autonomy. The widespread implementation of tracking systems, artificial intelligence, and mass monitoring raises urgent questions about privacy, regulation, and the control of personal information. In this context, the aim of this article is to identify the scientific production published between 2014 and 2024 related to the protection of personal data within the framework of digital surveillance. A bibliometric review study was conducted using the Scopus database, analyzing indicators of productivity, impact, keyword co-occurrence, and thematic, geographic, and institutional distribution. The results reveal an interdisciplinary field, heavily concentrated in Global North countries, with publication peaks driven by specific events such as the COVID-19 pandemic and the implementation of the GDPR. Gaps were also identified in the representation of Global South regions and in the critical analysis of part of the literature. The study concludes that there is a need strengthen international cooperation and to develop comprehensive regulatory frameworks to effectively safeguard privacy in digitized environments.

Keywords: Data Protection; Digital Surveillance; Privacy; Bibliometrics; Artificial Intelligence.

Received Date: 25 August 2025
Date of Publication in RECPC: 10 October 2025
Contact: vvalero@unap.edu.pe

I. **Introduction**

The protection of personal data has emerged as a central topic in the discussion on human rights and technology, particularly in a context characterized by the rise of digital surveillance. The theoretical foundations of this study are based on the respect for privacy and informational self-determination, principles recognized as fundamental rights in multiple international conventions. According to [1], the right to privacy has been undermined by practices of mass surveillance that blur the line between security and freedom, posing new regulatory challenges. Additionally, [2]highlight the lack of clear regulations regarding surveillance technologies, which generates significant risks to human rights and underscores the need for a robust theoretical framework to guide privacy protection in the digital era. Likewise,[3] provides an analysis of the rule of law in the context of the COVID-19 pandemic, where emerging surveillance measures have tested existing legal frameworks, emphasizing the importance of their critical evaluation at the international level. Recent studies have begun to explore the relationship between scientific production and data protection, contributing to a more holistic understanding of this phenomenon[4]. reflects on how artificial intelligence may influence informational self-determination, suggesting that education and awareness regarding data management are essential to empower citizens. Similarly,[5] examines the implementation of AI-based surveillance systems in developing countries, identifying both benefits and potential risks associated with their use in the absence of proper regulatory frameworks. In the same vein,[6] argues that the impact of information technologies demands in-depth analysis to promote the effective protection of fundamental rights in diverse contexts. More recent studies delve further into this global issue. For example,[7] underscore the legal conflicts regarding personal data transfers between the European Union and the United States, where the General Data Protection Regulation (GDPR) faces U.S. surveillance policies. From a more critical perspective, addresses the dilemma between privacy and public security through the lens of the "digital risk society," questioning the

[1] Alshamy, Y., Coyne, C. J., Hall, A. R., & Owens, M. A. (2024). Surveillance capitalism and the surveillance state: a comparative institutional analysis. *Constitutional Political Economy*, 1-23.
[2] Trujillo, W. A. A., Martinez, R. G. A., Macías, J. V. E., & Macías, P. F. E. (2025). Derechos Humanos frente a la vigilancia digital: Análisis crítico y propuestas. *SAPIENS International Multidisciplinary Journal*, *2*(1), 1-12.
[3] Lara, M. d. R. H. (2021). Estado de Derecho y emergencia sanitaria. *Enfoques Jurídicos*(04), 100-119.
[4] Gutiérrez, J. C. B. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revista de la Facultad de Derecho de México*, *74*(290), 125-148.
[5] Kshetri, N. (2020). Artificial Intelligence in Developing Countries. *IT Prof.*, *22*(4), 63-68.
[6] Jiménez, J. M. (2024). Seguridad y privacidad en el tiempo digital, la era de la información líquida. *Ciencia Latina: Revista Multidisciplinar*, *8*(2), 7399-7420.
[7] Lalova-Spinks, T., Valcke, P., Ioannidis, J. P., & Huys, I. (2024). EU-US data transfers: an enduring challenge for health research collaborations. *NPJ digital medicine*, *7*(1), 215.

proportionality of mass interceptions. In the labor context,[8] examines how algorithmic surveillance degrades workers' informational autonomy and advocates for stronger control over personal data. On the other hand,[9] introduce the concept of privacy literacy, emphasizing the role of university libraries in educating citizens about their digital rights. This educational approach is crucial in light of increasingly sophisticated surveillance systems, as noted by[10], who propose models of "forced trust" in smart environments where users lack control over their data. Similarly,[11] address surveillance capitalism from a comparative institutional perspective, highlighting the differing social impacts of data usage by private actors versus authoritarian states. Despite these advances, significant gaps remain in the current literature. For instance,[12] argues that although discussions on privacy and data are common, the intersection of these topics with digital surveillance practices has not been thoroughly explored. Likewise,[13] emphasizes that although studies exist on privacy in digital platforms, they often fail to address state and corporate surveillance in a comprehensive manner[14]. Complements this critique by noting that existing research tends to focus on case descriptions without providing sufficient analytical evaluation of the impact of mass surveillance on fundamental rights. From a criminological and penal law standpoint, digital surveillance reshapes core domains of criminal justice: policing strategies (including algorithmic/predictive policing), evidentiary reliability and chain of custody for digital traces, and the proportionality/necessity test governing investigative powers. It also raises due-process concerns (presumption of innocence, equality of arms) and risks of discriminatory or chilling effects. Consequently, the governance of personal data is not merely a privacy question but a criminal justice and fundamental-rights question, requiring legal safeguards, auditability, and independent oversight.

II. **Research Objective**

[8] Carter, C. (2025). AI surveillance: Reclaiming privacy through informational control. *European Labour Law Journal*, *16*(2), 245-258.

