Revista de Științe Politice. Revue des Sciences Politiques • No. 85 • 2025: 43 – 56

ORIGINAL PAPER

Theorizing Digital Security Governance and Biometric Data Inputs based on Research Topics and Online Mentions Tracking

Anca Parmena Olimid[1], Cătălina Maria Georgescu[2], Daniel Alin Olimid[3], Silviu Dorin Georgescu[4], Cosmin Lucian Gherghe[5]

Abstract:
Introduction: Research on topics in the field of digital security governance and biometrics presents multiple opportunities for analysis depending on the conceptual framework and informational support of data collection.

Research objectives: This study initiates and engages in a complex and interdisciplinary investigation of topics in the field of digital security governance and biometric data. The primary objective focuses on the analysis of the frequency of use in the scientific literature of the most important concepts associated with the two fields, and the second objective of the study illustrates the acceptability and circulation of relevant topics in the digitized literature.

Research methodology: The research uses the Google Ngram Viewer technique to select, collect and extract over twenty topics and other phrases relevant to the analysis of digital security governance and biometrics in the period 2000-2022. For the selection of topics and associated phrases, we will use the specific terminology provided by the International Organization for Standardization (ISO/IEC 2382-37:2022, Information technology — Vocabulary Part 37: *Biometrics*) (edition 3, 2022), but also the collection of sources and references provided by the World Bank (Practitioner's Guide) regarding the fields: biometric identification, legal and digital identity, privacy framework, personal data, data protection, digital signatures, e-governance and information technology.

Results and discussion: The results of the online investigation offer multidimensional perspectives on digital security governance, biometrics and behavioral biometrics,

[1] Associate Professor, Ph.D., Faculty of Social Sciences, University of Craiova, 13th Street A. I. Cuza, Craiova, Romania, Email: anca.olimid@edu.ucv.ro. ORCID: 0000-0002-7546-9845.

[2] Lecturer, Ph.D., Faculty of Social Sciences, University of Craiova, 13th Street A. I. Cuza, Craiova, Romania, Email: catalina.georgescu@edu.ucv.ro, ORCID ID https://orcid.org/0000-0002-4462-4689

[3] Lecturer, Ph.D., Biology Specialization, University of Craiova, 13th Street A. I. Cuza, Craiova, Romania, Email: daniel.olimid@edu.ucv.ro. ORCID: orcid.org/0000-0001-5583-668X

[4] Ph.D., ORCID ID https://orcid.org/0000-0002-5187-6892.

[5] Associate Professor, PhD, University of Craiova, Faculty of Social Sciences, Craiova, Romania, Phone: 0040351403149, Email: cosmin.gherghe@edu.ucv.ro. https://orcid.org/0000-0002-9131-0391

projecting the applicability of the topics for data security and information confidentiality. The results also indicate the importance of the biometric component and the role of the characteristics of the technologies.

Conclusions: The conclusions of the study provide an overview of the taxonomy of topics in the digital security governance and biometrics, but also an indexing of the highest conceptual frequencies. The limits of the research are also discussed, as well as future directions for analysis.

Keywords: *digital security governance, biometrics, biometric data, legal and digital identity, e-governance.*

Introduction

The increase in Denial of Service and ransomware cyberattacks has led to numerous breaches of cybersecurity protocols in recent years. With the increase in attacks and the vulnerability of personal and biometric data protection systems, the scientific community has expanded the scope of research in the field of digital security (Kavitha, Prasannakuma, Pranav, 2024) with the aim of identifying the most secure connection methods, biometric data security keys and authentication applications, including facial ID connection, as well as other facial and fingerprint recognition possibilities and the approach to human security developments and features (Olimid, Georgescu, Olimid, 2024a).

The research reflects a deep interdisciplinary and multidisciplinary character, being based on knowledge from (a) the field of biometrics, personal data and genetic data: fingerprint, facial recognition, biological properties, psychological characteristics (Olimid, Rogozea, Olimid, 2018); (b) the legal field: legislation on personal data and the processing of such data, equal provisions on data breaches, free movement of personal data and risk assessment; (c) the field of digital security and data management: using a password, unlocking a system, password leaks, password transfer.

In this context, the present research approach investigates a broad evolution of the use of topics in the field of digital security governance and biometrics by using the Google Ngram Viewer platform. The investigation also has the role of highlighting in the first part of the research how the scientific literature digitized by Google has accessed, employed and used these topics in the field of biometric login and identity verification. At the same time, the most important frequency notifications of the selected topics will be expressly mentioned and specific discussions and analyses will be developed regarding the appropriateness of using the topic or the associated phrase of words.

The paper delimits in the final section the limits of the research regarding human security personal data, their protection and free circulation (Olimid, Georgescu, Olimid, 2024b). Also, in considering the arguments presented, guidelines are offered for future research in the field of digital security and biometric data.

Literature review

The analysis of the digital security governance and biometric data field in the dedicated literature review section primarily reflects the criteria used to collect and analyze relevant information by focusing on the most important topics, concepts and word associations, as well as theories and applicable models of digitized literature in the analyzed period.

This category includes thematic domains of recent scientific literature focused on the analysis of security vulnerabilities and the impact on biometric systems (Abdullaeva, Imamverdiyev, Musayev, Wayman, 2008), as well as new trends and developments in the field of biometric security (Maguire, 2009; Bromby, 2010; Ross, Banerjee, Chowdhury, 2020).

The second criterion for selecting works records the role of standards, classification criteria and methodologies for the specific category of selected topics, but also for the classes of concepts of the research area namely: (a) approaches to biometric security, financial systems and digital payment solutions (Maskey, 2024); (b) research patterns and links between AI, big data and biometric authentication (Mukkamala, Mahida, Vishwanadham Mandala, 2024) and (c) factual and categorical analysis data related to biometric-based physical and cybersecurity management (Obaidat, Traore, Woungang, 2019).

