The Easta Journal Law and Human Rights
Vol. 2, No. 03, June 2024, pp. 165 - 175
ISSN: 2985-7112, DOI: 10.58812/eslhr.v2i03

A Bibliometric Analysis of Legal Approaches to Personal Data Protection

Loso Judijanto[1], Nuryati Solapari[2], Donny Eddy Sam Karauwan[3]
[1] IPOSS Jakarta, Indonesia
[2] Universitas Sultan Ageng Tirtayasa
[3] Sekolah Tinggi Ilmu Hukum Manokwari

Article Info

Article history:

Received Jun, 2024
Revised Jun, 2024
Accepted Jun, 2024

Keywords:

Bibliometric Analysis
Data Privacy
Data Security
VOSviewer

ABSTRACT

This study employs bibliometric analysis to explore the expansive field of data privacy and security, utilizing data extracted from VOSviewer to identify thematic clusters, discern research trends, evaluate research opportunities, and analyze author collaboration networks. The analysis reveals several key thematic areas, including data security, legal frameworks, information privacy, and technological challenges associated with big data. These themes have evolved over time, demonstrating a shift from foundational legal principles to addressing complex technological and demographic-specific challenges, such as those related to children's data privacy. The study highlights significant concentrations of research activity as well as less explored areas that offer new opportunities for research, such as the legal status of data and specific privacy concerns that are under-represented in current literature. Furthermore, the author collaboration network provides insights into the structure of the research community, showing both dense clusters of collaboration and potential for new entrants to establish niches in emerging topics. This bibliometric perspective not only elucidates the current landscape of data privacy and security research but also points to future directions that can enhance the field's development.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta, Indonesia
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

In the era of digital transformation, the significance of personal data protection cannot be overstated [1]. With the increase in online activities, from e-commerce transactions to social networking, vast amounts of personal information are constantly being generated and collected by various entities [2]. This surge in data flow has escalated concerns regarding privacy and security, making personal data protection a critical area of legal and regulatory interest worldwide [3]. Consequently, governments and international bodies have been compelled to enact and update legal frameworks to safeguard personal data against unauthorized access and misuse [4], [5].

The landscape of data protection laws varies significantly across different jurisdictions, reflecting diverse cultural values, governance models, and technological advancements [6], [7]. For instance, the

European Union's General Data Protection Regulation (GDPR) is often considered a benchmark for personal data protection, influencing legislation beyond Europe [8]. In contrast, other countries may have less stringent or disparate approaches that pose challenges in terms of enforcement and compliance [9]. This disparity necessitates a comprehensive study to understand the evolution and effectiveness of these laws in a global context [10].

Bibliometric analysis serves as a powerful tool to map the development and focus areas within the field of legal approaches to personal data protection [11], [12]. By examining the volume and citation impact of relevant scholarly articles, this method provides insights into the most influential studies, prevailing themes, and emerging trends [13], [14]. Such an analysis not only highlights the academic discourse but also aids policymakers and practitioners in identifying best practices and areas needing further exploration [15]vv.

Despite the critical importance of legal frameworks for personal data protection, there remains a gap in comprehensive scholarly analysis that quantifies and interprets the evolution and impact of these laws globally. Most existing research tends to focus on specific regions or frameworks, such as the GDPR, without providing a global overview. There is a need for a bibliometric study that encapsulates a wide array of data protection laws, analyzing how they adapt to technological changes and address privacy challenges. This research aims to fill this gap by providing a detailed bibliometric analysis that offers a holistic view of the field's development and the interconnections between different legal systems.

The objective of this research is to conduct a bibliometric analysis of legal approaches to personal data protection. This study aims to identify the most influential works, key themes, and trends within the field over the past decade. By mapping these elements, the research seeks to understand the academic and practical impacts of various data protection laws and to evaluate how these laws evolve in response to technological advancements and societal changes.