[9] Johann, A. L., & Muriel-Torrado, E. (2024). Competência em privacidade: abordagens e conteúdos em universidades e suas bibliotecas do mundo. *Revista Interamericana de Bibliotecologia*, *47*(3).

[10] Halla-Aho, L., Isoaho, J., & Virtanen, S. (2024). Defining and Modelling Forced Trust and Its Dependencies in Smart Environments. *IEEE Access*.

[11] Alshamy, Y., Coyne, C. J., Hall, A. R., & Owens, M. A. (2024). Surveillance capitalism and the surveillance state: a comparative institutional analysis. *Constitutional Political Economy*, 1-23.

[12] Barbudo, C. F. (2020). Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia. *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, *17*(1), 69-76.

[13] Amiradakis, M. J. (2016). Social networking services: A digital extension of the surveillance state? *South African Journal of Philosophy= Suid-Afrikaanse Tydskrif vir Wysbegeerte*, *35*(3), 2810-2292.

[14] DELGADO FRANCO, C. (2019). ENSAYO GANADOR DEL X PREMIO ENRIQUE RUANO CASANOVA: VIGILANCIA MASIVA Y EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES. *FORO: Revista de Ciencias Juridicas y Sociales Nueva Epoca*, *22*(1).

In response to these gaps, the objective of this article is to identify the scientific production published between 2014 and 2024 related to personal data protection in the context of digital surveillance.

III. **Methodology**

The bibliometric analysis carried out in this study is descriptive in nature and aimed to explore trends in scientific production indexed in Scopus between 2014 and 2024. Bibliometric methods were employed to present both qualitative and quantitative findings, providing a comprehensive overview of the evolution and characteristics of the scientific output during this period. The sample was derived from publications indexed in the Scopus database, which encompasses a wide range of academic disciplines. The search strategy employed the following Boolean query: ("data protection" OR "personal data" OR "data privacy") AND ("digital surveillance" OR "mass surveillance" OR "technological surveillance" OR "AI surveillance"), applied to the title, abstract, and keyword fields. Specific filters were then applied, including publication year (2014–2024) and document type, which allowed for the extraction of relevant metadata. Initially, 160 documents were identified. After applying filtering parameters, the selection was reduced to 151 documents. Subsequently, during the data cleaning process, 18 documents were excluded, resulting in a final sample of 133 documents for analysis. We excluded (a) editorials, notes, errata, book reviews, and non-peer-reviewed items; (b) records whose primary focus was not personal data protection within digital/mass/AI surveillance; (c) duplicates and retracted items; and (d) documents without sufficient bibliographic metadata. Two reviewers independently screened titles/abstracts, resolving disagreements by discussion. The query was applied in English to titles/abstracts/keywords; therefore, items lacking English metadata may be underrepresented. A keyword co-occurrence analysis was conducted to examine relationships between key terms and other relevant categories within the body of scientific production. Additionally, the bibliometric analysis was standardized using internationally recognized indicators, focusing on personal data protection in the digital surveillance era. These indicators included publication year, authors, institutions, countries, sources or journals, document types, subject areas, and keywords. For data processing and visualization, VOSviewer software (version 1.6.20) was used, complemented by Microsoft Excel for the construction of tables.

IV. **Results and discussion**

1. ***Articles Published Per Year in the Scopus Database***

Figure 1 shows the annual evolution of the number of documents indexed in the

Scopus database between 2014 and 2024 that address the topic of personal data protection in the context of digital surveillance. Overall, publication output fluctuated, with peaks of high publication activity interspersed with periods of decline.