Thirdly, another important criterion for selecting relevant works must target both the theoretical and applied foundations of the research field of digital security and biometric data and distinguish essential information chronologically and thematically, including relevant research on: (a) authentication systems and behavioral biometrics published in the last two years (Oduri, 2024; Sett, Gupta, 2024; Shafik, Tufail, Apong, Balasubramaniam, 2024; Sriman, Thapar, Alyas, Singh, 2024, January); (b) relevant aspects for digital security and e-commerce (Patil, Dudhankar, Shukla, 2024).

Numerous studies have revealed and analyzed concerns over biometric security and information security breaches, mechanisms and services (Singleton, 2003: 1-24). Several studies have focused on analysing biometric systems enhancement of authentication through deep learning against cyber-attacks (Arora, Bhatia, 2021: 28-48). The dawns of biometric security technologies with the introduction of innovative authentication but also identification programs have pushed forwards the discussions over security and privacy with a straightforward focus over conceptualization details (van der Ploeg, 2003: 85–104).

The use of biometric security in authentication has also been discussed with focus on implications, predictions and perceptions over governmental policy options (Seyal, Turner, 2012: 1242–1256). The efficiency of different solutions for the use of biometric passports and e-passports has also been discussed (Choudhury, Rabbani, 2019: 199–229). Also, in essential economic fields such as finances and banks, breaches to cyber-security have brought into discussion legislative options of increasing authentication security, thus focusing on the factors and perceptions for the effectiveness and outcomes of such measures (Laux, Luse, Mennecke, Townsend, 2011: 221–245). It is further argued that biometrics increases security of online transactions, still researchers inquire on the manner in which markets respond to such measures (Kleist, 2007: 319-329).

Various biometric solutions are the target of academic research, comparisons including unimodal biometric versus multimodal fusion biometric frameworks (Bala, Gupta, Kumar, 2021: 289–337). Different approaches against falsifying authentication procedures are also discussed in terms of effects and outcomes, roles in the process for governments and legislatives, scope of actions and regulations, and acts of the falsifier (Grünenberg, 2020: 223–240). Cyber security concerns have also been elevated to the Internet of Things (IoT) to apply new biometric authentication systems instead of traditional text password (Meena, Choudhary, 2019: 643–652).

Research methodology

The research uses the Google Ngram Viewer collection technique, which is a graphical tool for analyzing and interpreting the frequencies of use of words or phrases of words associated with them in the period selected for analysis. The selected, collected and extracted data set is categorized for analysis by entering the search options for a word, phrase or expression and analyzing the frequencies of occurrences, that is, the number of times the respective word or phrase was used in the selected period.

The topic repertoire is based on text search in English and is intended to highlight the most important dependencies of the use of topics in the selected data interval.

Data exploration highlights the relative frequency of their use over time, reflecting the semantic characteristics of the selected words and phrases by reporting to the following typology of investigation depending on the value that < n> can take: n=1 (unigram); n=2 (bigram); n=3 (trigram); n=4 (quadgram); n (ngram).

To select over twenty topics and other expressions relevant to the field of digital security governance and biometrics analysis, we will use the semantic and terminological features provided by the International Organization for Standardization (ISO/IEC 2382-37:2022, Information technology — Vocabulary Part 37: Biometrics, 3rd edition), as well as reference sources from the World Bank (data retrieved March 2025), as well (Practitioner's Guide) on the specific research areas of biometric identification, legal and digital identity, privacy and personal data (World Bank, 2025).

The research results reflect thirteen distinct figures as a result of frequency representations and graphical visualization as follows: 1) topics according to data types: digital age, information age, data governance, government data, e-governance; 2) topics according to the category of personal data and informational support: genetic data, biometric data, personal data, personal information, sensitive information; 3) topics in the category of biometric data and biological data (including biological properties, psychological characteristics): data privacy, facial recognition, fingerprint, DNA samples; 4) topics in the category of identification and recognition on digital support: digital identification, information privacy, biometric technologies, data protection, individual authentication; 5) results of the wildcard search (*) according to the terminological and semantic variables in a phrase such as wildcard search for biometric concept; 6) results of the wildcard search (*) according to the conceptual associations of a topic such as wildcard search for conceptual associations with biometric concept; 7) identifying the most frequent and common expressions and studying the semantic and linguistic variability of a term in the lexical field of a concept such as: biometric verification, biometric characteristics, biometric recognition, biometric sensor, biometric verification; 8) identifying and analyzing the frequencies of appearance and use in the digitalized literature of topics in the lexical field of authentication technologies intended to identify a person based on biometric traits namely: voice biometric, physiological biometric, behavioral biometrics; 9) identifying and analyzing the frequencies of appearance and use of heath data intended to provide information related to the health status of a person namely: wild card search for concepts associated with health * data. This type of data selected for analysis is based on the extraction of data used by the digitalized literature relating to a wider and more complex range of types of health data such as: clinical data, genetic data and personal data of the patient, data and information related to the use and utilization of medical devices.

Results and findings

The interest in biometric systems and biometric data security has developed rather recently, proof for this statement residing in the outcomes of online searches and the presence in the scientific literature. Thus, the following graphical representations outline the results of searches on Google Ngram Viewer platform for concepts and associations of concepts occurrences in the online digitized literature.

The first word search has been centered around *digital age, information age, data governance, government data and e-governance*. We noticed that except for "information age" (which recorded its highest occurrence value in 1998) all concepts peaked towards 2022, the prevailing concept in the search group being "digital age".