The significance of this research lies in its potential to influence both academic scholarship and practical policy-making in the field of personal data protection. By providing a detailed bibliometric perspective, this study will help clarify the development trajectory of data protection laws and identify influential regions and authors. For policymakers and legal practitioners, the findings can serve as a basis for enhancing existing regulations, fostering international cooperation, and addressing gaps in the current legal frameworks. Ultimately, this research will contribute to the enhancement of personal data security and privacy in an increasingly digital world.

2. LITERATURE REVIEW

2.1 Evolution of Personal Data Protection Laws

The evolution of personal data protection laws has been significantly influenced by technological advancements and the increasing value of data in the digital economy. [16] provide a comprehensive overview of how early privacy concerns have morphed with the advent of digital technologies. They discuss the shift from basic data protection principles, established in early frameworks like the OECD Guidelines, to more comprehensive and enforceable regulations such as the GDPR. Furthermore, [17] extends this analysis by documenting the global proliferation of data protection laws, noting that over 120 countries have now established some form of legal protection for personal data. This global spread indicates a growing recognition of privacy as a fundamental human right, albeit implemented with varying degrees of rigor and effectiveness.

2.2 *Comparative Analysis of Data Protection Frameworks*

Research comparing different national and regional data protection frameworks highlights the diversity in legal approaches and enforcement mechanisms. [18] analyze the alignment—or lack thereof—between the United States' sectoral approach and the European comprehensive model. Their findings suggest that cultural, economic, and political factors play significant roles in shaping the specific contours of data protection laws. On the other hand, [19] focuses on the impact of the GDPR on non-EU countries, illustrating how this regulation has set a de facto global standard that many nations are adopting or adapting in their local contexts. These comparative studies are crucial for understanding the interoperability of data protection laws in a globalized world where cross-border data flows are ubiquitous.

2.3 *Bibliometric Analyses in Legal Studies*

Bibliometric methods have increasingly been applied in legal studies to explore the development of various legal fields, including personal data protection. [20] provide an example of such an application, analyzing the citation networks and thematic evolution in intellectual property law. Their methodology offers a framework that can be adapted to the study of data protection laws, enabling scholars to trace the influence of landmark papers and key themes over time. Additionally, [21] discuss the use of bibliometric tools to identify emerging trends and gaps in environmental law research, demonstrating how these methods can help predict future directions in legal scholarship.

2.4 *Challenges and Future Directions*

Despite the growth in data protection legislation, several authors identify ongoing challenges and future research directions. [22] argue that current legal frameworks are often reactive rather than proactive, struggling to keep pace with rapid technological changes such as artificial intelligence and big data analytics. They call for more dynamic and flexible legal mechanisms that can adapt to new privacy challenges as they arise. Moreover, [17] emphasize the need for greater international cooperation in enforcing data protection laws, especially in tackling issues like data breaches that have global ramifications. These challenges underscore the importance of continuous research and adaptation of data protection laws to meet the needs of the digital age.

3. METHODS

This research employs a bibliometric analysis to systematically examine the scholarly literature on legal approaches to personal data protection. The initial phase involves data collection, where articles published between 1977 and 2024 are extracted from Google Scholar. Keywords such as "data protection", "privacy law", and "personal data regulation" are used to ensure comprehensive coverage. Following the collection, the VOSviewer software tool is utilized to perform citation and co-citation analysis, allowing for the identification of the most influential authors and articles within the field. Additionally, content analysis is conducted on the abstracts and keywords of the collected articles to discern prevalent themes and trends over the observed period.

