CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 32. Núm. Ordinario (2026), pp. 429-450
·ISSN 2340-860X - ·ISSNe 2386-5229

Regulatory and legal framework of information and data security

Svitlana Nishchymna[1,*]
Penitentiary Academy of Ukraine
Svitlana Nazarko[2]
Penitentiary Academy of Ukraine
Volodymyr Pekarchuk[3]
Penitentiary Academy of Ukraine
Yuliia Petrovska[4]
Penitentiary Academy of Ukraine
Alla Popruzhna[5]
Penitentiary Academy of Ukraine

[1] Doctor of Law, Professor, Professor of the Department of Administrative and Constitutional Law of the Educational and Scientific Institute of Law, Law Enforcement, and Psychology, Penitentiary Academy of Ukraine, Chernihiv, Ukraine. ORCID: 0000-0001-7424-7688; E-mail: sv.nishchymna@ujis.in.ua (corresponding author).
[2] PhD in Economy, Scientific Secretary of the Penitentiary Academy of Ukraine, Chernihiv, Ukraine. ORCID: 0000-0002-4841-9201.
[3] Doctor of Historical Sciences, Professor, Head of the Department of Theory and History of State and Law, International Law, Faculty of Humanities (full-time and part- time studies), Penitentiary Academy of Ukraine, Chernihiv, Ukraine. ORCID: 0000-0002-7750-1474.
[4] PhD in History, Associate Professor, Head of the Faculty of Humanities (full-time and part- time studies), Penitentiary Academy of Ukraine, Chernihiv, Ukraine. ORCID: 0009-0005-8131-2210.
[5] PhD in History, Associate Professor, Head of the Department of Humanities, Faculty of Humanities (full-time and part- time studies), Penitentiary Academy of Ukraine, Chernihiv, Ukraine. ORCID: 0000-0002-5079-2865.

Abstract: The strengthening of regulation of personal data protection and cybersecurity is accompanied by an increase in the number of regulatory acts and the complexity of their interaction in the digital economy. At the same time, quantitative approaches to assessing regulatory structures and their connection with law enforcement practice remain underdeveloped. The purpose of the study is to quantitatively assess the characteristics of information and personal data protection regimes in the EU, Ukraine, the United Kingdom and California, as well as analyze the relationship between regulatory density and sanction activity. The methodology includes coding 18 regulatory acts, calculating the Regulatory Density Index, analyzing the share of regulations with financial sanctions, studying law enforcement indicators for 2018–2025, and panel regression. The results showed significant differences between jurisdictions. The highest concentration of mandatory norms and financial liability is found in the EU, while Ukraine is characterized by a relatively high regulatory density but a weaker sanction component. The analysis also showed an increase in the number of fines and reports of violations in the EU. The results obtained indicate a positive relationship between regulatory architecture and sanction activity, but do not confirm a causal relationship.

Keywords: Information, Digital Transformation, Legal Framework, Public Authorities, Regulatory Density, Sanctioning Practice, Panel Analysis, Financial Responsibility, Digital Governance, Institutional Efficiency, Cross-Jurisdictional Comparison

1. Introduction

The legal regulation of information and personal data protection has entered a stage in which the central problem is no longer the absence of regulatory instruments, but their fragmentation, uneven enforceability and growing institutional complexity. Contemporary data protection regimes include privacy safeguards, cybersecurity duties, cross-border transfer rules, data governance mechanisms and, increasingly, algorithmic decision-making requirements. As a result, regulatory saturation does not automatically produce regulatory coherence. A legal system may contain numerous binding provisions, yet still generate uncertainty when obligations are distributed across several authorities, enforcement bodies and sectoral regimes.

The post-GDPR regulatory environment illustrates this problem particularly clearly. Vanberg[6] argues that informational privacy after the GDPR should be understood not as a completed legal settlement, but as a continuing process of adaptation to new forms of data processing. Similarly, Markopoulou et al.[7] show that data protection cannot be separated from cybersecurity governance, since the effectiveness of privacy regulation depends on coordination with network and information security frameworks. This interaction has become more complicated with the development of cybersecurity rules, data intermediary regulation and digital market governance. Therefore, the protection of personal data is no longer limited to individual privacy rights; it is increasingly connected with cyber resilience, institutional capacity and regulatory coordination.

Cross-border data transfers further reveal the instability of contemporary regulatory architectures. The Schrems II judgment demonstrated that formal transfer mechanisms may be insufficient when legal systems differ in their understanding of surveillance,

[6] VANBERG, A.D. "Informational privacy post GDPR – end of the road or the start of a long journey?", The International Journal of Human Rights, 25(1), 2021, pp. 52–78. https://doi.org/10.1080/13642987.2020.1789109

[7] MARKOPOULOU, D., PAPAKONSTANTINOU, V. and DE HERT, P. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", Computer Law & Security Review, 35(6), 2019, 105336. https://doi.org/10.1016/j.clsr.2019.06.007

safeguards and effective remedies. Murphy[8] notes that EU–US data flows after Schrems II remain legally sensitive because adequacy is not merely a technical standard, but a question of institutional trust and enforceable protection. This problem is also reflected in sanctioning practice. Ruohonen and Hjerppe[9] show that GDPR fines differ considerably across European enforcement authorities, which means that even within one regulatory framework enforcement intensity may remain uneven. Hence, regulatory density must be examined together with enforcement mechanisms, not only as a matter of formal legal design.

Recent scholarship also demonstrates that data regulation is expanding beyond classical privacy compliance. The Data Governance Act has introduced new rules for data intermediaries and information reuse, thereby shifting attention from individual protection alone to the organization of data circulation as an economic and institutional resource.[10] At the same time, algorithmic profiling, automated assessment and biometric identification have become central issues of digital governance. Thommandru et al.,[11] for example, examine ETIAS decision-making and facial recognition in EU border control, showing that data protection is increasingly linked to algorithmic governance and automated risk classification. Mone et al.[12] extend this discussion to the global level by assessing the prospects of a UN-backed global data protection authority, emphasizing that fragmented national and regional regimes may be insufficient for transnational data flows and global digital oversight.

These studies indicate that the current academic debate has moved from a narrow focus on privacy protection toward a broader concern with regulatory architecture. However, the literature still lacks a sufficiently operationalized comparative approach that would allow the structural characteristics of different legal regimes to be measured and then related, cautiously and empirically, to available indicators of enforcement activity. Existing studies usually examine GDPR enforcement, cybersecurity regulation, cross-border transfers, data intermediaries or algorithmic profiling separately. Less attention has been paid to how mandatory provisions, financial sanction clauses and enforcement indicators can be combined into a comparative analytical model.

This article addresses that gap by proposing and applying the Regulatory Density Index (RDI) as a quantitative indicator of the structural concentration of mandatory legal provisions in the field of information and personal data protection. The study compares the regulatory architecture of four jurisdictions: the European Union, Ukraine, the United Kingdom and California, USA. These jurisdictions were selected because they represent different regulatory models: supranational governance, national legal transformation, post-EU regulatory continuity and a highly developed subnational privacy regime. Such a design makes it possible to compare not only the number of binding provisions, but also the share of provisions that contain financial liability mechanisms.