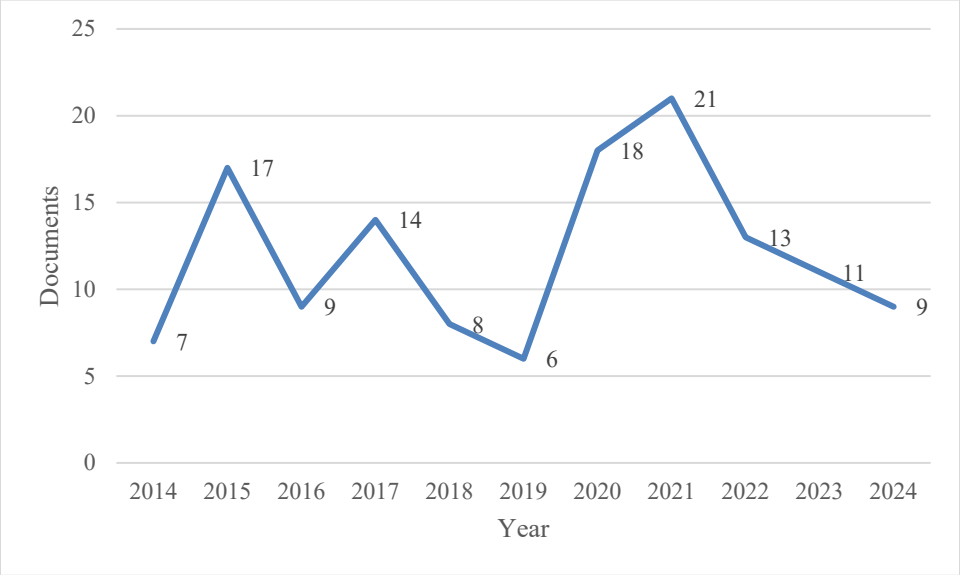

Figure 1: Articles Published Per Year in the Scopus Database

The year 2015 stands out as one of the first peaks, with 17 publications, reflecting a significant increase compared to 2014 (7 documents). This increase may be associated with the growing international debate on privacy following revelations of mass surveillance in previous years. Subsequently, a decline is observed in 2016 (9 documents) and a slight recovery in 2017 (14), followed by a steady decrease reaching its lowest point in 2019, with only 6 publications. From 2020 onwards, a notable rebound was recorded, reaching a historical peak in 2021 with 21 documents, possibly driven by the COVID-19 pandemic, which intensified the use of digital monitoring technologies and, consequently, raised new concerns about personal data privacy. However, after this peak, the trend progressively declined: 13 publications in 2022, 11 in 2023, and 9 in 2024, which could indicate stabilization or a shift in academic interest toward emerging topics such as generative artificial intelligence or algorithmic governance within the same field of study. The data suggest that academic interest in personal data protection in the digital surveillance era has been intermittent but reactive, influenced by key global events and changes in international regulation (such as the GDPR in Europe or debates on digital sovereignty). This implies that scientific production in this area is strongly conditioned by political, technological, and regulatory contexts.

2. *Most Productive Countries in the Field of Personal Data Protection in the Era of Digital Surveillance*

The results show a diverse geographical distribution in the scientific production related to personal data protection in the context of digital surveillance. A total of 43 countries contributed at least one publication during the analyzed period.

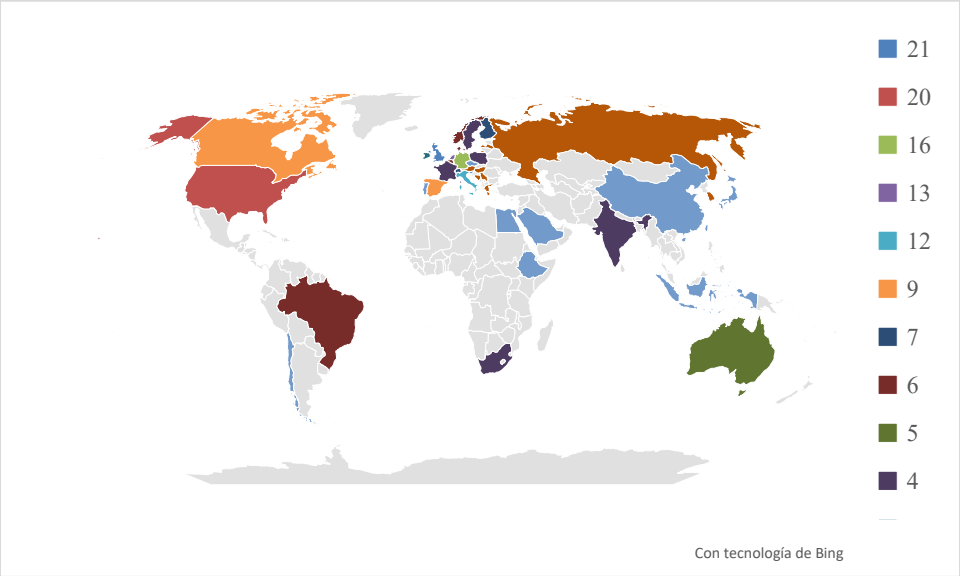

Figure 2: Most Productive Countries in the Field of Personal Data Protection in the Era of Digital Surveillance

The countries with the highest output are the United Kingdom (21 documents) and the United States (20 documents), reflecting the strong academic and institutional presence of both nations in topics related to privacy, technology regulation, and digital rights. This leadership may also be linked to the influence of pioneering regulations such as the UK Data Protection Act and U.S. debates on mass surveillance and data protection following the Snowden disclosures and the Cambridge Analytica scandal. Germany ranks third (16 documents), followed by the Netherlands (13) and Italy (12). These European countries have played key roles in the development and promotion of the General Data Protection Regulation (GDPR), which has significantly boosted academic output on data governance. An intermediate group of countries — including Canada and Spain (9 documents each), Finland and Switzerland (7), and Belgium, Brazil, Denmark, and Norway (6 each) — also demonstrates a growing commitment to the topic. In the case of Brazil and India, their participation is notable as it represents perspectives from the Global South, where regulatory development and digital surveillance have particular implications in contexts of weaker legal protections and greater digital inequality. In contrast, many countries registered only one or two publications during the period, such as Chile, China, Japan, Indonesia, Ethiopia, Egypt, Portugal, Saudi Arabia, and others. This limited representation may be associated with underdeveloped public policy frameworks on personal data, lower research funding, or limited indexing of their publications in international databases such as

Scopus. Overall, the data suggest that academic discourse on data protection in digital surveillance contexts is concentrated primarily in the Global North, particularly Western Europe and North America. This reveals the need to promote greater participation from regions such as Latin America, Africa, and Asia, especially given the profound implications of digital surveillance for human rights in settings where legislation is still emerging or underdeveloped. Concentration of outputs in the Global North has concrete effects: jurisdictions aligned with robust data-protection regimes (e.g., GDPR) tend to inform legislative reforms, proportionality/necessity standards, and evidentiary doctrines for digital traces. Under-resourced jurisdictions in the Global South face uneven incorporation of safeguards (lawful basis, oversight, effective remedies) and limited enforcement capacity, widening asymmetries in cross-border data flows, admissibility of digital evidence, and protection against discriminatory or chilling surveillance. Addressing this gap is therefore a normative priority for equal protection of fundamental rights across regions.

3. *Most Productive Journals on Personal Data Protection in the Era of Digital Surveillance*

Table 1 presents the scientific journals with the highest number of publications on personal data protection in the context of digital surveillance during the 2014–2024 period. In total, 13 journals with at least two published articles were identified, highlighting a multidisciplinary field where areas such as computer science, ethics, law, public policy, and digital media studies converge.