4. RESULT AND DISCUSSION

4.1 *Metrics Data of Literature*

Table 1. Research Data Metrics

Metrics Data	Information
Publication years	1977-2024
Citation years	47
Papers	980
Citations	97601
Cites/year	2076.62
Cites/paper	99.59
Cites/author	66519.32
Papers/author	710.86
Authors/paper	1.82
h-index	140
g-index	297
hI,norm	120
hI,annual	2.55
hA, index	48
Paper with ACC >=	1,2,5,10,20:714,583, 342,209,117

Source: Output Publish or Perish, 2024

Table 1 presents a comprehensive set of bibliometric indicators derived from an analysis of publications spanning from 1977 to 2024. Over these 47 years, a total of 980 papers were published, accruing an impressive 97,601 citations, which translates to an average of 2,076.62 citations per year and 99.59 citations per paper. This high citation rate reflects the significant impact of the research within the field. The data also reveals that each paper has an average of 1.82 authors, with a total author efficiency shown by 66,519.32 cites per author and 710.86 papers per author, indicating a prolific authorship within the examined studies. The h-index, a metric measuring both the productivity and citation impact of the publications, is notably high at 140, complemented by a g-index of 297, suggesting that a substantial number of papers have received a deep and broad citation impact. The normalized and annualized h-indexes are 120 and 2.55, respectively, further underscoring the enduring relevance of the research. The hA index stands at 48, indicating adjusted author impact. Additionally, a significant number of papers have achieved considerable citation counts, with 714 papers cited at least once and 117 papers cited at least 20 times, demonstrating widespread recognition and influence in the scholarly community.

4.2 *Citation Analysis*

Table 2. Most Cited Article

Citations	Author and Year	Title
3114	[23]	Information privacy: Measuring individuals' concerns about organizational practices
2884	[24]	Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness
2587	[25]	Information privacy research: an interdisciplinary review
2449	[26]	European Union regulations on algorithmic decision-making and a “right to explanation”
2126	[27]	Principles of information security
1998	[28]	Internet of Things–New security and privacy challenges
1756	[29]	Privacy in the digital age: a review of information privacy research in information systems
1567	[30]	Privacy concerns and consumer willingness to provide personal information
1514	[31]	Introduction: Privacy self-management and the consent dilemma
1442	[32]	Lex informatica: The formulation of information policy rules through technology

Source: Output Publish or Perish, 2024

Table 2 from "Publish or Perish" in 2024 lists the top ten most cited articles in the field of information privacy and security, showcasing a wide range of topics that highlight significant concerns and research directions over the years. The most cited paper by Smith, Milberg, and Burke, with 3,114 citations, delves into individual concerns about organizational practices regarding information privacy, indicating a high level of academic and practical interest in how personal information is handled by organizations. The second most cited article by Bulgurcu, Cavusoglu, and Benbasat, which has received 2,884 citations, explores the factors influencing compliance with information security policies, underscoring the importance of rationality-based beliefs and awareness in effective security management. Further down the list, articles by Goodman and Flaxman, and by Weber, address emerging issues like algorithmic decision-making in the EU and security challenges posed by the Internet of Things, reflecting evolving technological landscapes and their implications for privacy and security. This table not only highlights the pivotal contributions of these articles to the discourse on information privacy and security but also mirrors the shifting focus of research as it responds to new technological challenges and regulatory environments.

