Data and Metadata. 2025; 4:1135
doi: 10.56294/dm20251135

ORIGINAL

Impact of data protection legislation on the digitalization of small and medium-sized enterprises

Impacto de la legislación sobre protección de datos en la digitalización de las pequeñas y medianas empresas

Carina Del Rocío Cevallos Ramos[1], Gabriela Natali Fonseca Romero[1], Katherine Elizabeth Sandoval Escobar[1], Myriam Johanna Naranjo Vaca[1]

[1]Escuela Superior Politécnica de Chimborazo (ESPOCH), Riobamba - Ecuador.

Cite as: Cevallos Ramos CDR, Fonseca Romero GN, Sandoval Escobar KE, Naranjo Vaca MJ. Impact of data protection legislation on the digitalization of small and medium-sized enterprise. Data and Metadata. 2025; 4:1135. https://doi.org/10.56294/dm20251135

Submitted: 07-11-2024 **Revised:** 29-03-2025 **Accepted:** 23-08-2025 **Published:** 24-08-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding author: Carina Del Rocío Cevallos Ramos

ABSTRACT

Introduction: decision-making in small and medium-sized enterprises (SMEs) relies heavily on the proper management of data.
Objective: the objective of this research was to describe the scientific output on data protection legislation in the digitization of small and medium-sized enterprises, which is required by these enterprises for decision-making.
Method: to this end, the Scimago portal was used as a source for analyzing scientific output, and a review of the distribution by quartiles was carried out based on bibliometric indicators such as the H index, the impact factor of journals, the number of documents published, the average number of citations per document, international scientific collaboration, and citations from public funding agencies. Likewise, the number of articles cited in the most relevant journals in each quartile was analyzed in order to assess the relevance of scientific innovation in the formulation of adequate data protection legislation in the process of digitizing SMEs.
Results: the findings reveal that most scientific output is concentrated in journals belonging to countries with a high level of technological development. The areas with the highest representation are threat detection and data protection.
Conclusions: a low level of dissemination of research related to the development of specific legislative frameworks for data protection in the context of the digitization of small and medium-sized enterprises was identified.

Keywords: Threats; Cybersecurity; Data; Companies; Legislation.

RESUMEN

Introducción: la toma de decisiones en las pequeñas y medianas empresas (pymes) se basa en gran medida en el manejo adecuado de los datos.
Objetivo: el objetivo de esta investigación fue describir la producción científica sobre la legislación de protección de datos en la digitalización de pequeñas y medianas empresas información que es requerida por estas para la toma de decisiones.
Método: para ello, se utilizó el portal Scimago como fuente de análisis de producción científica, y se llevó a cabo una revisión de la distribución por cuartiles con base en indicadores bibliométricos tales como el índice H, el factor de impacto de las revistas, el número de documentos publicados, el promedio de citas por documento, la colaboración científica internacional y las citas de organismos financiadores públicos.

Asimismo, se analizó el número de artículos citados en las revistas más relevantes de cada cuartil con el fin de evaluar la relevancia de la innovación científica en la formulación de una legislación adecuada sobre protección de datos en el proceso de digitalización de las pymes.

Resultados: los hallazgos revelan que la mayor parte de la producción científica se concentra en revistas pertenecientes a países con un alto nivel de desarrollo tecnológico. Las áreas con mayor representatividad corresponden a la detección de amenazas y la protección de datos

Conclusiones: se identificó una baja difusión de investigaciones relacionadas con el desarrollo de marcos legislativos específicos para la protección de datos en el contexto de la digitalización de las pequeñas y medianas empresas.

Palabras clave: Amenazas; Ciberseguridad; Datos; Empresas; Legislación.

INTRODUCTION

The development of the internet and artificial intelligence is key to the growth of small and medium-sized industry, which relies on the use of data to optimize production processes, where data management is essential for decision-making in companies both in the present and for the development of future decisions, given that data can be integrated with mathematical simulation models and artificial intelligence algorithms.(1,2)

Although data management allows for scenario prediction and model building, it is a risky activity if the data is not adequately protected. There is an inherent risk in the use of data, which is subject to attacks that not only compromise the security of companies, but also the data of users and customers, whose misuse can lead to financial fraud. Therefore, legal measures and techniques are required to prevent such incidents from occurring.(3,4)