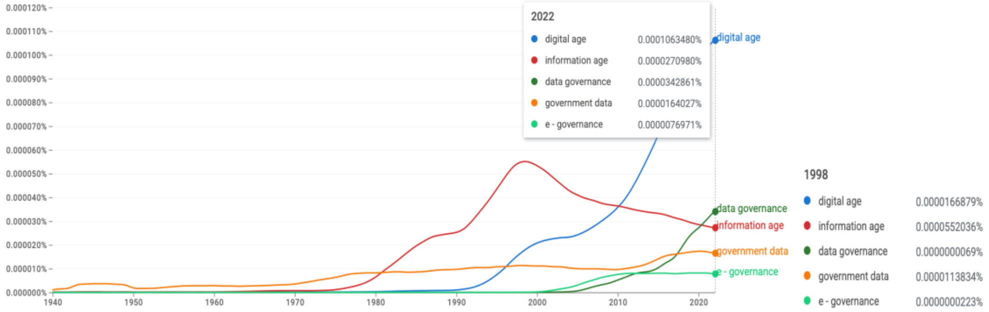


Figure 1. Ngram search for digital age, information age, data governance, government data, e-governance conceptual cluster

The second search evolved around the cluster of sensitive information and data: *genetic data, biometric data, personal data, personal information, sensitive information*. We noticed the growing rate of occurrences after 1970 towards the end of the monitoring period, especially for the concepts "personal data" and "personal information", which formed a huge interest for the literature, for regulatory bodies and regulation options.

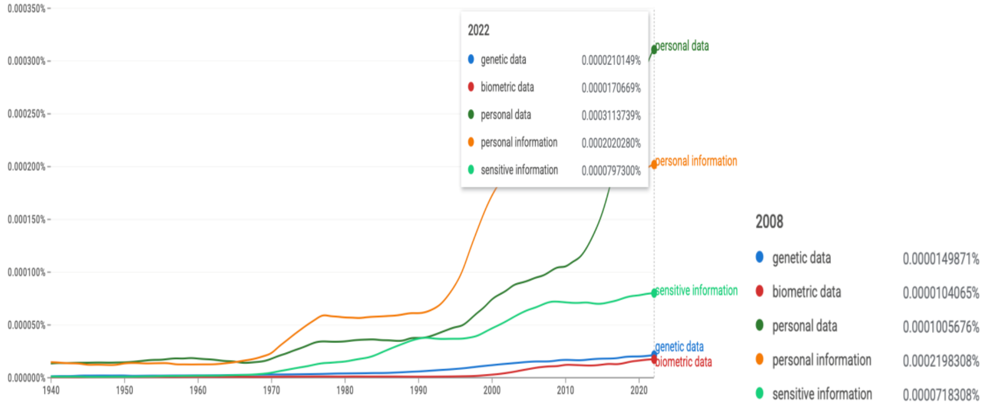


Figure 2. Ngram search for genetic data, biometric data, personal data, personal information, sensitive information conceptual cluster.

Further, we introduced in the *ngram* search data engine the concepts *data privacy, facial recognition, fingerprint and DNA samples.* Based on the *ngrams* returned, we observed a higher interest around DNA discussions around 2008, while facial recognition and data privacy show a steep increase between 2010-2022.

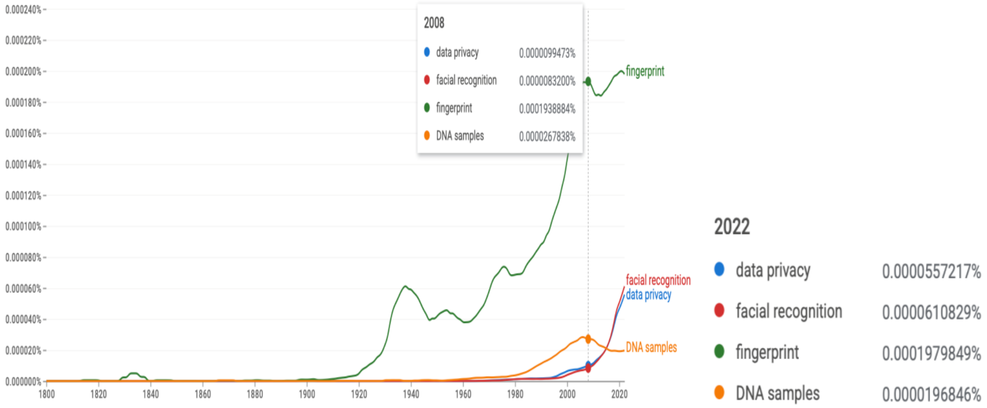


Figure 3. Ngram search for data privacy, facial recognition, fingerprint, DNA samples

Moreover, the data search for *digital identification, information privacy, biometric technologies, data protection, individual authentication* returned a representation of concept occurrences which makes obvious the literature interest for information privacy and especially for data protection.