4.3 Keyword Co-Occurrence Analysis

1. Network Visualization

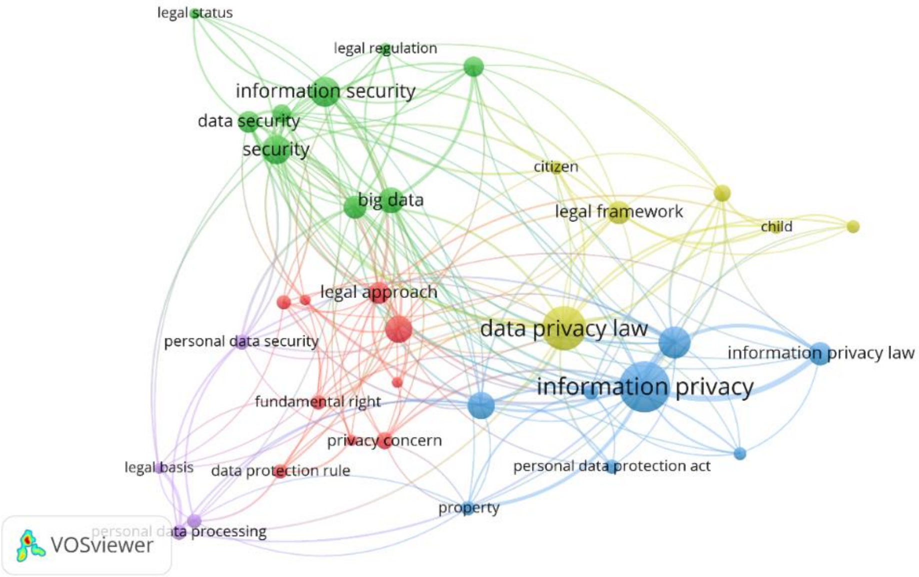

Figure 1. Network Visualization
Source: Data Analysis, 2024

The image displays various nodes (representing key terms or topics) connected by lines, which indicate the relationships (such as thematic or terminological similarities) between these nodes. The different colors of the nodes and the clusters they form represent distinct thematic areas within the broader topic of data privacy and protection:

1. Red cluster, this seems to focus on the legal and personal security aspects of data privacy, with terms like "personal data security", "legal approach", and "privacy concern". This cluster suggests an emphasis on the individual's rights and the legal mechanisms in place to protect these rights.
2. Green cluster, it includes terms like "information security", "data security", and "big data". This cluster appears to deal with the technical and practical aspects of protecting data, particularly in contexts involving large datasets or complex information systems.
3. Blue cluster, highlighting "information privacy", "data privacy law", and "information privacy law", this cluster is closely related to regulatory and legal frameworks specific to privacy. It seems to center on the laws that govern information privacy, indicating a focus on statutory provisions and legal discourse.
4. Yellow cluster, with nodes like "legal framework", "citizen", and "child", this cluster might explore demographic-specific and jurisdiction-specific frameworks of data protection, possibly discussing how different segments of the population (like minors) are affected by data privacy laws.
5. Purple cluster, comprising terms like "personal data security," "legal basis," and "personal data processing," focuses on the intersection of legal principles and practical data management. It highlights the foundational legal justifications for data protection regulations and the practical methods of handling personal data securely. This cluster bridges the gap between theoretical legal frameworks and their practical application in safeguarding personal information. It underscores the importance of compliance, detailing how organizations must adapt their data handling processes to align with legal requirements. This focus on both the legal underpinnings and the operational aspects of data privacy serves as a critical guide for stakeholders in developing effective data protection strategies that comply with existing laws.