The first step in protection is the development of cybersecurity protocols, which, although costly, are becoming increasingly robust. However, these actions are not sufficient to protect the information of companies and users. Legal action is required to protect those affected and severely punish this type of crime. Despite being aware that such crimes are increasing every day, legal reforms have not been fast enough to prevent them.(5,6)

Scientific publication is one of the most valued activities in the academic world, given its importance in disseminating knowledge to the global scientific community and as a mechanism for evaluating university professionals and research institutions to leverage technological development. which is why they are increasingly required to publish in higher quality and more prestigious journals, allowing them to be evaluated according to the impact of the journals and through the use of bibliometric indicators based on the number of citations, as highlighted in this case, which allow the impact of data protection legislation on the digitization of small and medium-sized enterprises to be quantified.(7,8)

Legislation on cybersecurity is recent, so it is necessary to evaluate its impact through a bibliometric analysis reporting the main findings on this topic. In this regard, bibliometric analysis allows, through the use of computer programs, the visualization of scientific production and the determination of progress in data protection legislation in the digitization of small and medium-sized enterprises.(9,10)

Considering the above, the objective of this research was to describe the scientific output on data protection legislation in the digitization of small and medium-sized enterprises, information that is required by small and medium-sized enterprises for decision-making, to increase their productivity and competitiveness.

METHOD

The methodology developed was an observational, descriptive, bibliometric study of scientific output on data protection legislation in the digitization of small and medium-sized enterprises in the protection of data in the digitization of small and medium-sized enterprises. The combination of both types allows for the analysis, measurement, and identification of bibliographic data and relevant aspects of scientific publications on a given topic. The methodology is based on several steps, such as searching for bibliographic references in databases and filtering by keywords and period.

Inclusion criteria

Journals contained in Scimago that took into account the terminology in the search for information were considered, using words such as threats, risks, legislation, and cybersecurity, limiting the search to expected results in English-language articles related to scientific production on the impact of data protection legislation on the digitization of small and medium-sized enterprises, which was analyzed in digital journals in databases exclusively for Scopus, whose content covers the years 2019-2024 of active journals.

Exclusion criteria

Publications that deviated from the content of this study or were not indexed in Scopus were not considered.

Publications that lacked a scientific basis and reference databases derived from products that did not correspond to publications during the search period or that were not active in Scopus at the time of analysis were excluded.

Bibliometric analysis

The quantitative analysis of the information was carried out using a bibliometric approach to scientific production on the impact of data protection legislation on the digitization of small and medium-sized enterprises. Likewise, examples of some research papers published in the aforementioned area of study were analyzed from a qualitative perspective, using a bibliographic approach to describe the position of different authors on the proposed topic. The search was carried out using the Scimago database to determine scientific productivity in terms of the number of articles cited in the last year through keyword analysis.

Information search

For the purposes of this research, documentary exploration relating to scientific output on the impact of data protection legislation on the digitization of small and medium-sized enterprises was carried out by identifying similar works with relevant objectives and other aspects, using the following keywords in each journal: threats, risks, data, cybersecurity, and legislation.

The Scopus database was used to obtain bibliographic data, as it is one of the world's leading academic information databases. This analysis is carried out in two stages. In the first stage, a general search is conducted, and in the second stage, a search by country is carried out. First, a search string was established in the "Article title," "abstract," and "keywords" fields with the following terms in English and enclosed in quotation marks: threats, risks, data, cybersecurity, and legislation.

Techniques used to select journals for bibliometric analysis

The bibliographic search and journal location were carried out by analyzing the main bibliometric indicators obtained from Scimago, which characterizes journals using indicators such as the H index, journal impact factor, number of documents, citations per document, international scientific collaboration, and citations by public planners through the reuse of Scopus metadata, which are described below:

H index: the H index expresses the number of articles in the journal (H) that have received at least H citations. It quantifies both the scientific output and the scientific impact of the journal; it also applies to scientists and countries.

Journal impact factor: represents the average of weighted citations received in the selected year for documents published in the chosen journal during the previous three years.

Number of documents: number of documents published by a journal in the selected year. All types of documents are considered, both citable and non-citable.

Citations per document: number of citable documents published by a journal in the three years prior to the selected year (documents from the selected year are excluded). Only articles, reviews, and conference papers are considered.

International scientific collaboration: list of documents whose affiliation includes more than one country address.