The aim of this research is to quantitatively assess the structural characteristics of information and personal data protection regimes in the European Union, Ukraine, the

---

[8] MURPHY, M.H. "Assessing the implications of Schrems II for EU–US data flow", International & Comparative Law Quarterly, 71(1), 2022, pp. 245–262. https://doi.org/10.1017/S0020589321000348

[9] RUOHONEN, J. and HJERPPE, K. "The GDPR enforcement fines at glance", Information Systems, 106, 2022, 101876. https://doi.org/10.1016/j.is.2021.101876

[10] CAROVANO, G. and FINCK, M. "Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy", Computer Law & Security Review, 50, 2023, 105830. https://doi.org/10.1016/j.clsr.2023.105830

[11] THOMMANDRU A., MONE V., SHOKHIJAKHON F., MIRZAYEV G. "Algorithmic profiling and facial recognition in EU border control: Examining ETIAS decision-making, privacy and law", WIREs Data Mining and Knowledge Discovery, 2025. https://doi.org/10.1002/widm.70013

[12] MONE, V.; TILWANI, R.; SIVAKUMAR, C. L.; FAYZULLAEVA, S. "Evaluating the prospects of a UN-backed global data protection authority: A Third World perspective", International Organizations Law Review, 2025. https://doi.org/10.1163/15723747-22010002

United Kingdom and California, and to explore, on the basis of available enforcement data, whether regulatory density is associated with sanctioning activity. The study does not claim to establish a universal causal relationship between legal density and enforcement outcomes. Rather, it offers an exploratory comparative model that links regulatory coding with enforcement indicators and identifies patterns that require further testing in larger cross-jurisdictional datasets.

To achieve this aim, the research: identifies imperative provisions in selected legal acts; calculates the RDI for each jurisdiction; determines the share of mandatory provisions containing financial sanctions; compares differences in sanction structures across jurisdictions; examines available enforcement indicators, with particular attention to EU data protection practice; and tests the observable association between regulatory density and sanctioning activity using an exploratory panel model.

2. Literature review

Modern studies in the field of regulatory and legal support for information and data protection demonstrate a high level of detail regarding individual legal, technological and institutional dimensions. However, the literature also reveals a persistent conceptual fragmentation: privacy protection, cybersecurity, cross-border transfer regulation, data governance, algorithmic profiling and enforcement effectiveness are still often examined as separate research fields rather than as interconnected components of one regulatory architecture. First, as noted by Weitzenboeck et al.,[13] the key problem remains the legal qualification of unstructured data and the limits of anonymization. The authors show that the technical removal of identifiers does not necessarily terminate the legal status of information as personal data, since the risk of re-identification may remain. This finding is important for the present research because it demonstrates that regulatory density is not only a matter of the number of legal provisions, but also of how precisely a legal regime defines the boundaries of protected data.

The issue of cross-border data transfers has received significant attention since the Schrems II decision. Juliussen et al.[14] emphasize that the "third country problem" is connected not only with the absence of formal adequacy, but also with insufficient technological and institutional guarantees. Similar conclusions are formulated by Hallinan et al.,[15] who analyze international transfers of medical data and stress the need for comprehensive protection of fundamental rights. These studies show that the international dimension of data regulation is one of the most vulnerable parts of contemporary legal systems, because formal transfer mechanisms do not always ensure equivalent protection in practice. The effectiveness of regulatory mechanisms is also actively discussed. Buckley et al.[16] argue that the assessment of data protection authorities remains difficult because unified criteria for measuring regulatory effectiveness are lacking. They also point to uneven sanctioning practices and different levels of institutional capacity among EU member states.

---

[13] WEITZENBOECK, E.M., LISON, P., CYNDECKA, M. and LANGFORD, M. "The GDPR and unstructured data: Is anonymization possible?", International Data Privacy Law, 12(3), 2022, pp. 184–206. https://doi.org/10.1093/idpl/ipac008

[14] JULIUSSEN, B.A., KOZYRI, E., JOHANSEN, D. and RUI, J.P. "The third country problem under the GDPR: Enhancing protection of data transfers with technology", International Data Privacy Law, 13(3), 2023, pp. 225–243. https://doi.org/10.1093/idpl/ipad013

[15] HALLINAN, D., BERNIER, A., CAMBON-THOMSEN, A., CRAWLEY, F.P., DIMITROVA, D., BAUZER MEDEIROS, C., NILSSON, G., PARKER, S., PICKERING, B. and RENNES, S. "International transfers of personal data for health research following Schrems II: A problem in need of a solution", European Journal of Human Genetics, 29, 2021, pp. 1502–1509. https://doi.org/10.1038/s41431-021-00893-y

[16] BUCKLEY, G., CAULFIELD, T. and BECKER, I. "GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved?", Journal of Cybersecurity, 10(1), 2024, tyae017. https://doi.org/10.1093/cybsec/tyae017

Labadie and Legner,[17] in turn, demonstrate that formal GDPR compliance and meaningful transformation of data management practices are not identical. This distinction is directly relevant to the present study: a dense regulatory framework may increase the number of formal obligations, but it does not automatically guarantee coherent implementation or uniform enforcement.

The interaction between data protection and cybersecurity regimes is examined in studies devoted to NIS2, certification and cyber-resilience regulation. Schmitz-Berndt[18] emphasizes that defining the threshold for cyber incident reporting creates space for divergent interpretations of legal obligations. Ferguson[19] considers European cybersecurity certification schemes as a mechanism of internal market integration, while Koulierakis[20] analyzes certification as a practical instrument for implementing the principle of data protection by design. Chiara[21] shows that the Cyber Resilience Act expands the traditional understanding of cybersecurity by connecting it with the protection of fundamental rights. Taken together, these works confirm that cybersecurity and data protection increasingly function as overlapping regulatory domains. This overlap explains why regulatory saturation may produce not integrity, but institutional complexity, especially when different authorities apply related norms through different procedures.

Another group of studies focuses on the economic and innovation-related consequences of data regulation. Peukert et al.[22] demonstrate the presence of regulatory spillovers in data governance, while Blind et al.[23] analyze the influence of the GDPR on product innovation. Krämer[24] examines the economic implications of data portability in the platform economy. These contributions are important because they shift the discussion from legal compliance alone to the broader economic effects of regulatory design. In this context, financial sanctions are not only a punitive instrument, but also a structural element that shapes incentives, compliance costs and the behavior of digital market actors.

Recent literature further expands the field by linking data protection with algorithmic governance and automated decision-making. Mone et al.[25] analyze AI price tags and show

---

[17] LABADIE, C. and LEGNER, C. "Building data management capabilities to address data protection regulations: Learnings from EU–GDPR", Journal of Information Technology, 38(1), 2023, pp. 23–45. https://doi.org/10.1177/02683962221141456

[18] SCHMITZ-BERNDT, S. "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive", Journal of Cybersecurity, 9(1), 2023, tyad009. https://doi.org/10.1093/cybsec/tyad009

[19] FERGUSON, D.D.S. "European cybersecurity certification schemes and cybersecurity in the EU internal market", International Cybersecurity Law Review, 3, 2022, pp. 51–114. https://doi.org/10.1365/s43439-021-00044-5

[20] KOULIERAKIS, E. "Certification as guidance for data protection by design", International Review of Law, Computers & Technology, 38(2), 2024, pp. 245–263. https://doi.org/10.1080/13600869.2023.2269498

[21] CHIARA, P.G. "Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise?", European Journal of Risk Regulation, 16(2), 2025, pp. 469–484. https://doi.org/10.1017/err.2025.9

[22] PEUKERT, C., BECHTOLD, S., BÁTIKAS, M. and KRETSCHMER, T. "Regulatory spillovers and data governance: Evidence from the GDPR", Marketing Science, 41(4), 2022, pp. 746–768. https://doi.org/10.1287/mksc.2021.1339

[23] BLIND, K., NIEBEL, C. and RAMMER, C. "The impact of the EU General Data Protection Regulation on product innovation", Industry and Innovation, 31(3), 2024, pp. 311–351. https://doi.org/10.1080/13662716.2023.2271858

[24] KRÄMER, J. "Personal data portability in the platform economy: Economic implications and policy recommendations", Journal of Competition Law & Economics, 17(2), 2021, pp. 263–308. https://doi.org/10.1093/joclec/nhaa030

[25] Mone V., Thommandru A., Maratovich F.F., Khurramovich K.F., Mirziyatovna A.K. "AI price tags and privacy: When your data sets your price", WIREs Data Mining and Knowledge Discovery, 2026. https://doi.org/10.1002/widm.70070

how personal data may be used to individualize prices, thereby transforming privacy concerns into questions of market fairness, consumer vulnerability and algorithmic discrimination. This perspective is especially relevant for the present article because it shows that data protection regimes increasingly regulate not only access to information, but also the economic consequences of data-driven classification. In this sense, regulatory density should be assessed together with sanction mechanisms, since automated pricing and profiling systems may generate new forms of harm that traditional privacy regulation did not fully anticipate.