2. Overlay Visualization

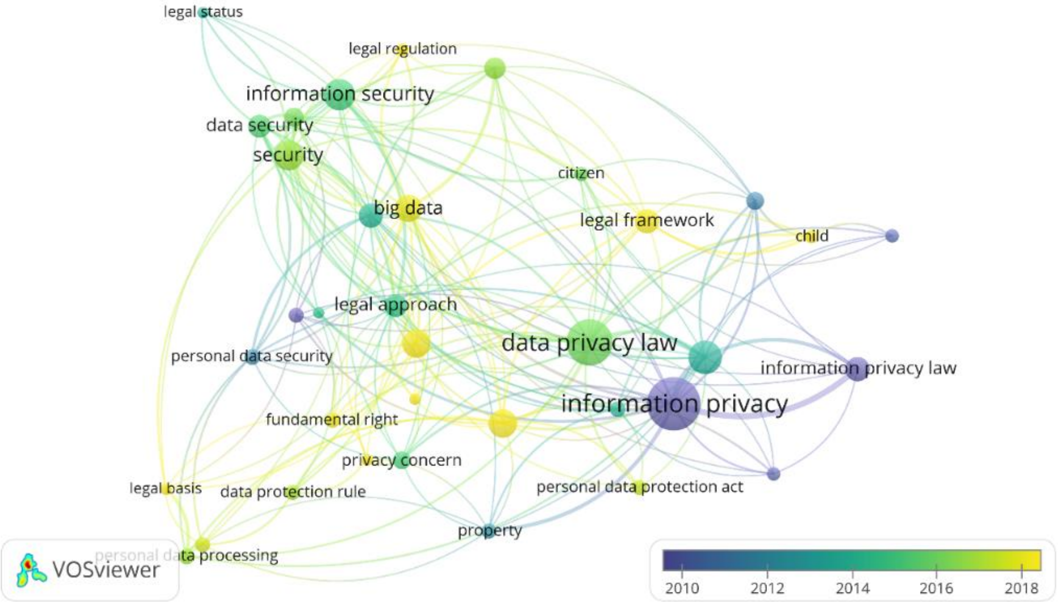

Figure 2. Overlay Visualization
Source: Data Analysis, 2024

This second shows a temporal overlay on a bibliometric network, using VOSviewer, focusing on the key topics within the domain of data privacy and security laws, mapped over the years from 2010 to 2018. The temporal overlay indicates the prominence and evolution of different themes over time based on color coding from blue (earlier years) to yellow (later years).

In the earlier years, topics such as "legal basis," "personal data security," and "data protection rule" dominate the discourse, shown in blue and green hues. This suggests that during this period, the focus was heavily on establishing foundational legal principles and frameworks for data protection. The prominence of "legal approach" during these years aligns with global movements towards crafting and solidifying laws like the GDPR in Europe, which was formally proposed in 2012. The discussion appears to be more centered around the conceptualization and initial formulation of data protection regulations, setting the stage for more detailed and specific legislation.

As we move towards the middle years, represented by green and transitioning into yellow nodes, there is a noticeable shift towards more specific applications of these legal frameworks. Terms like "information privacy" and "personal data processing" gain prominence. This shift likely correlates with the broader implementation of data protection laws and the growing public and corporate awareness of data privacy issues. During this period, there's an increasing focus on how laws are practically applied and enforced, including discussions on the implications for both individuals and organizations.

In the more recent years, leading up to 2018, the nodes become predominantly yellow, indicating a matured focus on topics such as "information security" and "big data." This evolution signifies a response to technological advancements and the challenges posed by the increasing volume and complexity of data. The discussion around "big data" reflects the burgeoning issues related to managing vast datasets under strict privacy laws like the GDPR, which was enforced starting in 2018. Furthermore, the node "child" emerging in these later years suggests a nuanced concern for specific demographic groups, possibly driven by rising online engagement among younger populations and the consequent privacy risks.