Citations from public bodies: number of documents cited by public policy documents according to the Overton database.

Subsequently, a comparison and bibliometric analysis of the importance of the main journals in the field of economics was carried out to determine the importance of each journal in scientific production on threats, risks, legislation, data, and cybersecurity.

Analysis of the information

Once the clusters were identified at random, six journals were selected for each quartile, which are presented in table 1, and were subsequently analyzed based on the bibliometric indicators derived from Scimago. The bibliometric indicators were analyzed using analysis of variance (ANOVA) to determine whether there were differences between the previously visualized quartiles, and in those where there were significant differences with a probability of 5 %, Tukey's mean tests were performed using the InfoStat statistical package. Multivariate statistical techniques were also applied using principal component analysis (PCA) to compare the results with the quartiles observed in Scimago.

RESULTS

When analyzing scientific output on the impact of data protection legislation on the digitization of small and medium-sized enterprises, in terms of computer science journals indexed in Scopus, the results shown in figure 1 indicate that most correspond to Europe and North America with 929 and 576 journals, while the lowest output was observed in Latin America with 28 journals and Africa with less than 10 publications.

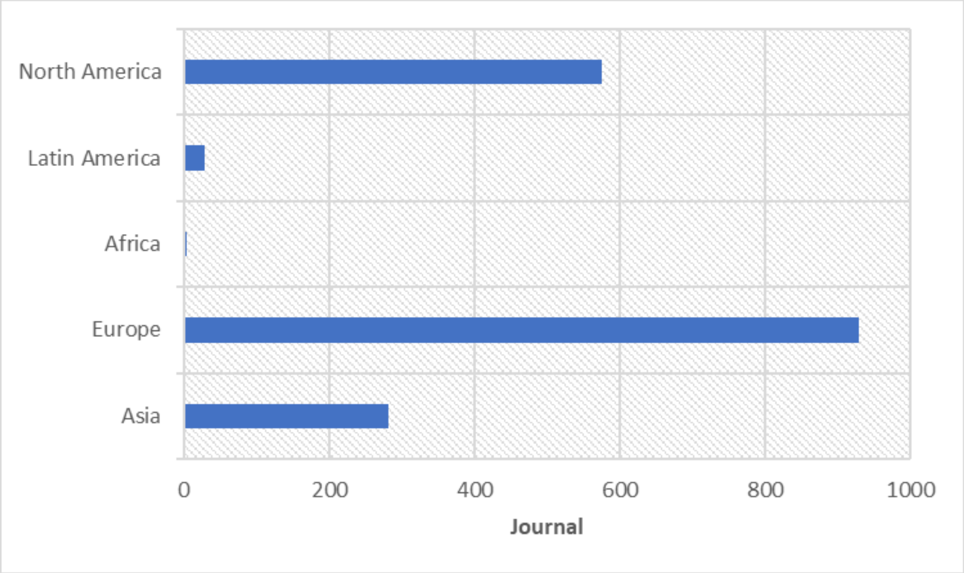

Figure 1. Scientific output on strengthening cyber resilience in universities through artificial intelligence for proactive threat detection

Once the scientific output had been identified at random, six journals were selected for each cluster, which allowed the scientific output to be analyzed by region. Figure 2 shows that most of the Q1 journals (highest H-index) are concentrated in the US and China, which correspond to the most important journals in the field of computer science, while those with the lowest scientific relevance (lowest H index) are located in African countries such as Egypt, South Africa, Tunisia, Morocco, and Algeria, and in Latin America, such as Brazil, Mexico, Chile, Colombia, and Argentina, as described in figure 2.