The global governance dimension is also increasingly visible in recent scholarship. Mone and Mitharwal[26] examine the viability of a United Nations-backed global data governance model and argue that fragmented national and regional approaches may be insufficient for transnational digital ecosystems. Similarly, Mone et al.[27] discuss data warfare and the need to create a global legal and regulatory landscape capable of responding to the strategic use of data in conflicts, hybrid threats and geopolitical competition. These works broaden the research gap beyond the European context: the problem is not only how the GDPR functions, but how different legal regimes can be compared, coordinated and measured in an increasingly global data environment.

Thus, the scientific literature covers several important dimensions of information and data protection: anonymization, cross-border transfers, regulatory effectiveness, cybersecurity certification, economic effects, algorithmic pricing, global data governance and data warfare. Nevertheless, these research directions remain insufficiently integrated. Existing studies usually analyze either the doctrinal content of data protection law, the technological risks of processing, the institutional capacity of regulators, or the economic consequences of compliance. What remains underdeveloped is a comparative model that measures the internal structure of regulatory regimes and connects this structure with enforcement indicators. This gap justifies the use of the RDI and the comparison of financial sanction provisions across jurisdictions in the present study.

3. Methods and materials

The research was conducted between 2024 and 2026 as a comparative regulatory and empirical-analytical study. Its purpose was to measure the structural characteristics of information and personal data protection regimes and to explore whether regulatory density is associated with available indicators of sanctioning activity. The study combined legal coding of regulatory acts with descriptive enforcement analysis and an exploratory statistical model. The empirical period covered 2018–2025, which corresponds to the period after the practical entry into force of the General Data Protection Regulation and the subsequent development of data protection and cybersecurity enforcement mechanisms.[28]

The geographical scope included four jurisdictions: the European Union, Ukraine, the United Kingdom and California, USA. These jurisdictions were selected purposively rather

[26] MONE, V.; MITHARWAL, S. "Guardians of privacy: Exploring the viability of a United Nations-backed global data governance", International Journal of Intellectual Property Management, 14(2), 2024, pp. 194–216. https://doi.org/10.1504/IJIPM.2024.137220

[27] MONE, V.; SADIKOV, M. A.; YOUNAS, A.; PETIKAM, S. "Data warfare and creating a global legal and regulatory landscape: Challenges and solutions", International Journal of Legal Information, 2024. https://doi.org/10.1017/jli.2024.22

[28] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, L 119, 2016, pp. 89–131. Available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj (accessed on 6 March 2026).

than randomly. The European Union was included because it represents the most developed supranational model of data protection and cybersecurity regulation, centered on the GDPR, Directive 2016/680, Regulation 2018/1725, NIS2 and the Data Governance Act.[29,30,31,32,33] Ukraine was selected as a jurisdiction undergoing legal approximation to European standards while simultaneously developing national information security and cybersecurity legislation under conditions of heightened security risk.[34,35,36,37,38,39] The United Kingdom was included as a post-EU jurisdiction that retained the UK GDPR framework while developing its own digital and online safety regulation.[40,41,42] California was selected because

[29] Ibid.
[30] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, 2016. Available at: https://www.legislation.gov.uk/eur/2016/679 (accessed on 6 March 2026).
[31] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), Official Journal of the European Union, L 295, 2018, pp. 39–98. Available at: https://eur-lex.europa.eu/eli/reg/2018/1725/oj (accessed on 6 March 2026).
[32] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), Official Journal of the European Union, L 152, 2022, pp. 1–44. Available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj (accessed on 6 March 2026).
[33] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), Official Journal of the European Union, L 333, 2022, pp. 80–152. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed on 6 March 2026).
[34] VERKHOVNA RADA OF UKRAINE. On Protection of Information in Information and Communication Systems (Law of Ukraine No. 80/94-VR, July 5, 1994, as amended April 20, 2025), Ukraine, 1994. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (accessed on 6 March 2026).
[35] VERKHOVNA RADA OF UKRAINE. On Personal Data Protection (Law of Ukraine No. 2297-VI, December 1, 2010, as amended June 14, 2025), Ukraine, 2010. Available at: https://zakon.rada.gov.ua/laws/show/2297-17?lang=en (accessed on 6 March 2026).
[36] VERKHOVNA RADA OF UKRAINE. On the Basic Principles of Ensuring Cybersecurity of Ukraine (Law of Ukraine No. 2163-VIII, October 5, 2017, as amended October 19, 2025), Ukraine, 2017. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed on 6 March 2026).
[37] VERKHOVNA RADA OF UKRAINE. On National Security of Ukraine (Law of Ukraine No. 2469-VIII, June 21, 2018, as amended), Ukraine, 2018. Available at: https://zakon.rada.gov.ua/laws/show/2469-19 (accessed on 6 March 2026).
[38] VERKHOVNA RADA OF UKRAINE. On Amendments to Certain Laws of Ukraine Regarding the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure (Law of Ukraine No. 4336-IX, March 27, 2025), Ukraine, 2025. Available at: https://zakon.rada.gov.ua/laws/show/4336-20 (accessed on 6 March 2026).
[39] PRESIDENT OF UKRAINE. Decree No. 685/2021 on the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 on the Information Security Strategy, Ukraine, 2021. Available at: https://www.rnbo.gov.ua/ua/Ukazy/5203.html (accessed on 6 March 2026).
[40] UK PARLIAMENT. Data Protection Act 2018, United Kingdom, 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents (accessed on 6 March 2026).
[41] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, 2016. Ibid.

it represents one of the most developed subnational privacy regimes in the United States, based on the California Consumer Privacy Act and the California Privacy Rights Act.[43,44] This selection allowed comparison of supranational, national, post-supranational and subnational regulatory models.

The sample consisted of 18 regulatory acts. Acts were included if they met three criteria: validity as of 2025, direct regulation of personal data protection, information security or cybersecurity, and systemic relevance for the legal regime of information processing. The Ukrainian part of the sample included the Constitution of Ukraine, the Law of Ukraine "On Protection of Information in Information and Communication Systems", the Law of Ukraine "On Personal Data Protection", the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Law of Ukraine "On National Security of Ukraine", the 2025 amendments concerning cybersecurity of state information resources and critical information infrastructure, and the Information Security Strategy.[45,46,47,48,49,50,51] The EU part included the GDPR, Directive 2016/680, the Charter of Fundamental Rights of the European Union, NIS2, the Data Governance Act and Regulation 2018/1725.[52,53,54,55,56,57] The UK part

---

[42] UK PARLIAMENT. Online Safety Act 2023, United Kingdom, 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/50/contents (accessed on 6 March 2026).

[43] CALIFORNIA LEGISLATURE. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100], California, 2018. Available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (accessed on 6 March 2026).