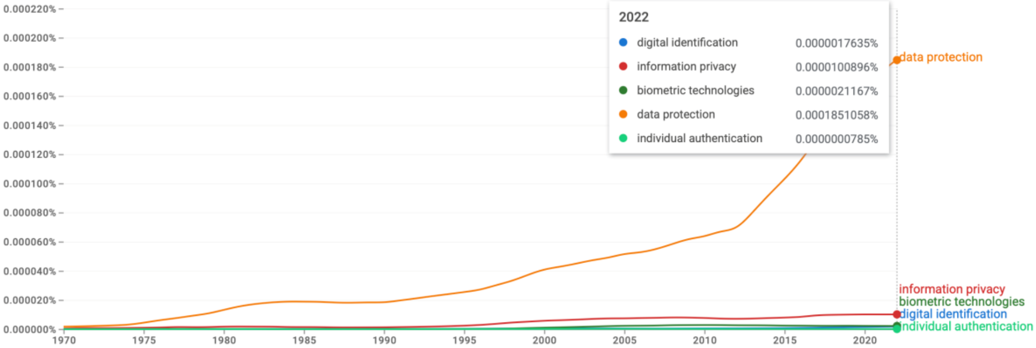
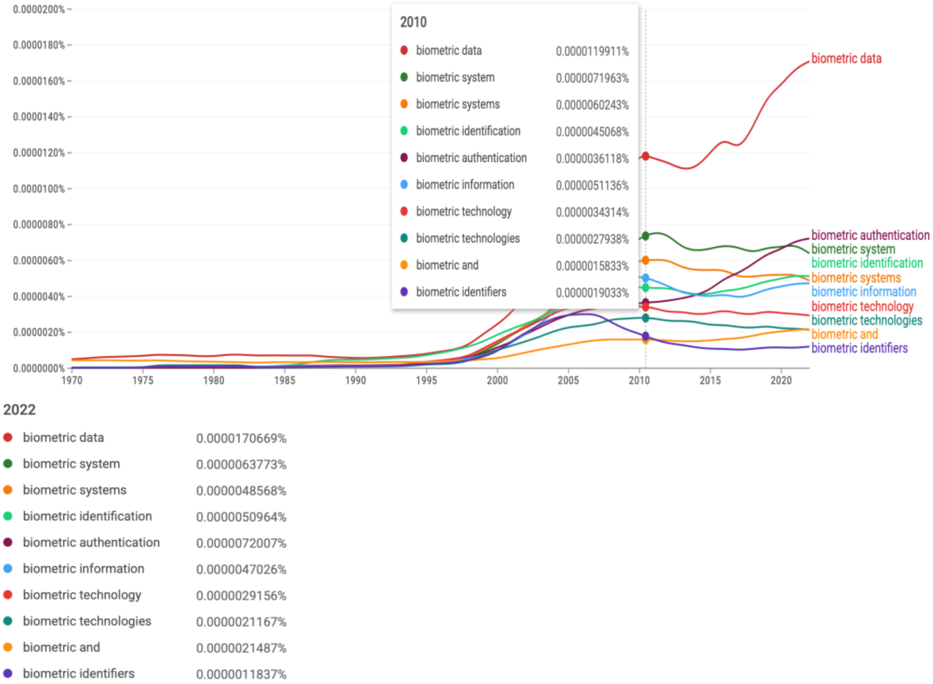


Figure 4. Ngram search for digital identification, information privacy, biometric technologies, data protection, individual authentication

The next stage was the analysis of returns following the wildcard search for conceptual associations around biometric adjective: biometric data, biometric system(s), biometric identification, biometric authentication, biometric information, biometric technology(ies), and biometric identifiers. These associations appear to have increased their occurrences in general at the end of 90s, reaching a peak around 2010. Biometric data continued its ascension towards 2022.

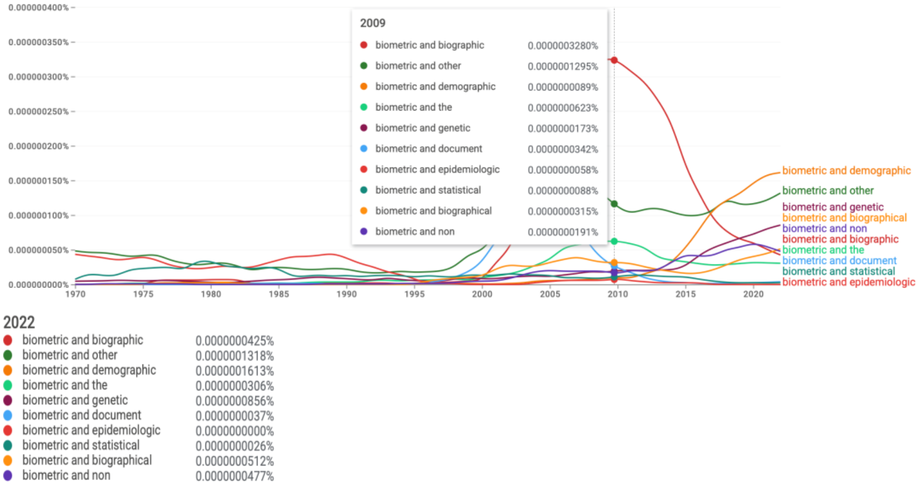


2010	
● biometric data	0.0000119911%
● biometric system	0.0000071963%
● biometric systems	0.0000060243%
● biometric identification	0.0000045068%
● biometric authentication	0.0000036118%
● biometric information	0.0000051136%
● biometric technology	0.0000034314%
● biometric technologies	0.0000027938%
● biometric and	0.0000015833%
● biometric identifiers	0.0000019033%

2022	
● biometric data	0.0000170669%
● biometric system	0.0000063773%
● biometric systems	0.0000048568%
● biometric identification	0.0000050964%
● biometric authentication	0.0000072007%
● biometric information	0.0000047026%
● biometric technology	0.0000029156%
● biometric technologies	0.0000021167%
● biometric and	0.0000021487%
● biometric identifiers	0.0000011837%

Figure 5. Wildcard search for biometric concept

Another wildcard search around the same concept aimed at identifying the most frequent online occurrences returned the associations of the concept biometric with the following terms: biographic, demographic, genetic, document, epidemiologic, statistical, and biographical.