3. Density Visualization

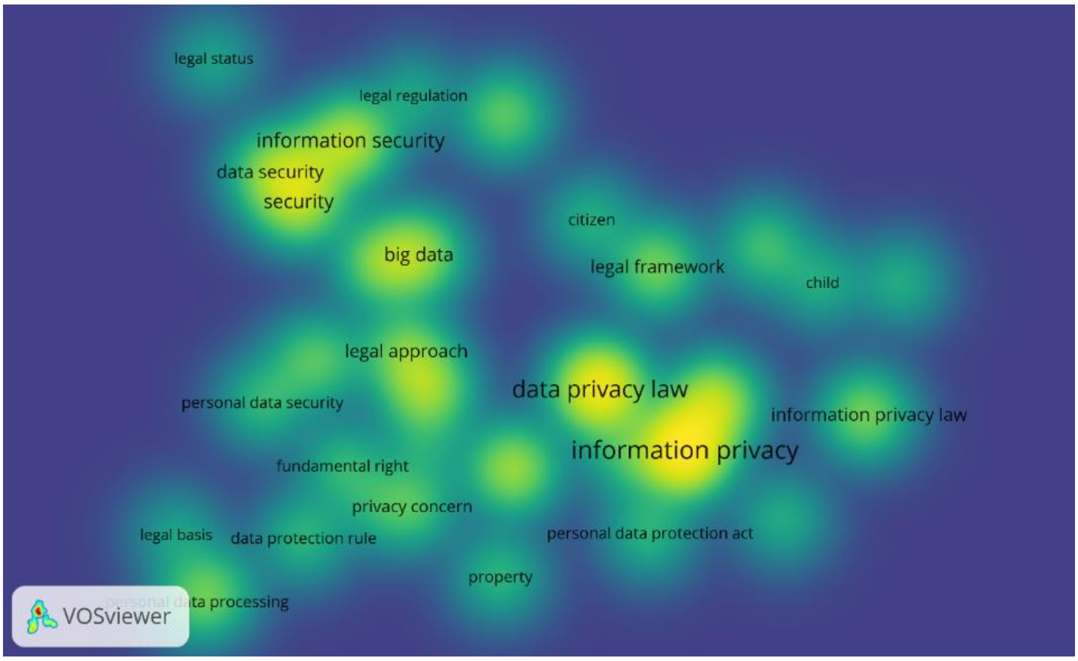

Figure 3. Density Visualization
Source: Data Analysis, 2024

The third is a density visualization created with VOSviewer, illustrating the distribution and concentration of research topics within the field of data privacy and security. This type of visualization uses color intensity to indicate the relative density of research activity around specific terms or topics, with brighter areas showing higher concentrations of research and darker areas indicating less research activity.

The bright areas in the visualization, particularly around terms like "information privacy," "data privacy law," and "big data," suggest these are well-trodden research paths with a substantial body of existing literature. This concentration could indicate that these areas are continuously evolving and remain critical topics within the field, possibly due to ongoing developments in technology and legislation.

The darker areas in the visualization, such as around "legal basis," "legal status," and "privacy concern," indicate topics that might be less explored in comparison to the core areas. These less illuminated regions represent potential research opportunities where future studies could make significant contributions:

1. Legal Basis and Legal Status

These areas might benefit from further exploration to understand the foundational legal principles that underpin data privacy laws and how they are recognized and applied in different jurisdictions. There could be a need for comparative legal studies that examine the variances in the legal status of data privacy across different countries, which could be crucial for multinational corporations and policymakers.

2. Privacy Concern

   Despite being a central theme in data privacy discourse, the less intense illumination suggests that there might be new dimensions of privacy concerns that are under-researched. This could involve studying the evolving nature of privacy concerns in the face of new technologies like AI and IoT, or understanding demographic-specific privacy concerns, which could guide more targeted and effective privacy policies and technologies.

3. Personal Data Security

   Although it is a crucial aspect of data privacy, the relatively darker area around this term compared to the central topics might indicate a gap in specific sub-topics within the realm of personal data security, such as advanced encryption methods or security practices for emerging technologies.

4. Child

   This term appears in a less bright area, suggesting that the specific issues related to data privacy for children might not be as heavily researched. This presents an opportunity to delve into how data protection laws cater to minors, especially in online environments, which are increasingly accessed by younger age groups.