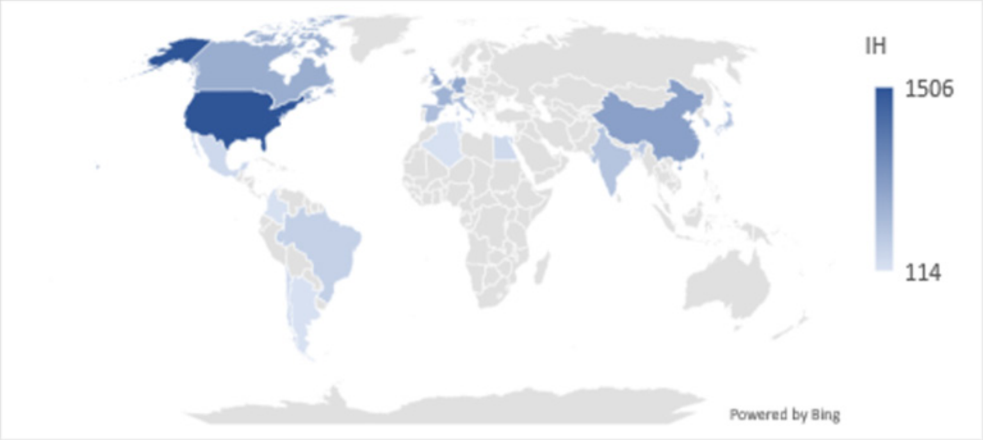

Figure 2. Distribution of scientific publications by region and country according to the H index

The results presented highlight, as other studies have documented, the importance of computer science in high-level scientific production, which reveals the importance of emphasizing that the information obtained from the Scimago portal for H index, journal impact factor, number of documents, citations per document, international scientific collaboration, and citations from public planners, whose results are presented in table 2, The journals ranked in quartile 1, published in countries with high technological levels, are those with the best performance (table 1).

Table 1. Comparisons of average bibliometric indicators generated by Scimago

Quartile	SJR	IH	DT	CPD	CI	OV
1	201,25	150,17	258,00	22,02	43,39	2
2	0,69	50,33	75,17	3,42	34,91	0
3	0,42	28,00	48,67	2,09	20,21	0
4	0,19	13,33	34	1,44	26,60	0,17

H index, journal impact factor (SJR), number of documents (DT), citations per document (CPD), international scientific collaboration (CI), and citations by public planners (OV).

The results in table 1 confirm the relevance of the scientific publications that were classified as Q1 by Scimago and are from the United States and the European Union, which coincides with other authors' findings that high-level scientific production is generated more frequently in countries with higher levels of technology. The reason for this productivity is due to greater human talent with level V education, high investment in science and technology, and more advanced technological infrastructure compared to countries in Latin America and Africa.

Once the most important journals in the field of information technology had been selected, in order to determine the relevance of the scientific output Impact of data protection legislation on the digitization of small and medium-sized enterprises, in order to ascertain progress in the field, a search was conducted of the scientific output in each journal, highlighting that journals in quartile 1 have the highest number of publications on topics such as threats, data, risks, cybersecurity, and legislation for digital security in small and medium-sized enterprises, a summary of which is presented in table 2.

Table 2. Average comparisons for publications analyzed

Quartile	PD	LD	DA	PDE	LDE	DAE
1	439,33	807	1 223,33	330,17	47,17	441,33
2	3 897,33	449,50	7 352,17	1 040,67	220,67	1 606,83
3	1 117,33	678,83	1 116,17	827,83	300,67	185,67
4	31,17	10,17	71	14,50	4,17	26

Protection of (PD); digital legislation (LD); threat detection (DA); data protection for companies (PD); digital legislation for companies (LDE), threat identification for companies (DAE).

In general, the results show that there is greater scientific output in articles related to data protection and threat detection than in those related to data protection legislation in the digitization of small and medium-sized enterprises, which shows that the trend in science is toward the production of scientific innovations, in line with advances in artificial intelligence and cybersecurity, which must be accompanied by adequate management of data protection and user integrity.