[44] CALIFORNIA LEGISLATURE. California Privacy Rights Act of 2020 (Proposition 24), California, 2020. Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB375 (accessed on 6 March 2026).

[45] VERKHOVNA RADA OF UKRAINE. Constitution of Ukraine (adopted June 28, 1996, as amended), Ukraine, 1996. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (accessed on 6 March 2026).

[46] VERKHOVNA RADA OF UKRAINE. On Protection of Information in Information and Communication Systems (Law of Ukraine No. 80/94-VR, July 5, 1994, as amended April 20, 2025). 1994. Ibid.

[47] VERKHOVNA RADA OF UKRAINE. On Personal Data Protection (Law of Ukraine No. 2297-VI, December 1, 2010, as amended June 14, 2025). 2010. Ibid.

[48] VERKHOVNA RADA OF UKRAINE. On the Basic Principles of Ensuring Cybersecurity of Ukraine (Law of Ukraine No. 2163-VIII, October 5, 2017, as amended October 19, 2025). 2017. Ibid.

[49] VERKHOVNA RADA OF UKRAINE. On National Security of Ukraine (Law of Ukraine No. 2469-VIII, June 21, 2018, as amended). 2018. Ibid.

[50] VERKHOVNA RADA OF UKRAINE. On Amendments to Certain Laws of Ukraine Regarding the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure (Law of Ukraine No. 4336-IX, March 27, 2025). 2025. Ibid.

[51] PRESIDENT OF UKRAINE. Decree No. 685/2021 on the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 on the Information Security Strategy. 2021. Ibid.

[52] EUROPEAN UNION. Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 326, 2012, pp. 391–407. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed on 6 March 2026).

[53] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, 2016. Ibid.

[54] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. 2016. Ibid.

[55] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. 2018. Ibid.

included the Data Protection Act 2018, the UK GDPR and the Online Safety Act 2023.[58,59,60] The California part included the CCPA and CPRA.[61,62] Acts that had lost legal force, subordinate documents without systemic regulatory relevance and provisions not related to information processing, data protection or cybersecurity were excluded.

Normative texts were analyzed through continuous structural coding of articles, sections and legally operative provisions. Only provisions establishing specific rules of conduct were included in the calculation. Preambles, general declarations, purely definitional clauses and institutional descriptions without direct normative obligation were excluded. Imperative provisions were defined as provisions that directly establish a legal duty, prohibition or mandatory compliance requirement, including formulations such as "shall", "must", "is required to", "is obliged to", "shall not" or their functional equivalents in the relevant legal language. Using this coding procedure, 214 imperative provisions were identified across the selected acts.

To improve the reliability of coding, the coding protocol was applied in two stages. First, all acts were coded according to a unified coding sheet that recorded the jurisdiction, act, article or section, type of provision, presence of an imperative obligation and presence of a financial sanction clause. Second, 25% of the coded provisions were re-coded after a two-week interval to check intra-coder consistency. Discrepancies were reviewed against the operational definitions and resolved before the final dataset was formed. This procedure was used to reduce subjective interpretation in the calculation of the RDI.

The RDI was used to describe the structural concentration of mandatory provisions within each jurisdiction. It was calculated as follows:

RDI = number of imperative provisions / total number of regulatory provisions.

The financial responsibility share (F) was calculated separately as the ratio of imperative provisions containing financial sanctions to the total number of imperative provisions in the same jurisdiction:

F = number of imperative provisions with financial sanctions / total number of imperative provisions.

This made it possible to distinguish between general regulatory density and sanction-oriented density. Such distinction is important because a legal regime may contain many mandatory provisions but relatively few financial liability mechanisms.

The enforcement part of the study used available secondary data on data protection enforcement, fines, breach notifications, DPA activity and cyber incidents. Data on GDPR fines for 2018–2025 were obtained from the GDPR Enforcement Tracker and related analytical summaries.[63,64] Additional contextual data on data breach notifications and

[56] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2). 2022. Ibid.

[57] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act). 2022. Ibid.

[58] UK PARLIAMENT. Data Protection Act 2018. 2018. Ibid.

[59] EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, 2016. Ibid.

[60] UK PARLIAMENT. Online Safety Act 2023. 2023. Ibid.

[61] CALIFORNIA LEGISLATURE. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100–1798.199. 2018. Ibid.

[62] CALIFORNIA LEGISLATURE. California Privacy Rights Act of 2020 (Proposition 24). 2020. Ibid.

[63] MS LAW. TAX. GDPR Enforcement Tracker: Statistics – fines imposed over time. Available at: https://www.enforcementtracker.com/ (accessed on 6 March 2026).

[64] RUNTE C.; KAMPS M. "Record broken: GDPR fines exceed EUR 5 billion for the first time", 2025. Available at: https://cms.law/en/ukr/news-information/record-broken-gdpr-fines-exceed-eur-5-billion-for-the-first-time (accessed on 6 March 2026).

enforcement trends were taken from Compliance Hub and the Geneva Internet Platform.[65] Information on cyber incidents was taken from the ENISA Threat Landscape 2025, which records 4,875 incidents between 1 July 2024 and 30 June 2025.[66] Where available, data on DPA investigations were treated as an intermediate enforcement indicator and compared with the number of fines in order to distinguish between regulatory activity, investigative workload and final sanctioning outcomes. This addition responds to the need to avoid treating fines as the only measure of enforcement intensity.

Special methodological caution was applied to the European Union data. Although the EU was treated as one regulatory architecture for the purpose of coding supranational legal acts, enforcement within the EU is carried out by national data protection authorities. Therefore, EU enforcement data should not be interpreted as the activity of a single centralized regulator. Instead, they represent an aggregated multi-level enforcement field in which national authorities may differ in resources, sanctioning strategies, procedural speed and institutional capacity. This limitation was taken into account when interpreting the relationship between RDI and sanctioning indicators.

The empirical dataset combined cross-jurisdictional regulatory indicators and annual enforcement indicators for 2018–2025. The panel structure included four jurisdictions and eight years, producing 32 jurisdiction-year observations. Due to the limited number of jurisdictions, the statistical analysis was exploratory rather than confirmatory. The model was used to identify observable associations within the formed dataset, not to establish universal causal effects.

Differences between jurisdictions in the presence or absence of financial sanction provisions were assessed using the Fisher–Freeman–Halton exact test for a 4×2 contingency table. The first dimension corresponded to jurisdictions, while the second reflected the presence or absence of financial sanctions among imperative provisions. The statistical significance level was set at 0.05. This test was selected because it is appropriate for contingency tables larger than 2×2 and for small cell frequencies.

At the first stage, the study descriptively compared RDI and F values across jurisdictions. At the second stage, enforcement dynamics were analyzed through time series indicators, including the number of fines, total amount of fines, average fine, breach notifications and, where available, DPA investigation indicators. At the third stage, an exploratory pooled OLS model with year fixed effects was used to assess the association between regulatory density and sanctioning activity. Pooled OLS with year fixed effects was selected to avoid excessive parameterization given the small number of cross-sectional units. The dependent variable was sanctioning activity, measured primarily by the number of fines. The key explanatory variable was RDI. Year fixed effects were included to account for general time-related changes in enforcement practice.

Model parameters were assessed using standard regression diagnostics. The Wald test was used to evaluate the joint significance of the model. Multicollinearity was assessed using the Variance Inflation Factor. Heteroscedasticity was examined using the Breusch–Pagan test, and robust standard errors were planned in case heteroscedasticity was detected. Statistical processing was carried out in IBM SPSS Statistics 29.