Table 1: Most Productive Journals on Personal Data Protection in the Era of Digital Surveillance

Journal	TD	SJR2024	Q	H	Country
Lecture Notes in Computer Science	10	0.352	Q2	499	Germany
Internet Policy Review	3	1.263	Q1	39	Germany
Communications In Computer and Information Science	2	0.182	Q4	75	Germany
Ethics And Information Technology	2	1.107	Q1	79	Netherlands
European Journal of Privacy Law and Technologies	2	0.133	Q4	4	Italy
IFIP Advances in Information and Communication Technology	2	0.210	Q3	70	Germany
Ibersid	2	0.174	Q3	6	Spain
Information Communication and Society	2	2.026	Q1	125	United Kingdom
Journal Of Digital Media and Policy	2	0.363	Q2	13	United Kingdom
Lecture Notes in Networks and Systems	2	0.166	Q4	48	Switzerland
Science And Engineering Ethics	2	0.961	Q1	83	Netherlands
Social Media and Society	2	2.169	Q1	82	United Kingdom
Surveillance and Society	2	0.579	Q1	59	United Kingdom

Note. TD: Total Documents. SJR2024: Scimago Journal Ranks 2024. Q: Quartile. H: H Index

The journal with the highest output is Lecture Notes in Computer Science (10 articles), a German-based editorial series widely used for disseminating research in computer science. Although its 2024 Scimago Journal Rank (SJR) is 0.352 (Q2), its high H-index (499) positions it as a leading technical source. This suggests that many studies on data protection are framed within technological and engineering approaches, focusing on algorithmic solutions, encryption, or secure system design. In second place is Internet Policy Review (3 articles, SJR 1.263, Q1), also based in Germany, which focuses on critical studies of digital policy, technology regulation, and online rights. Its high editorial quality (Q1) and regulatory analysis orientation make it a key outlet for research with legal and ethical perspectives. Other journals with two articles each include high-impact interdisciplinary publications such as Ethics and Information Technology (Netherlands, Q1, SJR 1.107), Science and Engineering Ethics (Netherlands, Q1), Social Media and Society (United Kingdom, Q1, SJR 2.169), and Information, Communication and Society (United Kingdom, Q1, SJR 2.026). These journals reflect a growing trend to approach the topic from ethical, philosophical, and sociological frameworks, linking digital surveillance challenges to the social and normative implications of data protection. Also identified were technically oriented journals such as IFIP Advances in Information and Communication Technology and Communications in Computer and Information Science, both with lower impact rankings (Q3 and Q4), yet maintaining a sustained presence. The journal Surveillance and Society, based in the United Kingdom, also stands out for its explicit focus on critical surveillance studies, reinforcing the academic interest in understanding the mechanisms and social effects of mass data collection. Geographically, Germany leads with four journals in the ranking, followed by the United Kingdom with three, and the Netherlands, Italy, Switzerland, and Spain with one each. This pattern reaffirms Europe's dominance in scientific production on this topic, consistent with its regulatory leadership in data protection (e.g., GDPR).

4. *Top Ten Most Productive Institutions on Personal Data Protection in the Era of Digital Surveillance*

Figure 3 shows the ten most productive academic and research institutions in publishing studies on personal data protection in digital surveillance contexts between 2014 and 2024. Institutional participation is diverse and geographically distributed, including European, American, and international research centers.

Leading the list with three publications each are: Aalto University (Finland), Sant'Anna School of Advanced Studies (Italy), ETH Zurich (Switzerland), Howard University (United States), Technical University of Denmark, University of Turku (Finland), and Delft University of Technology (Netherlands). These institutions

mostly belong to countries with strong data protection regulations and prominent academic traditions in areas such as ethical technology, privacy system design, surveillance, and legal engineering.

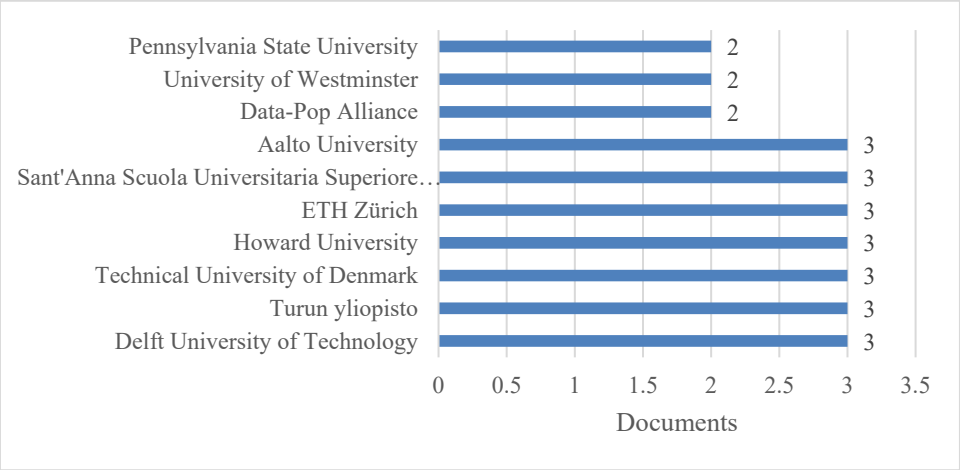

Figure 3: Top Ten Most Productive Institutions on Personal Data Protection in the Era of Digital Surveillance

Other institutions with two published documents also stand out: Pennsylvania State University (USA), University of Westminster (UK), and Data-Pop Alliance, an international organization promoting the ethical use of data for sustainable development. The latter reflects an openness to non-academic actors with significant influence on public policy and digital rights advocacy. This institutional leadership not only evidences a sustained commitment to research in this area but also points to the importance of multidisciplinary and transnational collaboration in addressing the challenges posed by digital surveillance. The presence of universities from Nordic countries (Finland, Denmark), as well as Italian and Swiss centers, confirms the leading role of continental Europe in developing conceptual and technological frameworks for privacy protection. This institutional panorama also suggests opportunities for inter-institutional academic collaboration and the potential to strengthen comparative research networks that bridge legal, ethical, and technical approaches to personal data protection.