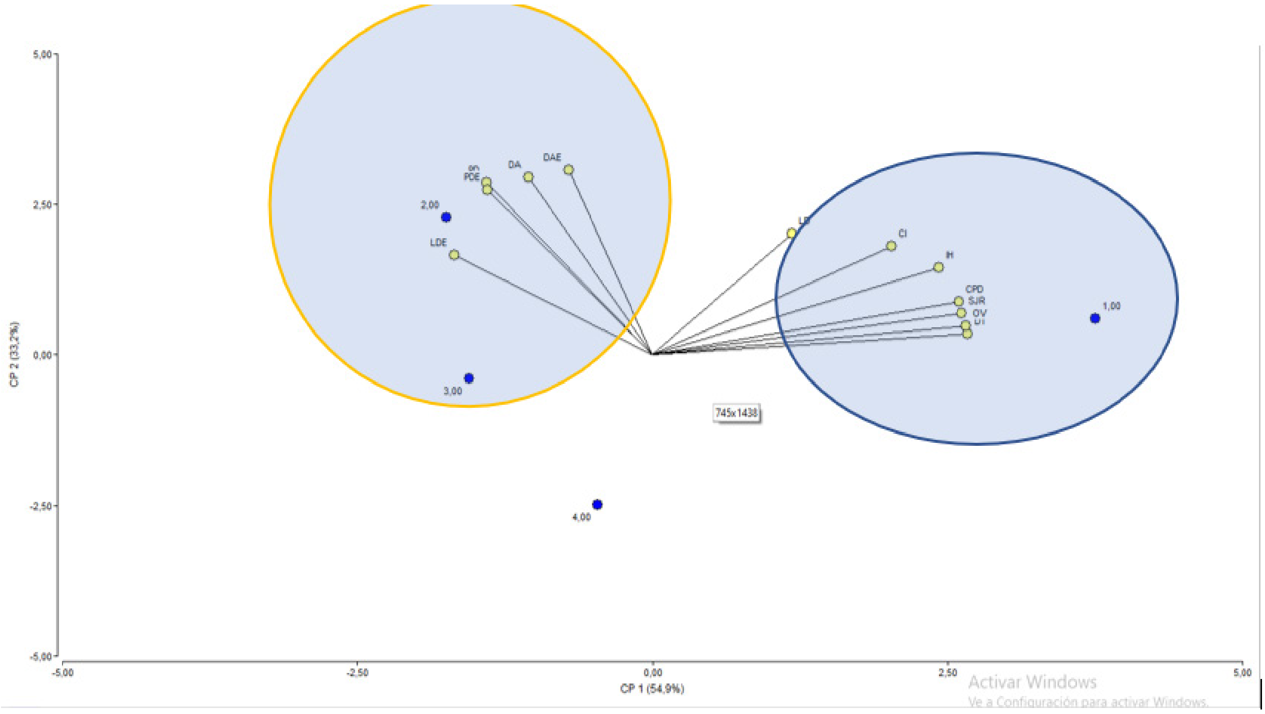

Figure 3. Distribution of scientific publications using principal component analysis

Table 2 shows the number of publications referring to the search terms used, both in general and in the field of cybersecurity in companies, threats, risks, and legislation, where the mean comparison tests show that the journals grouped in quartiles 1 and 2 have the highest number of publications compared to quartiles 3 and 4.

The trend observed by the analysis of the quartiles generated by the Scimago portal was confirmed by the principal component analysis (PCA), shown in figure 3, where along principal component 1, which explains 54,90 % of the variation in the data, two groups are clearly observed: group 1, located in the left quadrant, corresponding to the journals with the highest impact (Q1) and with international collaboration, and group 2 (located in the left quadrant), which grouped the journals with the highest number of publications addressing the topics of legislation, data, threats, risks, and cybersecurity, both in the field of small and medium-sized enterprises.

The results of the PCA are confirmed by the comparison of means of bibliometric indicators generated by Scimago, firstly, by those presented in table 2, referring to the quality of the journals, where it can be seen that the journals in quartile 1 have on average a higher citation index (H), total documents cited (DT), citations per document (CPD), and citations from public organizations (OV) compared to these same indicators for quartiles 2, 3, and 4.

From a graphical point of view, figure 4 shows that, based on search terms such as data, legislation, threat detection, and cybersecurity, most are concentrated in journals in quartiles Q1 and Q2, with a tendency towards fewer publications in the university context, especially when addressing the issue of data protection legislation in the digitization of small and medium-sized enterprises.