2009	
● biometric and biographic	0.0000003280%
● biometric and other	0.0000001295%
● biometric and demographic	0.0000000089%
● biometric and the	0.0000000623%
● biometric and genetic	0.0000000173%
● biometric and document	0.0000000342%
● biometric and epidemiologic	0.0000000058%
● biometric and statistical	0.0000000088%
● biometric and biographical	0.0000000315%
● biometric and non	0.0000000191%

2022	
● biometric and biographic	0.0000000425%
● biometric and other	0.0000001318%
● biometric and demographic	0.0000001613%
● biometric and the	0.0000000306%
● biometric and genetic	0.0000000856%
● biometric and document	0.0000000037%
● biometric and epidemiologic	0.0000000000%
● biometric and statistical	0.0000000026%
● biometric and biographical	0.0000000512%
● biometric and non	0.0000000477%

Figure 6. Wildcard search for conceptual associations with biometric concept

The following search targeted the associations *biometric verification, biometric characteristics, biometric recognition, biometric sensor, biometric verification* in order to infer on the trends and values of occurrences monitored until 2022.

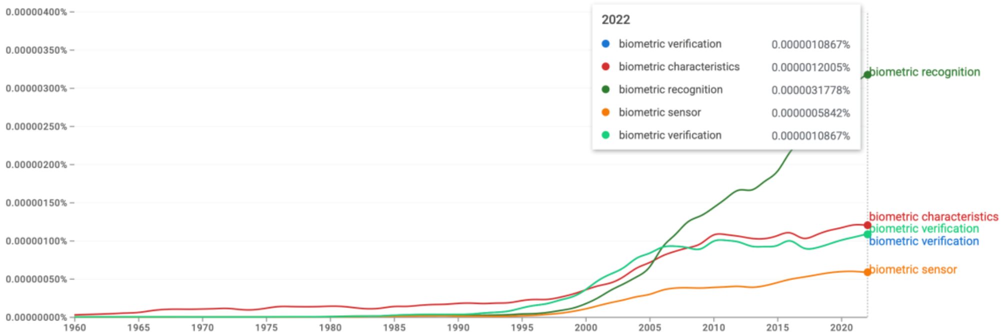


Figure 7. Occurrence of concepts: biometric verification, biometric characteristics, biometric recognition, biometric sensor, biometric verification

Also, the search retrieved the following conceptual associations voice biometric, physiological biometric, behavioural biometrics, which boost their presence in the online literature following 2000s.

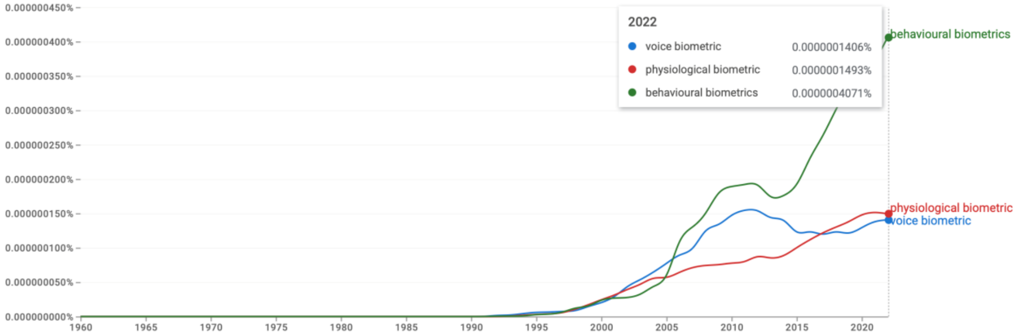
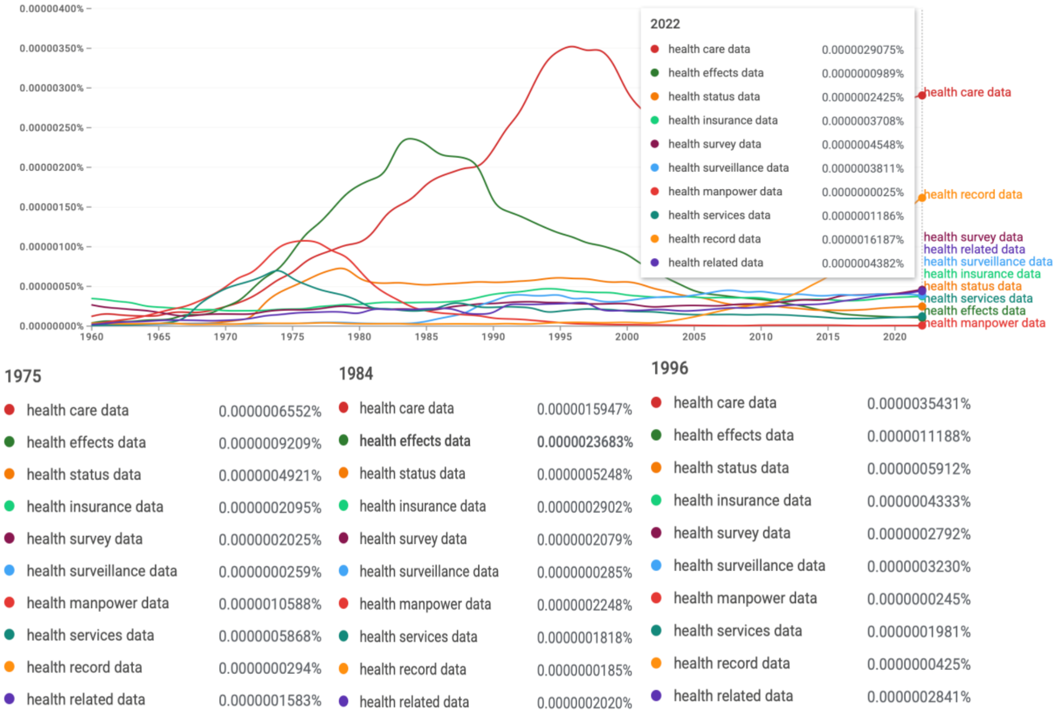


Figure 8. Occurrence of concepts: voice biometric, physiological biometric, behavioral biometrics

Aimed at identifying the manner in which essential and sensitive societal fields such as healthcare are associated to data, we accomplished a wildcard search for concepts associated to both health and data which returned the following *ngrams*: health care data, health effects data, health status data, health insurance data, health survey data, health surveillance data, health manpower data, health services data, health record data, health related data.