5. ***Publications by Subject Area***

Figure 4 presents the distribution of documents by thematic classification in the Scopus database. The Social Sciences stand out prominently, with a total of 77 documents, followed closely by Engineering (72 documents). This dual dominance reflects the convergence of sociopolitical and technological approaches in analyzing privacy in digital environments. While Social Sciences explore ethical, legal, cultural, and political aspects of digital surveillance, Engineering contributes with the design of security systems, anonymization algorithms, and automated data

protection mechanisms.

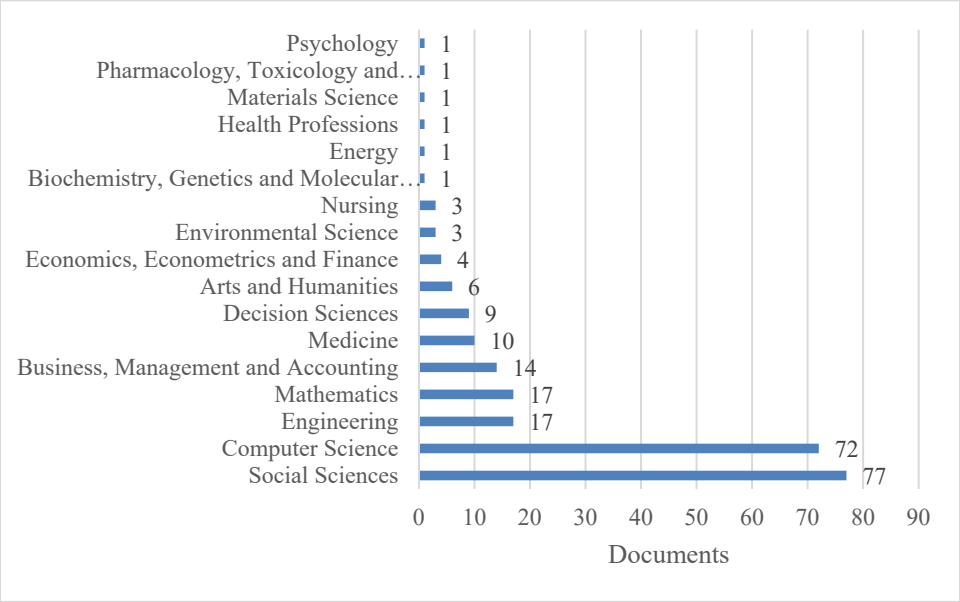

Figure 4: Publications by Subject Area

At a second level are fields such as Business, Management and Accounting (14 documents), indicating interest in the economic, organizational, and compliance implications of data protection in corporate practices, especially in response to regulations such as the GDPR or national laws. Other significant contributions come from Decision Sciences (9 documents), suggesting the application of decision-making models to privacy policy and data governance strategies, and Economics, Econometrics and Finance (6 documents), where research addresses the costs, risks, and economic benefits associated with protecting (or compromising) personal data. Minor but relevant contributions also appear from areas such as Nursing (3 documents), which likely address clinical data protection and health information ethics; as well as Energy, Materials Science, Psychology, and others, each with one document. These entries show more specific or marginal applications of the topic, reflecting its still limited reach in those fields. The results reinforce the interdisciplinary nature of personal data protection studies in the digital age, confirming that it is not solely a technical or legal phenomenon, but a complex issue that calls upon multiple fields of knowledge. This diversity of approaches enriches academic debate and fosters a deeper understanding of the many dimensions of contemporary digital surveillance.

6. *Top Ten Most Cited Articles on Personal Data Protection in the Era of Digital Surveillance*

Table 2 presents the ten most cited articles published between 2014 and 2024 addressing topics related to personal data protection in digital surveillance contexts. This analysis helps identify the most influential academic and thematic

contributions, as well as the dominant lines of research in the field.

Table 2(a): Top Ten Most Cited Articles on Personal Data Protection in the Era of Digital Surveillance

Authors	Title	Journal	Citations
Lupton, D [15]	The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance	Economy and Society	272
Saura, J. R et al.[16]	Assessing Behavioral Data Science Privacy Issues in Government Artificial Intelligence Deployment	Government Information Quarterly	131
Bradford, L et al.[17]	COVID-19 Contact Tracing Apps: A Stress Test for Privacy, The GDPR, And Data Protection Regimes	Journal of Law and the Biosciences	108
Dunn Cavelty, M[18]	Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities	Science and Engineering Ethics	94
Bellare, M et al.[19]	Mass-Surveillance Without the State: Strongly Undetectable Algorithm-Substitution Attacks	Proceedings of the ACM Conference on Computer and Communications Security	80
Prinsloo, P et al.[20]	Student Privacy Self-Management: Implications for Learning Analytics	ACM International Conference Proceeding Series	73
Newlands, G et al.[21]	Innovation Under Pressure: Implications For Data Privacy During the Covid-19 Pandemic	Big Data and Society	71
Radanliev, P et al.[22]	COVID-19 What Have We Learned? The Rise of Social Machines and Connected Devices in Pandemic Management	EPMA Journal	68

[15] Lupton, D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society*, *45*(1), 101-122.
[16] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.
[17] Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), lsaa034.
[18] Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.
[19] Bellare, M., Jaeger, J., & Kane, D. (2015). Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. Proceedings of the 22nd ACM SIGSAC conference on computer and communications security,
[20] Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. Proceedings of the fifth international conference on learning analytics and knowledge,
[21] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.
[22] Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Montalvo, R. M., Santos, O., Maddox, L. T., & Cannady, S. (2020). COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. *EPMA journal*, *11*(3), 311-332.