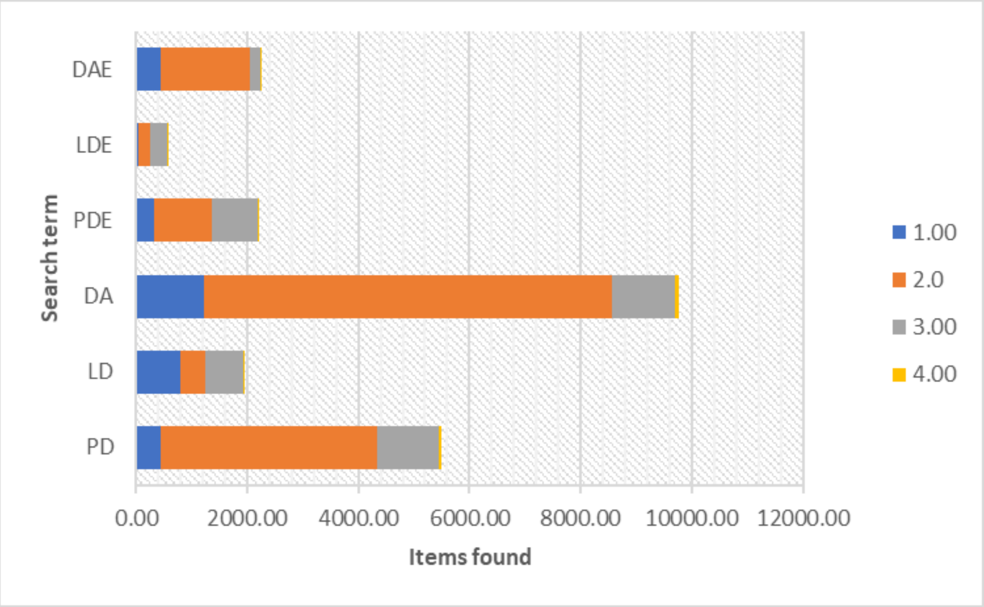

Figure 4. Comparison of scientific output by search terms. Legend: Protection of (PD); digital legislation (LD); threat detection (DA); data protection for companies (PD); digital legislation for companies (LDE), threat identification for companies (DAE)

DISCUSSION

Globalization has made competition between companies increasingly difficult by allowing more developed companies to enter the country, forcing local companies to develop digital tools that allow them to invest adequately in technological innovations to ensure their continued presence in the market by seeking new customers. This requires a large amount of data management, which, although it facilitates decision-making, is subject to cybersecurity risks, as reported in previous research.(11,12)

Despite cybersecurity requirements, the results of the bibliometric analysis demonstrate the low capacity for action in the context of cybersecurity, especially in Latin American countries, Southeast Asia, and Africa, where technological limitations prevent the development of strategies such as cyber resilience. This makes these countries more vulnerable to attacks by hackers and, more seriously, hinders their ability to respond to the consequences of such actions, which puts the operations of small and medium-sized enterprises at risk, as confirmed by the results of similar research.(13,14)

The importance of this type of research is that the preservation of the world's documentary heritage must be guaranteed, which should not be limited to creating and storing digital information, but should also strengthen the work of information professionals so that they can play a key role in global development. In this vein, work has already been done at the international level to create the legal and technological standards necessary for the proper management of digital archives and data protection, particularly in technologically advanced countries.(15,16)

The need to develop protocols and tools for the protection of digital information arises because, as new technologies spread throughout organizations, along with the growing influence of digital transformation and cloud technologies, security challenges also began to appear with new and ever-increasing threats and attacks, which also requires the development of robust legislation. Unfortunately, bibliometric analysis shows that little progress has been made, as reported by , which highlights that most research in this area has been carried out in developed countries, as shown in previous publications in this context.(17,18)

With the advancement of technology, new tools have emerged for data protection and digital evidence preservation, such as data encryption, the use of automated algorithms, artificial intelligence applications, machine learning, and other computerized tools, whose fundamental objective is to protect information, ensure its confidentiality and integrity, and prevent the violation of the databases where it is stored.(19,20)

The results of the bibliometric analysis show significant advances in the development of technologies for threat detection and in the implementation of cybersecurity protocols aimed at data protection, especially in countries with a high level of technological development, as demonstrated by the number of scientific publications in this context in high-impact journals, as evidenced in the reports analyzed using Scimago indicators based on Scopus metadata. However, progress in legislation has not kept pace with developments. The lack of regulatory updates in the face of rapid technological change leaves companies and users increasingly vulnerable to cybercrime, which could have serious financial and operational consequences.(21,22)

CONCLUSION

In conclusion, the results show that legislative development around data preservation is still in its infancy, as demonstrated by the reports analyzed using Scimago indicators based on Scopus metadata, which focus on threat detection rather than legislation for data protection in the business environment. Although significant progress has been made in the creation of technical cybersecurity protocols, specific regulations to support and regulate these processes have not evolved as quickly or as thoroughly. This lack of robust legislation represents a structural weakness, especially in the face of the increase and sophistication of cyberattacks that threaten data integrity in business and academic contexts.