2022	
● health care data	0.0000029075%
● health effects data	0.0000000989%
● health status data	0.0000002425%
● health insurance data	0.0000003708%
● health survey data	0.0000004548%
● health surveillance data	0.0000003811%
● health manpower data	0.0000000025%
● health services data	0.0000001186%
● health record data	0.0000016187%
● health related data	0.0000004382%

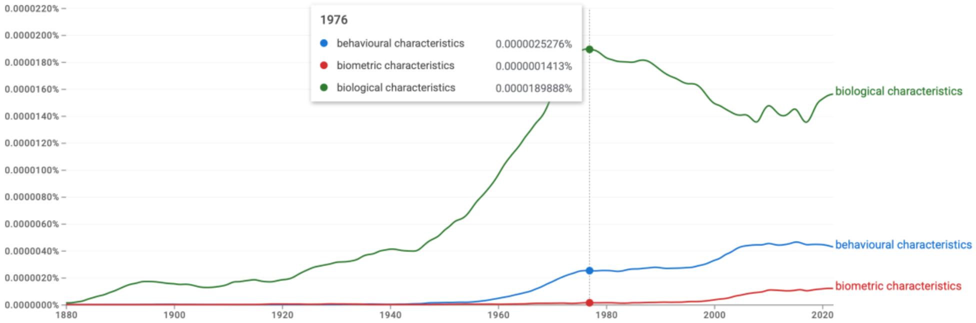
1975	
● health care data	0.0000006552%
● health effects data	0.0000009209%
● health status data	0.0000004921%
● health insurance data	0.0000002095%
● health survey data	0.0000002025%
● health surveillance data	0.0000000259%
● health manpower data	0.0000010588%
● health services data	0.0000005868%
● health record data	0.0000000294%
● health related data	0.0000001583%

1984	
● health care data	0.0000015947%
● health effects data	0.0000023683%
● health status data	0.0000005248%
● health insurance data	0.0000002902%
● health survey data	0.0000002079%
● health surveillance data	0.0000000285%
● health manpower data	0.0000002248%
● health services data	0.0000001818%
● health record data	0.0000000185%
● health related data	0.0000002020%

1996	
● health care data	0.0000035431%
● health effects data	0.0000011188%
● health status data	0.0000005912%
● health insurance data	0.0000004333%
● health survey data	0.0000002792%
● health surveillance data	0.0000003230%
● health manpower data	0.0000000245%
● health services data	0.0000001981%
● health record data	0.0000000425%
● health related data	0.0000002841%

Figure 9. Wild card search for concepts associated to health * data

Further, the research consisted in applying the search and extract the values for behavioral characteristics, biometric characteristics, biological characteristics associations referring to their appearance in the digitized literature. The data resulted shows a different onset for biological characteristics versus behavioral and biometric characteristics.



1976	
● behavioural characteristics	0.0000025276%
● biometric characteristics	0.0000001413%
● biological characteristics	0.0000189888%

Figure 10. Occurrence of concepts: behavioral characteristics, biometric characteristics, biological characteristics

The next step consisted in identifying the values of concept occurrence for specific concepts biometric capture, biometric recognition system, biometric verification system defined by the International Organization for Standardization (ISO/IEC 2382-37:2022). Consequently, we observed the usage trend after 2000 in line with industry developments.

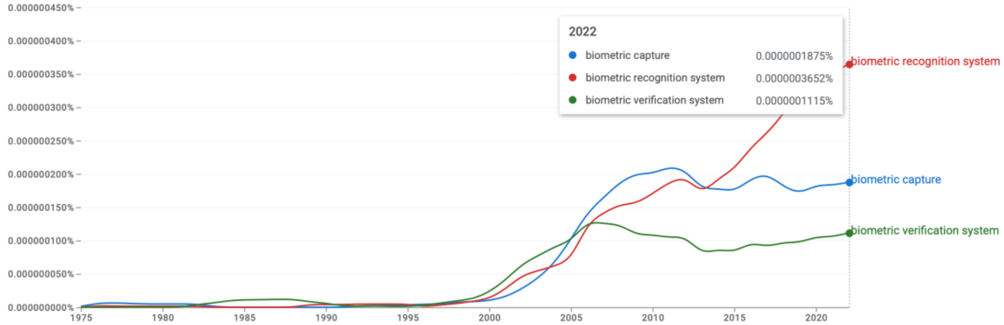


Figure 11. Occurrence of concepts: biometric capture, biometric recognition system, biometric verification system

More, the wildcard search for associations with multibiometric concept – multibiometric system(s) and multibiometric fusion – defined by the International Organization for Standardization (ISO/IEC 2382-37:2022) which revealed their appearance and increase in use after 2000 with a peak in 2009.