	Following the Concepts of Predictive, Preventive and Personalized Medicine		

Table 2(b): Top Ten Most Cited Articles on Personal Data Protection in the Era of Digital Surveillance

Authors	Title	Journal	Citations
Clarke, R [23]	Risks Inherent in the Digital Surveillance Economy: A Research Agenda	Journal of Information Technology	67
Bellanova, R [24]	Digital, Politics, and Algorithms: Governing Digital Data Through the Lens of Data Protection	European Journal of Social Theory	57

The article with the highest number of citations is "The diverse domains of quantified selves: self-tracking modes and dataveillance" by[25], published in Economy and Society, with 272 citations. This work conceptualizes the phenomenon of dataveillance (data surveillance) in the context of self-tracking and the culture of personal quantification, offering a sociological and critical perspective on new forms of exposure and control through data in everyday life. In second place, with 131 citations, is the study by Saura et al.[26], focused on privacy issues in the deployment of government artificial intelligence systems, published in Government Information Quarterly. This research reflects growing concerns over the use of big data and algorithms in the public sector, and highlights the need for institutional transparency and accountability. Also notable is the article by[27], with 108 citations, which analyzes COVID-19 contact tracing apps. Published in Journal of Law and the Biosciences, it is a key study on the challenges that legal frameworks such as the GDPR face in public health emergencies. Other important contributions address topics such as:

- Cybersecurity and systemic vulnerabilities ([28]; 94 citations),
- Undetectable algorithm-substitution attacks ([29]; 80 citations),
- Student privacy in learning analytics ([30]; 73 citations),

[23] Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of information technology*, *34*(1), 59-80.
[24] Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3), 329-347.
[25] Lupton, D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society*, *45*(1), 101-122.
[26] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.
[27] Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), lsaa034.
[28] Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.
[29] Bellare, M., Jaeger, J., & Kane, D. (2015). Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. Proceedings of the 22nd ACM SIGSAC conference on computer and communications security,

- Technological innovation and privacy during the pandemic ([31]; 71 citations),
- The digital surveillance economy ([32]; 67 citations),
- And critical approaches to data governance ([33]; 57 citations).

A common feature among these works is their interdisciplinary approach, combining legal, technological, ethical, political, and social perspectives. Furthermore, many of the most cited articles were published in high-impact journals covering contemporary issues such as artificial intelligence, state surveillance, and data capitalism. The results suggest that the most influential studies in this field not only propose innovative theoretical frameworks or critique control systems but also address urgent, real-world challenges for global citizens—explaining their high citation rates.

7. ***Keyword Co-Occurrence Map***

Figure 5 presents a keyword co-occurrence map generated using the VOSviewer tool, based on the most frequent terms found in the titles, abstracts, and keywords of documents indexed in Scopus. At the center of the map, prominent nodes include “privacy,” “data privacy” “data protection” and “surveillance” which represent the core concepts of the field. These terms are linked to several clusters that reflect the different thematic approaches to the issue

[30] Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. Proceedings of the fifth international conference on learning analytics and knowledge,

[31] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

[32] Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of information technology*, *34*(1), 59-80.

[33] Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3), 329-347.

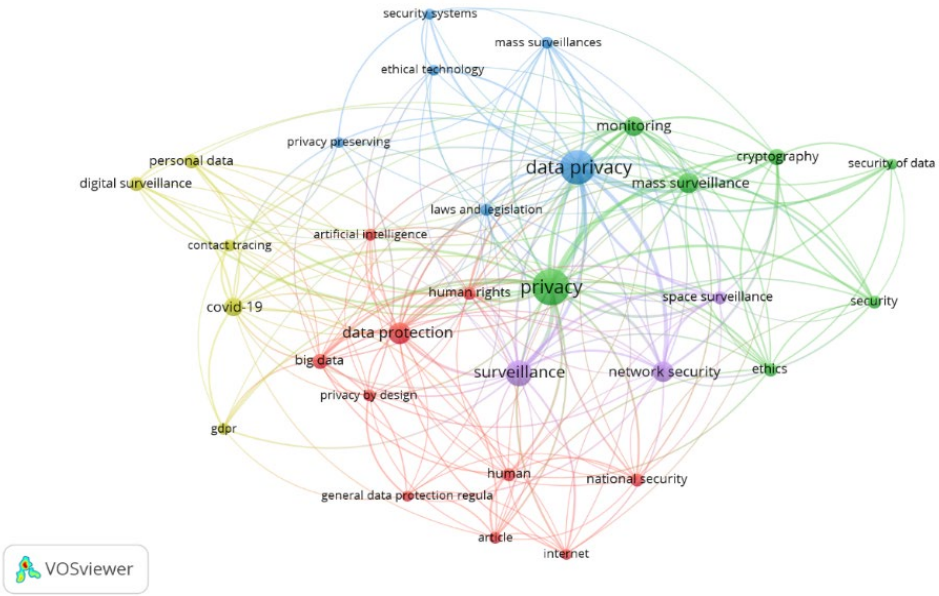

Figure 5: Keyword Co-Occurrence Map

Blue Cluster (technological focus): Includes terms such as “data privacy”, “security systems”, “ethical technology”, “monitoring”, “mass surveillance” and “laws and legislation”. This group indicates a focus on the intersection of data privacy, applied technology, and regulatory frameworks, where technical solutions with legal backing are discussed.