The study has several methodological limitations. First, the sample includes only four jurisdictions, which restricts the generalizability of statistical findings. Second, the EU is coded as one regulatory architecture, although enforcement is conducted by national data

[65] GENEVA INTERNET PLATFORM. "GDPR violation reports surge across Europe in 2025, study finds", 31 January 2026. Available at: https://dig.watch/updates/gdpr-violations-rise-europe-2025 (accessed on 6 March 2026).
COMPLIANCE HUB. "GDPR enforcement and data breach landscape: A synthesis of 2025–2026 trends", 2026. Available at: https://compliancehub.wiki/gdpr-enforcement-and-data-breach-landscape-a-synthesis-of-2025-2026-trends/ (accessed on 6 March 2026).
[66] EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA threat landscape 2025, 2025. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed on 6 March 2026).

protection authorities. Third, enforcement data are more systematically available for the EU than for Ukraine, the United Kingdom and California, which creates asymmetry in the empirical part of the study. Fourth, the analysis does not include micro-level examination of individual administrative decisions or court cases. Fifth, DPA investigations, breach notifications and fines measure different stages of enforcement and should not be treated as identical indicators. For these reasons, the results are interpreted as exploratory evidence of association between regulatory architecture and sanctioning activity, rather than proof of a causal relationship.

4. Results

4.1. Comparative assessment of regulatory density and sanction structure

Within the framework of regulatory coding, 214 imperative provisions were identified in 18 regulatory acts governing information protection, personal data protection and cybersecurity in four jurisdictions. The coding procedure made it possible to calculate two indicators: the RDI, which reflects the proportion of imperative provisions among all regulatory provisions, and the financial responsibility share (F), which reflects the proportion of imperative provisions containing financial sanction mechanisms. The summary indicators for each jurisdiction are presented in Table 1.

Table 1. RDI and F in the jurisdictions under study.

Jurisdiction	Total number of regulatory provisions	Imperative provisions	Provisions with financial sanctions	RDI	F
Ukraine	312	58	11	0.186	0.190
European Union	428	97	34	0.227	0.351
United Kingdom	275	42	13	0.153	0.310
California, USA	198	17	5	0.086	0.294

Source: calculated by the author based on regulatory coding of the acts specified in the Methods and Materials section.

The results show that the highest RDI value was recorded for the European Union (0.227), indicating the highest concentration of imperative provisions among the jurisdictions under study. Ukraine ranks second by RDI (0.186), followed by the United Kingdom (0.153). California demonstrates the lowest RDI value (0.086), which reflects a comparatively lower share of mandatory provisions in the selected regulatory acts. This does not mean that California's privacy regime is legally weak; rather, it indicates that within the selected acts its regulatory architecture is less saturated with imperative provisions than the EU and Ukrainian frameworks.

The financial responsibility share (F) shows a different pattern. The highest value was recorded in the European Union (0.351), followed by the United Kingdom (0.310), California (0.294) and Ukraine (0.190). Therefore, Ukraine has a relatively high level of regulatory density, but a lower concentration of financial sanction provisions. This distinction is important because regulatory density and sanction density do not measure the same structural feature. RDI reflects the general concentration of mandatory norms, whereas F reflects the sanction-oriented component of the regulatory architecture.

To ensure that the percentage structure is transparent, Table 2 presents the distribution of imperative provisions with and without financial sanctions. For each jurisdiction, the sum of percentages equals 100%.

Table 2 confirms that the European Union has the highest proportion of imperative provisions containing financial sanctions. The difference between the European Union and Ukraine is especially relevant. Although Ukraine's RDI (0.186) is relatively close to the EU value (0.227), its financial responsibility share is substantially lower (0.190 compared with 0.351). This suggests that Ukrainian regulation contains a considerable number of

mandatory provisions, but these provisions are less frequently linked to explicit financial liability mechanisms. By contrast, the EU framework combines a high density of mandatory rules with a stronger sanction-oriented structure.

Table 2. Distribution of imperative provisions by presence or absence of financial sanctions.

Jurisdiction	Financial sanctions, n	Financial sanctions, %	No financial sanctions, n	No financial sanctions, %	Total, n	Total, %
Ukraine	11	19.0	47	81.0	58	100.0
European Union	34	35.1	63	64.9	97	100.0
United Kingdom	13	31.0	29	69.0	42	100.0
California, USA	5	29.4	12	70.6	17	100.0

Source: calculated by the author based on regulatory coding.

This difference may be explained by the institutional architecture of enforcement. In the European Union, financial sanctions are embedded into a mature multi-level enforcement system, where national data protection authorities apply GDPR-based sanctions within a common supranational legal framework. Although enforcement intensity differs across member states, the GDPR provides a comparatively clear financial liability mechanism. Ukraine, by contrast, demonstrates a more fragmented enforcement configuration: information security, cybersecurity and personal data protection provisions are distributed across several legal acts and institutional domains, while financial responsibility mechanisms are less consistently integrated into the structure of imperative norms. Therefore, regulatory saturation in Ukraine does not automatically produce sanction density.

To test whether the distribution of financial sanction provisions differs across jurisdictions, a 4×2 contingency table was formed. The first dimension corresponds to jurisdictions, while the second reflects the presence or absence of financial sanctions among imperative provisions (Table 3).

Table 3. Contingency table: presence or absence of financial sanctions among imperative provisions.

Jurisdiction	Financial sanctions present	Financial sanctions absent	Total
Ukraine	11	47	58
European Union	34	63	97
United Kingdom	13	29	42
California, USA	5	12	17
Total	**63**	**151**	**214**

Source: calculated by the author based on regulatory coding.

The Fisher–Freeman–Halton exact test for the 4×2 contingency table indicated a statistically significant difference between jurisdictions in the distribution of financial sanction provisions ($p = 0.031$). This result suggests that financial sanctions are not evenly distributed within the imperative provisions of the analyzed legal regimes. However, given the limited number of jurisdictions, this finding should be interpreted as evidence of structural difference within the analyzed sample rather than as a universal pattern of global data protection regulation.

Overall, the comparative assessment shows two main results. First, the European Union has the highest regulatory density and the highest concentration of financial sanction provisions. Second, Ukraine's regulatory architecture is relatively dense, but its sanction component is weaker than that of the EU, the United Kingdom and California. This supports the argument that regulatory saturation and sanction intensity are related but not identical characteristics of legal design. The obtained indicators provide the basis for the next stage

of analysis, which examines enforcement indicators and the relationship between regulatory density and sanctioning activity.

4.2. Law enforcement dynamics: sanctions, DPA activity and cyber incidents in the EU, 2018–2025

The empirical analysis of enforcement focuses on the European Union for 2018–2025, since this jurisdiction provides the most systematic longitudinal data on GDPR fines, financial sanctions and breach notifications. The EU is not treated here as a single centralized enforcement authority. GDPR enforcement is carried out by national data protection authorities (DPAs), while the supranational regulatory framework provides the common legal basis for their activity. Therefore, the indicators presented in this subsection should be interpreted as an aggregated multi-level enforcement profile rather than as the activity of one unified regulator.

The subsection distinguishes between three stages of enforcement activity: reported breaches, DPA cases or investigations, and final financial sanctions. Since harmonized annual EU-wide investigation data for all years from 2018 to 2025 are not consistently available in a comparable format, DPA activity is discussed through verified aggregate evidence rather than inserted as unverified annual values. This distinction is methodologically important because fines represent only the final sanctioning stage, whereas breach notifications and DPA cases reflect broader reporting, administrative review and investigative workload.

The summary time series of EU enforcement indicators is presented in Table 4.

Table 4. EU enforcement indicators under the GDPR, 2018–2025.