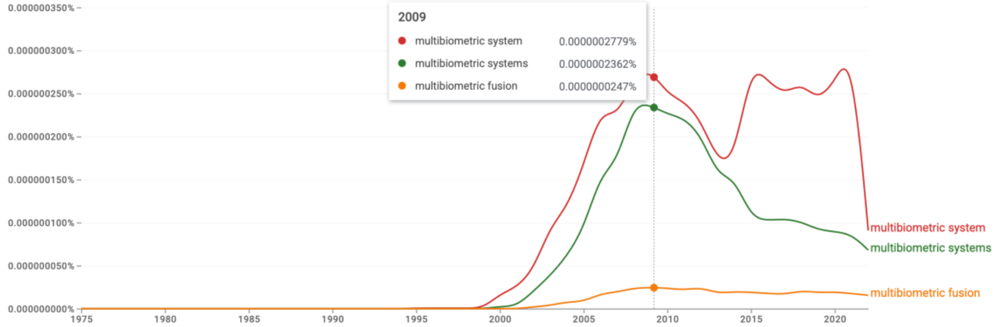


Figure 12. Wildcard search for multibiometric * concept

On the same note, the wildcard search for associations with multimodal concept traced the following: multimodal transport, multimodal approach, multimodal texts, multimodal therapy, multimodal interaction, multimodal data and multimodal analysis. The graphical representation and retrieved values shows the latest import of multimodal concept to the use of data, analysis of texts in a later stage following 2000s.

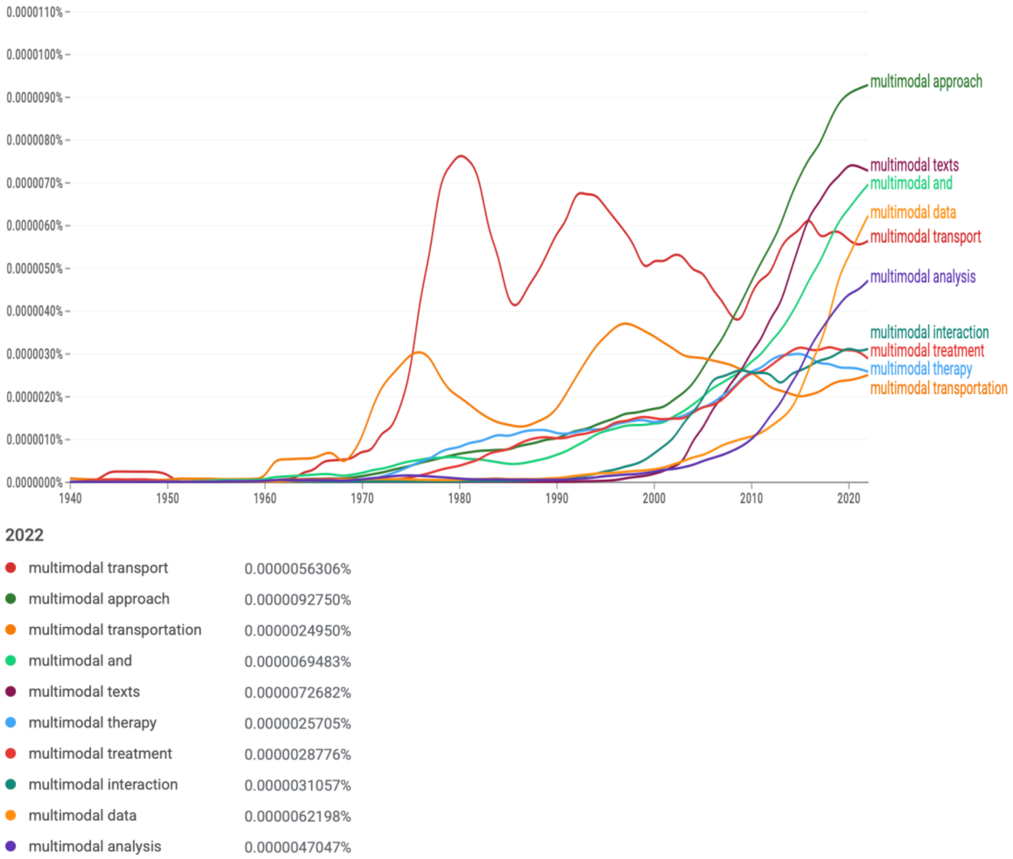


Figure 13. Wildcard search for multimodal * concept

Conclusions

This study contributes to the identification and answer to some questions in the field of research knowledge. First of all, the results identified based on the visualization of the figures highlight an ascending trend of the use of relevant topics since 1970 (Figure 3, Figure 4, Figure 5, Figure 6, Figure 7, Figure 8 and Figure 9). The study also differentiates the most important categories of topics and contributes to the identification and nomination of important sequential analysis categories for future research in the field of identity management, data access and protection, security protocols and security in various environments (Figure 1 and Figure 9). Furthermore, the study reveals new directions of personal and biometric data management, such as the field of operational security, by monitoring the constantly ascending trends of the use of key concepts, as well as the need to configure legal regulation policies, protection and risk assessment and planning of responses in case of cyber incidents.

The results have shown the wide interest in the emergence of new solutions to secure digital data and online transactions against cyber-attacks and intrusions, increasing authentication security, different options involving biometrics use in these processes and respecting privacy, personal data and sensitive information (Figures 10, 11, 12 and 13).

Authors' Contributions:

The authors contributed equally to this work.

References:

Abdullayeva, F., Imamverdiyev, Y., Musayev, V., Wayman, J. (2008, September). Analysis of security vulnerabilities in biometric systems. In *The second international conference: problems of cybernetics and informatics*.

Arora, S., & Bhatia, M. P. S. (2021). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, *31*(1), 28–48. https://doi.org/10.1080/19393555.2021.1873464

Bala, N., Gupta, R., & Kumar, A. (2021). Multimodal biometric system based on fusion techniques: a review. *Information Security Journal: A Global Perspective*, *31*(3), 289–337. https://doi.org/10.1080/19393555.2021.1974130

Bromby, M. (2010). Identification, trust and privacy: How biometrics can aid certification of digital signatures. *International Review of Law, Computers & Technology*, *24*(1), 133-141.