Green Cluster (security and cryptography): Groups terms such as “security”, “network security”, “security of data”, “cryptography”, “ethics” and “space surveillance”. The emphasis here is on technical strategies for information protection, particularly in contexts of mass surveillance and cybersecurity.

Red Cluster (regulation and rights): Includes terms such as “data protection” “gdpr”, “big data” “human rights”, “privacy by design”, “internet” and “general data protection regulation”. This cluster clearly connects to international regulation, digital rights, and the legal architecture of data protection, especially in the European context.

Yellow Cluster (pandemic and surveillance): Contains terms like “covid-19”, “contact tracing”. “personal data”, “digital surveillance” and “artificial intelligence” This group reflects recent thematic interest in the intensive use of surveillance technologies during the pandemic and their impact on individual privacy.

Purple Cluster (interdisciplinary connection): Includes terms such as “privacy”, “surveillance”, “national security”, “article” and "human”. These terms form a critical, interdisciplinary core linking digital surveillance to citizenship, human rights, and national security.

The map reveals a highly interconnected thematic structure, where various disciplines converge in the analysis of privacy and data protection in the digital age.

At least five semantic clusters are identified, reflecting concerns about technical security, legal and ethical frameworks, international regulation, responses to health crises, and interdisciplinary approaches.

Furthermore, the term "artificial intelligence" is notably linked to topics of surveillance and data protection, indicating an emerging trend in the analysis of algorithmic risks to privacy. This analysis confirms that the field is not only expanding but is also profoundly shaped by global events (e.g., the pandemic), technological innovations (e.g., AI, tracking systems), and the evolution of regulatory frameworks such as the GDPR. This bibliometric study identified the main characteristics of scientific production related to personal data protection in the context of digital surveillance between 2014 and 2024. The results show a pattern of intermittent but reactive publication, with peaks associated with global events such as the COVID-19 pandemic or the implementation of the General Data Protection Regulation (GDPR). Most of the research comes from Western Europe and North America, especially the United Kingdom, the United States, Germany, and the Netherlands, which also host the most productive institutions and journals. Thematically, the field reveals a highly interdisciplinary approach, combining legal, ethical, technological, and social perspectives. The keyword co-occurrence clusters confirm that core concepts such as privacy, surveillance, regulation, and artificial intelligence dominate academic discourse. These findings are consistent with authors such as [34], who argue that discussions around "surveillance capitalism" are largely driven by institutions in the Global North. Similarly,[35] reinforce the European leadership in privacy debates by analyzing legal conflicts in transatlantic data transfers. As noted by[36], the rise of algorithmic surveillance has shifted academic attention toward structural risks in areas such as labor, health, and education. The inclusion of highly cited articles like those by[37] and [38] further confirms that health emergencies accelerate the adoption of surveillance technologies and intensify academic debate on their impacts on fundamental rights. Several factors may explain the identified patterns. First, the strength of European regulations, particularly the GDPR, has stimulated increased academic interest in legal and policy aspects of data protection. Second, the rapid development of artificial intelligence, big data, and biometric surveillance systems has spurred

[34] Alshamy, Y., Coyne, C. J., Hall, A. R., & Owens, M. A. (2024). Surveillance capitalism and the surveillance state: a comparative institutional analysis. *Constitutional Political Economy*, 1-23.
[35] Lalova-Spinks, T., Valcke, P., Ioannidis, J. P., & Huys, I. (2024). EU-US data transfers: an enduring challenge for health research collaborations. *NPJ digital medicine*, *7*(1), 215.
[36] Carter, C. (2025). AI surveillance: Reclaiming privacy through informational control. *European Labour Law Journal*, *16*(2), 245-258.
[37] Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), lsaa034.
[38] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

research on ethical, technical, and institutional responses. Third, the reactive nature of the publications—such as the 2021 peak—suggests that scholarly output is influenced by global crises that temporarily increase demand for analytical frameworks. Finally, the limited participation from the Global South may be linked to structural barriers such as underfunding, poor indexing in international databases, and low visibility in dominant publication circuits.This study presents several limitations. First, it relies solely on the Scopus database, which may exclude relevant research indexed elsewhere (e.g., Web of Science, SciELO). Second, the search strategy focused on English-language terms, which may limit the inclusion of literature in other languages or with different terminology. Third, while the analysis examined quantitative indicators, it does not assess the theoretical or methodological quality of the articles reviewed—an important aspect for further exploration. Lastly, publications from 2024 may not yet have reached their full citation potential, which could affect trend interpretation. Theoretically, this study contributes to the consolidation of an interdisciplinary field of knowledge, showing the need to integrate legal, ethical, and technical frameworks for a comprehensive understanding of digital surveillance. It also encourages reconceptualizing privacy not only as an individual right but as a structural component of algorithmic governance, democratic accountability, and social justice. Practically, the findings can inform public policies, digital literacy strategies, and regulatory reforms, especially in underrepresented regions. The identification of leading journals, institutions, and countries provides reference points for strengthening academic networks and fostering international collaboration. The thematic analysis also helps researchers and policymakers focus on emerging areas with high societal relevance, such as AI regulation, workplace surveillance, and algorithmic transparency. Our findings highlight three priorities for criminal justice systems: (1) rigorous proportionality and legality tests prior to deploying algorithmic surveillance tools; (2) evidentiary reliability standards for digital traces (authenticity, integrity, audit trails) to protect due process; and (3) periodic, independent oversight to detect disparate impacts, false positives, and surveillance creep. Embedding these safeguards in statutory frameworks and courtroom practice can mitigate rights-infringing uses while enabling legitimate, accountable investigations. Based on the identified gaps, several future research directions are proposed. First, comparative studies between the Global North and South are needed to examine how institutional, legal, and social differences affect data protection. Second, qualitative and empirical studies should be developed to capture the lived experiences of citizens under surveillance, particularly in vulnerable contexts. Third, it is important to evaluate the effectiveness of digital privacy literacy programs, such as those discussed by [39], in strengthening critical

[39] Johann, A. L., & Muriel-Torrado, E. (2024). Competência em privacidade: abordagens e conteúdos em

capacity among users. Finally, continued research should explore the relationship between emerging technologies (AI, facial recognition, blockchain) and fundamental rights, and critically assess new regulatory frameworks like the European Union's AI Act.