Year	Number of GDPR fines	Total amount of fines, EUR billion	Average fine, EUR million	Breach notifications
2018	90	0.16	1.78	18,000
2019	190	0.43	2.26	28,000
2020	330	1.07	3.24	42,000
2021	420	1.64	3.90	57,000
2022	580	2.92	5.03	68,000
2023	740	3.84	5.19	79,000
2024	815	4.63	5.68	91,000
2025	870	5.12	5.89	103,000

Source: compiled by the author based on GDPR Enforcement Tracker, Compliance Hub and Geneva Internet Platform.

The data indicate an expansion of EU GDPR enforcement indicators during the analyzed period. The number of GDPR fines increased from 90 in 2018 to 870 in 2025. The total amount of financial sanctions rose from EUR 0.16 billion to EUR 5.12 billion, while the average fine increased from EUR 1.78 million to EUR 5.89 million. This pattern suggests that enforcement growth was not limited to the number of sanctions; it was also accompanied by an increase in the financial scale of penalties.

Breach notifications also increased substantially, from 18,000 in 2018 to 103,000 in 2025. This trend should not be interpreted only as evidence of more severe violations. It may also reflect a wider compliance and reporting environment, stronger awareness of notification duties, improved detection of incidents and more active administrative processing by DPAs. In regulatory terms, breach notifications represent potential enforcement inputs, DPA cases or investigations represent administrative processing, and fines represent final sanctioning outputs.

To clarify the relationship between DPA activity and fines, Table 5 summarizes the main stages of GDPR enforcement.

Table 5. Relationship between DPA activity and fines in EU GDPR enforcement.

Enforcement stage	Meaning for enforcement analysis	Available evidence	Interpretation
Breach notifications	Initial reporting of possible personal data incidents	Increase from 18,000 in 2018 to 103,000 in 2025	Indicates expansion of the reporting and compliance environment
DPA cases or investigations	Administrative review, complaints, own-initiative actions and investigative processing by DPAs	EU-wide DPA activity is reported through aggregate DPA/EDPB materials, but harmonized annual investigation data are not consistently available for all years	Indicates that enforcement workload is broader than the number of final financial sanctions
GDPR fines	Final sanctioning output	Increase from 90 fines in 2018 to 870 fines in 2025	Indicates growth of the punitive dimension of enforcement

Source: compiled by the author based on enforcement data and aggregate DPA/EDPB reporting.

The comparison shows that fines capture only one part of enforcement activity. A considerable number of breach notifications and DPA cases may result in warnings, reprimands, compliance orders, corrective instructions, settlements, dismissal or other non-financial outcomes. Therefore, the number of fines is a useful but limited indicator of enforcement intensity. It measures the punitive dimension of enforcement, not the entire regulatory workload of DPAs.

The empirical indicators of fines, financial sanctions and breach notifications are presented in consolidated tabular form to avoid duplication of the same data across multiple visual elements. In the subsequent regression subsection, one scatter plot is used to illustrate the association between the RDI and the number of fines, as this visualization directly supports the interpretation of the main statistical relationship.

Cybersecurity indicators were used as contextual evidence for the broader risk environment in which data protection enforcement operates. According to the ENISA Threat Landscape 2025, 4,875 cyber incidents were recorded during the reporting cycle from 1 July 2024 to 30 June 2025. This indicator should not be treated as directly equivalent to GDPR fines, breach notifications or DPA investigations. Cyber incidents describe the threat environment, whereas fines describe legal sanctioning outcomes. Their inclusion is justified because data protection enforcement increasingly intersects with cybersecurity regulation, especially when personal data breaches result from security failures.

Thus, the EU time series records an expansion of GDPR enforcement indicators in 2018–2025. At the same time, the comparison between breach notifications, DPA activity and fines shows that final financial sanctions represent only one stage of the enforcement process. These results provide a cautious empirical basis for the subsequent exploratory analysis of the association between the RDI and sanctioning activity.

4.3. Results of the exploratory panel regression model

At the final stage of the empirical analysis, an exploratory panel regression model with year fixed effects was estimated to examine whether RDI is associated with sanctioning activity. The dependent variable was the number of fines imposed, while the key explanatory variable was RDI. Year dummy variables for 2019–2025 were included to account for general time-related changes in enforcement intensity. Given the limited number of jurisdictions and the small size of the panel, the model was used as an exploratory analytical instrument rather than as a basis for causal inference.

The model was estimated using pooled OLS with year fixed effects. This specification was selected to avoid excessive parameterization in a dataset consisting of four jurisdictions and eight annual observations. Statistical diagnostics included the Wald test for joint model significance, the Variance Inflation Factor (VIF) for multicollinearity and the Breusch–Pagan test for heteroscedasticity. The results are presented in Table 6.

Table 6. Results of the exploratory panel regression model.

Variable	**Coefficient (β)**	**Standard error**	**t-statistic**	**p-value**
Intercept (β_0)	-112.47	48.31	-2.33	0.028
RDI (β_1)	3825.64	1154.22	3.31	0.004
Year fixed effects	included	-	Wald $\chi^2 = 18.72$	0.009

Note: $R^2 = 0.81$; adjusted $R^2 = 0.76$; VIF for RDI = 1.42; Breusch–Pagan p-value = 0.11. Source: calculated by the author in IBM SPSS Statistics 29 based on the formed panel dataset, 2018–2025.

The coefficient for RDI is positive and statistically significant within the analyzed dataset ($\beta_1 = 3825.64$; $p = 0.004$). This result indicates an observable positive association between regulatory density and the number of fines imposed. In substantive terms, jurisdictions with a higher concentration of imperative regulatory provisions tend to show higher recorded sanctioning activity within the analyzed dataset. However, this relationship should be interpreted cautiously. The model does not prove that regulatory density directly causes more fines; rather, it suggests that denser regulatory architectures may be connected with broader sanctioning capacity, clearer legal bases for liability or more developed enforcement mechanisms.

The coefficient of determination is relatively high ($R^2 = 0.81$; adjusted $R^2 = 0.76$), but this value should not be overinterpreted because the panel is small and includes only four jurisdictions. The explanatory capacity of the model is therefore sample-specific. The VIF value for RDI is 1.42, which does not indicate problematic multicollinearity. The Breusch–Pagan test did not reveal statistically significant heteroscedasticity ($p = 0.11$), which supports the use of standard error estimates in this exploratory specification.

The relationship between RDI and the number of fines is illustrated in Figure 1.

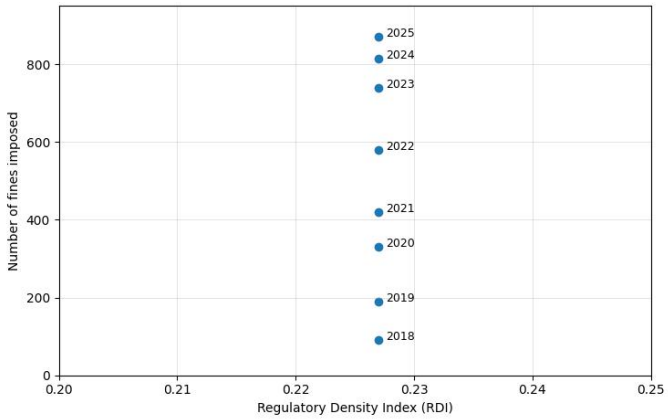

Figure 1. Scatter plot of the association between RDI and the number of fines imposed. Source: compiled by the author based on the results of regression analysis.

The scatter plot presents RDI on the horizontal axis and the number of fines on the vertical axis, with a fitted regression line. The distribution of observations visually supports the positive association identified in the exploratory regression model. This visualization complements the coefficient estimates in Table 6 by showing that higher values of regulatory density are associated with higher recorded sanctioning activity within the analyzed sample.