Choudhury, Z. H., & Rabbani, M. M. A. (2019). Biometric Passport for National Security Using Multibiometrics and Encrypted Biometric Data Encoded in the QR Code. *Journal of Applied Security Research*, *15*(2), 199–229. https://doi.org/10.1080/19361610.2019.1630226

Grünenberg, K. (2020). Wearing Someone Else's Face: Biometric Technologies, Anti-spoofing and the Fear of the Unknown. *Ethnos*, *87*(2), 223–240. https://doi.org/10.1080/00141844.2019.1705869

International Organization for Standardization (2022). ISO/IEC 2382-37:2022Information technology — Vocabulary Part 37: Biometrics) (edition 3, 2022). Reference number ISO/IEC 2382-37:2022(E), Switzerland. Retrieved from: https://cdn.standards.iteh.ai/samples/73514/84fbd32e307b4ca88b8cf1562415b8bf/ISO-IEC-2382-37-2022.pdf, accessed on March 6, 2025.

Kavitha, G., Prasannakumar, V., Pranav, R. P. (2024, July). Enhancing Digital Security: A Comprehensive Multi-Model Authentication Framework Leveraging Cryptography and Biometrics. In *2024 8th International Conference on Inventive Systems and Control (ICISC)* (pp. 476-486). IEEE.

Kleist, V. F. (2007). Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the Online Trust Silver Bullet? *Information Systems Management*, *24*(4), 319–329. https://doi.org/10.1080/10580530701586045

Laux, D., Luse, A., Mennecke, B., & Townsend, A. M. (2011). Adoption of Biometric Authentication Systems: Implications for Research and Practice in the Deployment of End-User Security Systems. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 221–245. https://doi.org/10.1080/10919392.2011.590111

Maguire, M. (2009). The birth of biometric security. *Anthropology today*, *25*(2), 9-14.

Maskey, R. (2024). Integrating Biometric Security into Digital Payment Solutions: Opportunities and Challenges. *Aitoz Multidisciplinary Review*, *3*(1), 306-312.

Meena, G., & Choudhary, S. (2019). Biometric authentication in internet of things : A conceptual view. *Journal of Statistics and Management Systems*, *22*(4), 643–652. https://doi.org/10.1080/09720510.2019.1609722

Mukkamala, S. S. K., Mahida, A., Vishwanadham Mandala, M. S. (2024). Leveraging AI And Big Data For Enhanced Security In Biometric Authentication: A Comprehensive Model For Digital Payments. *Migration Letters*, *21*(8), 574-590.

Obaidat, M. S., Traore, I., Woungang, I. (Eds.). (2019). *Biometric-based physical and cybersecurity systems* (pp. 1-10). Cham: Springer International Publishing.

Oduri, S. (2024). Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era. *International Journal of Innovative Research in Science Engineering and Technology*, *13*(7), 13632-13640.

Olimid, A.P., Rogozea, L.M., Olimid, D.A. (2018). Ethical approach to the genetic, biometric and health data protection and processing in the new EU General Data Protection Regulation (2018). *Romanian Journal of Morphology and Embryology* = Revue Roumaine de Morphologie et Embryologie. 2018 ;59(2):631-636. PMID: 30173275.

Olimid, A. P., Georgescu, C. M., Olimid, D. A. (2024a). EU Policies on Human Security, Environmental Sustainability, Strategic Foresight, and Digital Transition in EU Candidate Countries: Moldova and Ukraine. *Economics Ecology Socium*, *8*, 25-41. doi: https://doi.org/10.61954/2616-7107/2024.8.4-3

Olimid, A. P., Georgescu, C. M., Olimid, D. A. (2024b). Policy analysis of human factors and social innovation in EU EASI Programme Reports (2015-2022). *Baltic Journal of Economic Studies*, *10*(3), 1-9. https://doi.org/10.30525/2256-0742/2024-10-3-1-9. doi: 10.30525/2256-0742/2024-10-3-1-9

Patil, S., Dudhankar, V., Shukla, P. (2024). Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud. *Journal of Current Science and Research Review*, *2*(02), 69-81.

Ross, A., Banerjee, S., Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters*, *138*, 346-354.

Sett, S., Gupta, H. (2024, March). A Biometric Security Model for The Enhancement of Data Security. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-5). IEEE.

Seyal, A. H., & Turner, R. (2012). A study of executives' use of biometrics: an application of theory of planned behaviour. *Behaviour & Information Technology*, *32*(12), 1242–1256. https://doi.org/10.1080/0144929X.2012.659217

Shafik, W., Tufail, A., Apong, R. A. A. H. M., Balasubramaniam, S. (2024). Future Directions in Cybersecurity, Digital Forensics and Biometric Systems. In *AI Based Advancements in Biometrics and its Applications* (pp. 238-263). CRC Press.

Singleton, T. (2003). Biometric Security Systems: The Best Infosec Solution? *EDPACS*, *30*(9), 1–24. https://doi.org/10.1201/1079/43292.30.9.20030301/41230.1

Sriman, J., Thapar, P., Alyas, A. A., Singh, U. (2024, January). Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques. In *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 136-141). IEEE.

The World Bank (2025). Practitioner's Guide (Other References and Resources). https://id4d.worldbank.org/guide/other-references-and-resources, accessed on March 6, 2025.

van der Ploeg, I. (2003). Biometrics and Privacy A note on the politics of theorizing technology. *Information, Communication & Society*, *6*(1), 85–104. https://doi.org/10.1080/1369118032000068741

Article Info

Received: February 07 2025
Accepted: March 12 2025

How to cite this article:

Olimid, A.P., Georgescu, C.M., Olimid, D.A., Georgescu, S.D., Gherghe, C.L. (2025). Theorizing Digital Security Governance and Biometric Data Inputs based on Research Topics and Online Mentions Tracking. *Revista de Științe Politice. Revue des Sciences Politiques*, no. 85, pp. 43 – 56.