V. **Conclusions**

The results of this bibliometric study show that scientific production on personal data protection in the context of digital surveillance during the 2014–2024 period followed a dynamic trajectory, with significant increases linked to global events such as the COVID-19 pandemic and the implementation of the General Data Protection Regulation (GDPR) in Europe. Publications are predominantly concentrated in Global North countries, particularly the United Kingdom, the United States, and Germany and approached the phenomenon from a distinctly interdisciplinary perspective that integrates legal, ethical, technological, and social approaches. The most productive journals belong to the field of computer science, but prominent sources are also found in social studies, communication, law, and artificial intelligence. The most frequent keywords confirm the centrality of concepts such as privacy, data protection, surveillance, AI, and GDPR, capturing the most relevant contemporary debates on digital surveillance. As a final reflection, this study provides an empirical foundation for understanding the current configuration of the field and offers important theoretical and practical implications. It reaffirms the need to enhance the academic participation of underrepresented regions, promote privacy education, and develop regulatory frameworks adapted to the new scenarios of algorithmic surveillance. From a criminological perspective, the evidence underscores the urgency of embedding proportionality and necessity tests in surveillance law, consolidating digital chain-of-custody and authenticity standards for electronic evidence, and instituting independent audits to prevent discriminatory harms and safeguard due process. Future research should include comparative geopolitical analyses, evaluation of public policies, and investigation into the impact of emerging technologies, such as artificial intelligence, facial recognition, and federated learning, on fundamental rights. Although this article offers a panoramic overview of the field, complementary qualitative and critical studies are necessary to deepen the understanding of the legal, ethical, and social implications of growing surveillance practices in digital environments, particularly their concrete consequences for criminal investigations, prosecutorial decision-making, and judicial review.

VI. **Authors' Contribution**

universidades e suas bibliotecas do mundo. *Revista Interamericana de Bibliotecologia*, *47*(3).

All authors contributed equally to the conception and design of the study. All authors read and approved the published version of the manuscript.

References

Alshamy, Y., Coyne, C. J., Hall, A. R., & Owens, M. A. (2024). Surveillance capitalism and the surveillance state: a comparative institutional analysis. *Constitutional Political Economy*, 1-23.

Amiradakis, M. J. (2016). Social networking services: A digital extension of the surveillance state? *South African Journal of Philosophy= Suid-Afrikaanse Tydskrif vir Wysbegeerte*, *35*(3), 2810-2292.

Barbudo, C. F. (2020). Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia. *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, *17*(1), 69-76.

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3), 329-347.

Bellare, M., Jaeger, J., & Kane, D. (2015). Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. Proceedings of the 22nd ACM SIGSAC conference on computer and communications security,

Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), lsaa034.

Carter, C. (2025). AI surveillance: Reclaiming privacy through informational control. *European Labour Law Journal*, *16*(2), 245-258.

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of information technology*, *34*(1), 59-80.

DELGADO FRANCO, C. (2019). ENSAYO GANADOR DEL X PREMIO ENRIQUE RUANO CASANOVA: VIGILANCIA MASIVA Y EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES. *FORO: Revista de Ciencias Juridicas y Sociales Nueva Epoca*, *22*(1).

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.

Gutiérrez, J. C. B. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revista de la Facultad de Derecho de México*, *74*(290), 125-148.

Halla-Aho, L., Isoaho, J., & Virtanen, S. (2024). Defining and Modelling Forced Trust and Its Dependencies in Smart Environments. *IEEE Access*.

Jiménez, J. M. (2024). Seguridad y privacidad en el tiempo digital, la era de la información líquida. *Ciencia Latina: Revista Multidisciplinar*, *8*(2), 7399-7420.

Johann, A. L., & Muriel-Torrado, E. (2024). Competência em privacidade: abordagens e conteúdos em universidades e suas bibliotecas do mundo. *Revista Interamericana de Bibliotecologia*, *47*(3).

Kshetri, N. (2020). Artificial Intelligence in Developing Countries. *IT Prof.*, *22*(4), 63-68.

Lalova-Spinks, T., Valcke, P., Ioannidis, J. P., & Huys, I. (2024). EU-US data transfers: an enduring challenge for health research collaborations. *NPJ digital medicine*, *7*(1), 215.

Lara, M. d. R. H. (2021). Estado de Derecho y emergencia sanitaria. *Enfoques Jurídicos*(04), 100-119.

Lupton, D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society*, *45*(1), 101-122.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. Proceedings of the fifth international conference on learning analytics and

knowledge,

Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Montalvo, R. M., Santos, O., Maddox, L. T., & Cannady, S. (2020). COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. *EPMA journal*, *11*(3), 311-332.

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.

Trujillo, W. A. A., Martinez, R. G. A., Macías, J. V. E., & Macías, P. F. E. (2025). Derechos Humanos frente a la vigilancia digital: Análisis crítico y propuestas. *SAPIENS International Multidisciplinary Journal*, *2*(1), 1-12.