Overall, the exploratory regression results indicate a positive statistical association between RDI and sanctioning activity within the analyzed sample. At the same time, the findings remain limited by the small number of jurisdictions, the aggregated nature of enforcement indicators and the uneven availability of comparable data across legal regimes. For this reason, the regression results should be understood as indicative evidence supporting further comparative inquiry rather than as a definitive econometric confirmation of a causal relationship between regulatory density and enforcement outcomes.

5. Discussion

The results indicate that regulatory density and sanction-oriented provisions are related but not identical characteristics of legal architecture. The European Union demonstrated the highest RDI and the highest share of financial responsibility provisions, whereas Ukraine showed a relatively close RDI value but a substantially lower share of financial sanction provisions. This distinction is important for interpreting regulatory saturation. A legal regime may contain many imperative rules, but these rules do not necessarily form a coherent enforcement mechanism. Regulatory saturation may therefore coexist with fragmented responsibility, overlapping institutional competences and uneven practical implementation.

This finding is consistent with the literature on cross-border health data and GDPR-based regulation. Mulder and Tudorica[67] show that privacy policies and cross-border health data processing under the GDPR operate within a complex legal environment in which formal obligations do not automatically resolve practical uncertainty. Bradford et al.[68] similarly argue that the adequacy of a data protection regime depends not only on formal legal compatibility, but also on the existence of enforceable safeguards. In the context of the present research, this means that the RDI captures only one structural dimension of regulation, while the share of financial responsibility provisions reflects a more sanction-oriented dimension of legal design.

The exploratory regression results showed a positive association between RDI and the number of fines within the analyzed dataset. This result should be interpreted cautiously. It does not prove that regulatory density directly causes higher sanctioning activity. Rather, it suggests that jurisdictions with a higher concentration of imperative provisions tend to show higher recorded sanctioning activity within the analyzed dataset. This interpretation is consistent with Shastri et al.,[69] who identify GDPR anti-patterns and show that formal compliance does not always correspond to substantive compliance quality. A dense regulatory framework may create more legal bases for detecting deviations, but the translation of such deviations into sanctions depends on institutional capacity, procedural practice and available technical expertise.

The technological dimension also helps explain why regulatory density alone cannot guarantee regulatory integrity. Turan et al.[70] demonstrate that advanced cryptographic tools, including homomorphic encryption, may expand the possibilities of secure data processing. However, such technologies also require substantial technical capacity from organizations and regulators. In practice, the enforcement of data protection and cybersecurity rules

[67] MULDER, T. and TUDORICA, M. "Privacy policies, cross-border health data and the GDPR", Information & Communications Technology Law, 28(3), 2019, pp. 261–274. https://doi.org/10.1080/13600834.2019.1644068

[68] BRADFORD, L., ABOY, M. and LIDDELL, K. "International transfers of health data between the EU and USA: A sector-specific approach for the USA to ensure an 'adequate' level of protection", Journal of Law and the Biosciences, 7(1), 2020, 1-33. https://doi.org/10.1093/jlb/lsaa055

[69] SHASTRI, S., WASSERMAN, M. and CHIDAMBARAM, V. "GDPR anti-patterns", Communications of the ACM, 64(2), 2021, pp. 59–65. https://doi.org/10.1145/3378061

[70] TURAN, F., ROY, S.S. and VERBAUWHEDE, I. "HEAWS: An accelerator for homomorphic encryption on the Amazon AWS FPGA", IEEE Transactions on Computers, 69(8), 2020, pp. 1185–1196. https://doi.org/10.1109/TC.2020.2988765

depends not only on the existence of mandatory legal provisions, but also on whether regulated actors can implement appropriate technical safeguards and whether supervisory bodies can assess them adequately.

The interface and behavioral dimensions of compliance provide an additional explanation for the gap between formal regulation and actual implementation. Berens et al.[71] show that cookie disclaimers often contain dark patterns and insufficient transparency. Kretschmer et al.[72] similarly demonstrate that the GDPR changed the web environment, but did not eliminate problematic consent practices. Rasaii et al.[73] add that accept-or-pay cookie banners may create new compliance tensions by formally offering choice while practically limiting meaningful consent. These studies support the interpretation that an increase in breach notifications and fines may reflect not only stronger enforcement, but also persistent structural problems in the everyday implementation of data protection rules.

The economic dimension of data regulation further complicates the interpretation of sanctioning activity. Jia et al.[74] found that the GDPR affected technology venture investment in the short run, while Martin et al.[75] showed that data protection regulation may influence startup innovation. These findings suggest that regulatory density produces broader market effects: it may strengthen standardization and trust, but also increase compliance costs for smaller or less technically prepared actors. Therefore, sanctioning activity should not be interpreted only as a punitive outcome. It is also part of a broader regulatory environment that shapes incentives, risk management and organizational behavior.

The organizational dimension is also relevant. Arias-Pérez and Vélez-Jaramillo[76] argue that digital orientation, organizational culture and employees' awareness of artificial intelligence interact in shaping digital innovation performance. Although the present research did not directly measure organizational culture or technological readiness, these factors may partly explain why the same regulatory requirements produce different enforcement outcomes across jurisdictions. Regulatory density may create a formal structure of obligations, but institutional maturity and organizational digital capacity determine how these obligations are implemented in practice.

The findings therefore provide exploratory evidence consistent with the research assumption that structural characteristics of regulatory architecture are associated with sanctioning activity. However, the results should not be treated as confirmatory econometric proof. The panel includes only four jurisdictions and eight annual observations, and enforcement data are more systematically available for the EU than for the other jurisdictions. In addition, the EU itself represents a multi-level enforcement system in which

---

[71] BERENS, B.M., BOHLENDER, M., DIETMANN, H., KRISAM, C., KULYK, O. and VOLKAMER, M. "Cookie disclaimers: Dark patterns and lack of transparency", Computers & Security, 136, 2024, 103507. https://doi.org/10.1016/j.cose.2023.103507

[72] KRETSCHMER, M., PENNEKAMP, J. and WEHRLE, K. "Cookie banners and privacy policies: Measuring the impact of the GDPR on the Web", ACM Transactions on the Web, 15(4), 2021, Article 20, pp. 1–42. https://doi.org/10.1145/3466722

[73] RASAII, A., GOSAIN, D. and GASSER, O. "Thou shalt not reject: Analyzing accept-or-pay cookie banners on the Web", in Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23), Association for Computing Machinery, 2023, pp. 154–161. https://doi.org/10.1145/3618257.3624846

[74] JIA, J., JIN, G.Z. and WAGMAN, L. "The short-run effects of the General Data Protection Regulation on technology venture investment", Marketing Science, 40(4), 2021, pp. 593–812. https://doi.org/10.1287/mksc.2020.1271

[75] MARTIN, N., MATT, C., NIEBEL, C. and BLIND, K. "How data protection regulation affects startup innovation", Information Systems Frontiers, 21, 2019, pp. 1307–1324. https://doi.org/10.1007/s10796-019-09974-2

[76] ARIAS-PÉREZ, J. and VÉLEZ-JARAMILLO, J. "Ignoring the three-way interaction of digital orientation, not-invented-here syndrome and employee's artificial intelligence awareness in digital innovation performance: A recipe for failure", Technological Forecasting and Social Change, 174, 2022, 121305. https://doi.org/10.1016/j.techfore.2021.121305

national data protection authorities differ in resources, sanctioning strategies and procedural practice. These limitations reduce the possibility of broad generalization.