4.4 Co-Authorship Analysis

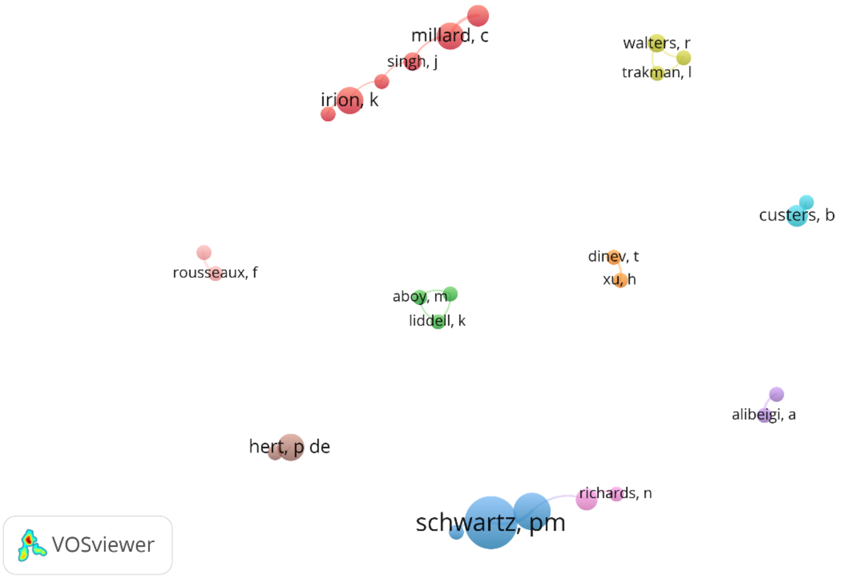

Figure 4. Density Visualization
Source: Data Analysis, 2024

The image above is a VOSviewer visualization that maps a network of authors within a specific research field, where each node represents an individual researcher. The proximity of nodes indicates collaborative relationships or thematic similarities in their work. The visualization is color-coded to differentiate between distinct clusters or groups. The red cluster, including authors like Irion K., Millard C., and Singh J., likely focuses on foundational aspects of the field. The green cluster, with Aboy M. and Liddell K., appears to explore a niche area, possibly a new or emerging topic. The blue cluster, featuring Richards N., Schwartz P.M., and Custers B., suggests a group working on applied aspects or specific technological applications. Lastly, the purple node, Alibeigi A., stands alone, indicating that this author might be a new entrant or working on a unique aspect of the field not yet widely integrated with other research. This map is useful for identifying key researchers and understanding their collaborative networks, which is beneficial for new researchers or those seeking to establish partnerships.

5. CONCLUSION

The various analyses of the bibliometric data reveal distinct thematic clusters, research trends, and potential opportunities within the field of data privacy and security. The thematic clusters identified through the VOSviewer visualizations, such as data security, legal frameworks, and information privacy, highlight the core areas of focus and their evolution over time. These themes have shifted from foundational legal discussions to more complex issues like big data and specific demographic concerns like child data privacy, reflecting the field's response to technological advancements and societal changes. The research trends show a maturation of the field, moving from theoretical legal bases to applied technological challenges. Opportunities for further research have been pinpointed in less explored areas, such as the legal status and specific privacy concerns, which are less represented in the current literature. Additionally, the visualization of author collaborations indicates a well-connected research community with potential for new researchers to join established networks or carve out new niches in under-researched areas. Collectively, these insights not only enhance understanding of the field's current landscape but also guide future scholarly and practical endeavors in data privacy and security.

REFERENCE

[1] A. Yarali, “Cybersecurity in Digital Transformation Era,” 2023.

[2] G. Harinath, “Does personal data protection matter in data protection law? A transformational model to fit in the digital era,” *Handb. Big Data Res. Methods*, pp. 267–278, 2023.

[3] V. P. Shehu and V. Shehu, “Human rights in the technology era–Protection of data rights,” *Eur. J. Econ. Law Soc. Sci.*, vol. 7, no. 2, pp. 1–10, 2023.

[4] M. Bocharnikova, T. Pestunova, and V. Selifanov, “Personal information security issues in the context of digital transformation of the economy, management and public communications,” *Digit. Technol. Secur.*, pp. 36–52, Apr. 2023, doi: 10.17212/2782-2230-2023-1-36-52.

[5] S. Solovkin, “Automated Collection of Data on a Person: Implicit Principles of Legal Regulation,” *Cour. Kutafin Moscow State Law Univ.*, pp. 90–100, Apr. 2023, doi: 10.17803/2311-5998.2023.102.2.090-100.

[6] A. Vuković, “Digital Evidence and Protection of Personal Data: Sociological and Law Aspect,” 2022.

[7] R. Romansky, *Digital Age and Personal Data Protection*. 2022.

[8] C. Wanyi and M. Luqi, “Shanghai Urban Digital Transformation and Enterprise Personal Data Protection,” *J. Circuits, Syst. Comput.*, vol. 32, Dec. 2022, doi: 10.1142/S0218126623501803.

[9] J. Bi, Y. Guo, N. He, and S. Wang, “Research on Personal Information Security Protection Measures in the Big Data Era,” *Int. J. New Dev. Eng. Soc.*, vol. 7, no. 2, 2023.