In this regard, strengthening lines of research aimed at analyzing the impact of cyberattacks and the need for updated legal frameworks is a significant contribution to closing this gap. Likewise, it has been identified that most scientific production in this area comes from countries with a high level of technological development, where there is greater institutional and social awareness of the risks of electronic fraud. This reinforces the urgency for developing countries to prioritize investment in research, specialized training, and legislation on cybersecurity in order to ensure effective protection of information in the digital transformation process.

BIBLIOGRAPHICAL REFERENCES

1. Tambare P, Meshram C, Lee CC, Ramteke RJ, Imoize AL. Performance measurement system and quality management in data-driven Industry 4.0: A review. Sensors. 2021;22(1):224.

2. Gokalp MO, Kayabay K, Akyol MA, Eren PE, Koçyiğit A. Big data for industry 4.0: A conceptual framework. En: 2016 International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, NV, USA: IEEE; 2016. p. 431-4. Disponible en: https://ieeexplore.ieee.org/abstract/document/7881381/

3. Lezzi M, Lazoi M, Corallo A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Comput Ind. 2018;103:97-110.

4. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: A survey. Comput Secur. 2020;89:101677.

5. Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. J Netw Comput Appl. 2023;209:103540.

6. Hossain MA, Raza MA, Rahman JY. Human factors and employee resistance to adopting new cybersecurity protocols and technologies. 2024. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5207157

7. Sulich A, Zema T, Kulhanek L. Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development. Procedia Comput Sci. 2023;225:1448-57.

8. Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. Int J Crit Infrastruct Prot.

2022;39:100571.

9. Cappelletti F, Papakonstantinou V. A question of strategic legislation: Can the EU deal with cybersecurity issues in space? Telecommun Policy. 2025;102954.

10. Mishra A, Alzoubi YI, Anwar MJ, Gill AQ. Attributes impacting cybersecurity policy development: An evidence from seven nations. Comput Secur. 2022;120:102820.

11. Javaid M, Haleem A, Singh RP, Suman R, Gonzalez ES. Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. Sustain Oper Comput. 2022;3:203-17.

12. Laskurain-Iturbe I, Arana-Landín G, Landeta-Manzano B, Uriarte-Gallastegi N. Exploring the influence of industry 4.0 technologies on the circular economy. J Clean Prod. 2021;321:128944.

13. Mullet V, Sondi P, Ramat E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access. 2021;9:23235-63.

14. Kayan H, Nunes M, Rana O, Burnap P, Perera C. Cybersecurity of Industrial Cyber-Physical Systems: A Review. ACM Comput Surv. 2022;54(11s):1-35.

15. Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Comput Biol Med. 2021;129:104130.

16. Yanamala AKY, Suryadevara S. Advances in data protection and artificial intelligence: Trends and challenges. Int J Adv Eng Technol Innov. 2023;1(01):294-319.

17. Andraško J, Mesarčík M, Hamuľák O. The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. AI Soc. 2021;36(2):623-36.

18. Makulilo A, Mwamlangala D, Ezekiel R, Buchner B, März E, Freye M. Data privacy and security in E-health: African and European perspectives: The example of post data protection legislation in Tanzania. Int Cybersecurity Law Rev. 2025;6(2):195-206.

19. Jia B, Zhang X, Liu J, Zhang Y, Huang K, Liang Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Trans Ind Inform. 2021;18(6):4049-58.

20. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med Ethics. 2021;22(1):122.

21. Vukovic J, Ivankovic D, Habl C, Dimnjakovic J. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Arch Public Health. 2022;80(1):115.

22. Niazi ZK, Rehman TU, Saraf D. Digital dilemmas: Free speech, privacy, and state control in Pakistan’s social media landscape. Wah Acad J Soc Sci. 2025;4(1):1286-300.

FUNDING

The authors received no funding for this research.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Carina Del Rocío Cevallos Ramos, Gabriela Natali Fonseca Romero, Katherine Elizabeth Sandoval Escobar, Myriam Johanna Naranjo Vaca.

Writing - original draft: Carina Del Rocío Cevallos Ramos, Gabriela Natali Fonseca Romero, Katherine Elizabeth Sandoval Escobar, Myriam Johanna Naranjo Vaca.

Writing - review and editing: Carina Del Rocío Cevallos Ramos, Gabriela Natali Fonseca Romero, Katherine Elizabeth Sandoval Escobar, Myriam Johanna Naranjo Vaca.