[10] T. Malik, “Digital Transformation through the Prism of Digital Identity,” *J. Public Policy Pract.*, vol. 1, no. 2, pp. 33–48, 2022.

[11] S. P. Index and G. Index, “Executive summary,” *URL https//glavcom. ua/pub/pdf/49/4938/10_1. pdf*, 2018.

[12] D. P. F. Möller, “Cybersecurity in digital transformation,” in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, Springer, 2023, pp. 1–70.

[13] C. Hu, “Protection of Personal Information in the Era of Big Data,” *Front. Humanit. Soc. Sci.*, vol. 2, pp. 184–193, Sep. 2022, doi: 10.54691/fhss.v2i9.2128.

[14] P. Samadi-Parviznejad, “The role of big data in digital transformation,” *J. Data Anal.*, vol. 1, no. 1, pp. 42–47, 2022.

[15] E. Kornacka and M. Monkiewicz, “Consumer protection in the financial market in the era of digital transformation,” in *Digital Finance and the Future of the Global Financial System*, Routledge, 2022, pp. 161–179.

[16] P. M. Schwartz and D. J. Solove, “The PII problem: Privacy and a new concept of personally identifiable information,” *NYUL rev.*, vol. 86, p. 1814, 2011.

[17] G. Greenleaf and S. Livingston, “China’s personal information standard: the long march to a privacy law,” 2017.

[18] C. J. Bennett and C. D. Raab, “Revisiting the governance of privacy: Contemporary policy instruments in global perspective,” *Regul. Gov.*, vol. 14, no. 3, pp. 447–464, 2020.

[19] L. A. Bygrave, “Data protection by design and by default: deciphering the EU’s legislative requirements,” *Oslo Law Rev.*, vol. 4, no. 2, pp. 105–120, 2017.

[20] L. M. I. Marcussen, “Promotion of Active and Healthy Ageing through mHealth for Healthy Older Adults: a scoping review.,” 2020.

[21] F. J. Martínez-López, J. M. Merigó, J. C. Gázquez-Abad, and J. L. Ruiz-Real, “Industrial marketing management: Bibliometric overview since its foundation,” *Ind. Mark. Manag.*, vol. 84, pp. 19–38, 2020.

[22] C. Kuner, “International organizations and the EU general data protection regulation: exploring the interaction between EU law and international law,” *Int. Organ. law Rev.*, vol. 16, no. 1, pp. 158–191, 2019.

[23] H. J. Smith, S. J. Milberg, and S. J. Burke, “Information privacy: Measuring individuals’ concerns about organizational practices,” *MIS Q.*, pp. 167–196, 1996.

[24] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness,” *MIS Q.*, pp. 523–548, 2010.

[25] H. J. Smith, T. Dinev, and H. Xu, “Information privacy research: an interdisciplinary review,” *MIS Q.*, pp. 989–1015, 2011.

[26] B. Goodman and S. Flaxman, “European Union regulations on algorithmic decision-making and a ‘right to explanation,’” *AI Mag.*, vol. 38, no. 3, pp. 50–57, 2017.

[27] M. E. Whitman and H. J. Mattord, *Principles of information security*. Thomson Course Technology Boston, MA, 2009.

[28] R. H. Weber, “Internet of Things–New security and privacy challenges,” *Comput. law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[29] F. Bélanger and R. E. Crossler, “Privacy in the digital age: a review of information privacy research in information systems,” *MIS Q.*, pp. 1017–1041, 2011.

[30] J. Phelps, G. Nowak, and E. Ferrell, “Privacy concerns and consumer willingness to provide personal information,” *J. public policy Mark.*, vol. 19, no. 1, pp. 27–41, 2000.

[31] D. J. Solove, “Introduction: Privacy self-management and the consent dilemma,” *Harv. L. Rev.*, vol. 126, p. 1880, 2012.

[32] J. R. Reidenberg, “Lex informatica: The formulation of information policy rules through technology,” *Tex. L. Rev.*, vol. 76, p. 553, 1997.