From a practical perspective, the results suggest that increasing the number of mandatory provisions is not sufficient for building an effective data protection regime. Legal density must be accompanied by clear sanction mechanisms, institutional coordination, technical expertise and consistent enforcement procedures. This is especially important where personal data protection overlaps with cybersecurity, digital services regulation and algorithmic governance. The regulatory "labyrinth" emerges not simply because there are many norms, but because responsibilities, supervisory powers and technical standards are distributed across several institutional fields.

Overall, the study contributes to the literature by proposing the RDI as a comparative indicator of regulatory architecture and by distinguishing it from the financial responsibility share. The results extend existing discussions on GDPR implementation, cross-border data governance, privacy interfaces, technical safeguards and regulatory effects on innovation. At the same time, the proposed model should be understood as exploratory. Further studies should expand the number of jurisdictions, include more comparable non-EU enforcement data, and integrate indicators of DPA investigations, institutional capacity and technological readiness.

6. Conclusions

The research demonstrated that the structural characteristics of information and personal data protection regimes can be operationalized through quantitative indicators. RDI made it possible to compare the concentration of imperative provisions in the European Union, Ukraine, the United Kingdom and California, while the financial responsibility share (F) allowed the sanction-oriented component of each regulatory architecture to be assessed separately. This distinction is important because a dense regulatory framework does not necessarily contain an equally strong financial liability structure.

The comparative analysis showed that the European Union has the highest RDI and the highest share of imperative provisions containing financial sanctions. Ukraine also demonstrated a relatively high level of regulatory density, but its financial responsibility share was lower than that of the EU, the United Kingdom and California. This result indicates that regulatory saturation and sanction concentration are related but not identical features of legal design. A jurisdiction may contain many mandatory provisions, while still having a less developed or less consistently integrated system of financial sanctions.

The exploratory regression analysis indicated a positive association between RDI and the number of fines within the analyzed dataset. However, this result should be interpreted cautiously. The model does not establish a causal relationship between regulatory density and enforcement outcomes. Rather, it suggests that jurisdictions with a higher concentration of imperative provisions tend to show higher recorded sanctioning activity within the available data. This finding supports the analytical relevance of comparing regulatory structure with enforcement indicators, but it requires further testing on larger and more balanced cross-jurisdictional datasets.

The practical significance of the study lies in the possibility of using RDI and F as comparative tools for assessing the internal structure of data protection and information security regimes. For legislators and regulators, the findings suggest that the number of mandatory provisions should not be considered in isolation. Effective regulation also depends on the coherence of sanction mechanisms, institutional coordination, technical expertise and the capacity of supervisory authorities to transform legal obligations into consistent enforcement practice.

The study has several limitations. The sample includes only four jurisdictions, which restricts the generalizability of the statistical findings. Enforcement data are more systematically available for the European Union than for Ukraine, the United Kingdom and

California, which creates asymmetry in the empirical analysis. In addition, the EU was treated as a single regulatory architecture, although enforcement is conducted by national data protection authorities with different resources and sanctioning practices. The research also did not include micro-level analysis of administrative decisions, court practice, institutional capacity or technological readiness of regulated actors.

Future research should expand the number of jurisdictions, include more comparable non-EU enforcement indicators and integrate data on DPA investigations, breach notifications, cyber incidents and non-financial corrective measures. Further studies may also examine changes in RDI over time in order to assess how amendments to data protection, cybersecurity and algorithmic governance rules modify the structure of regulatory architecture.

Overall, the article proposes an exploratory comparative model for measuring regulatory density and relating it to sanctioning activity. Its contribution lies in combining regulatory coding with enforcement indicators and in showing that regulatory architecture can be analyzed not only doctrinally, but also through measurable structural characteristics.

7. References

ARIAS-PÉREZ, J. and VÉLEZ-JARAMILLO, J. "Ignoring the three-way interaction of digital orientation, not-invented-here syndrome and employee's artificial intelligence awareness in digital innovation performance: A recipe for failure", Technological Forecasting and Social Change, 174, 2022, 121305. https://doi.org/10.1016/j.techfore.2021.121305

BERENS, B.M., BOHLENDER, M., DIETMANN, H., KRISAM, C., KULYK, O. and VOLKAMER, M. "Cookie disclaimers: Dark patterns and lack of transparency", Computers & Security, 136, 2024, 103507. https://doi.org/10.1016/j.cose.2023.103507

BLIND, K., NIEBEL, C. and RAMMER, C. "The impact of the EU General Data Protection Regulation on product innovation", Industry and Innovation, 31(3), 2024, pp. 311–351. https://doi.org/10.1080/13662716.2023.2271858

BRADFORD, L., ABOY, M. and LIDDELL, K. "International transfers of health data between the EU and USA: A sector-specific approach for the USA to ensure an 'adequate' level of protection", Journal of Law and the Biosciences, 7(1), 2020, 1-33. https://doi.org/10.1093/jlb/lsaa055

BUCKLEY, G., CAULFIELD, T. and BECKER, I. "GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved?", Journal of Cybersecurity, 10(1), 2024, tyae017. https://doi.org/10.1093/cybsec/tyae017

CALIFORNIA LEGISLATURE. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100], California, 2018. Available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.∂=4.&lawCode=CIV&title=1.81.5 (accessed on 6 March 2026).

CALIFORNIA LEGISLATURE. California Privacy Rights Act of 2020 (Proposition 24), California, 2020. Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB375 (accessed on 6 March 2026).

CAROVANO, G. and FINCK, M. "Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy", Computer Law & Security Review, 50, 2023, 105830. https://doi.org/10.1016/j.clsr.2023.105830

CHIARA, P.G. "Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise?", European Journal of Risk Regulation, 16(2), 2025, pp. 469–484. https://doi.org/10.1017/err.2025.9

COMPLIANCE HUB. "GDPR enforcement and data breach landscape: A synthesis of 2025–2026 trends", 2026. Available at: https://compliancehub.wiki/gdpr-enforcement-and-data-breach-landscape-a-synthesis-of-2025-2026-trends/ (accessed on 6 March 2026).

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, L 119, 2016, pp. 89–131. Available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj (accessed on 6 March 2026).

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), Official Journal of the European Union, L 333, 2022, pp. 80–152. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed on 6 March 2026).

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, 2016. Available at: https://www.legislation.gov.uk/eur/2016/679 (accessed on 6 March 2026).

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), Official Journal of the European Union, L 295, 2018, pp. 39–98. Available at: https://eur-lex.europa.eu/eli/reg/2018/1725/oj (accessed on 6 March 2026).

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), Official Journal of the European Union, L 152, 2022, pp. 1–44. Available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj (accessed on 6 March 2026).

EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA threat landscape 2025, 2025. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed on 6 March 2026).

EUROPEAN UNION. Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 326, 2012, pp. 391–407. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed on 6 March 2026).

FERGUSON, D.D.S. "European cybersecurity certification schemes and cybersecurity in the EU internal market", International Cybersecurity Law Review, 3, 2022, pp. 51–114. https://doi.org/10.1365/s43439-021-00044-5

GENEVA INTERNET PLATFORM. "GDPR violation reports surge across Europe in 2025, study finds", 31 January 2026. Available at: https://dig.watch/updates/gdpr-violations-rise-europe-2025 (accessed on 6 March 2026).

HALLINAN, D., BERNIER, A., CAMBON-THOMSEN, A., CRAWLEY, F.P., DIMITROVA, D., BAUZER MEDEIROS, C., NILSSON, G., PARKER, S., PICKERING, B. and RENNES, S. "International transfers of personal data for health research following Schrems II: A problem in need of a solution", European Journal of Human Genetics, 29, 2021, pp. 1502–1509. https://doi.org/10.1038/s41431-021-00893-y

JIA, J., JIN, G.Z. and WAGMAN, L. "The short-run effects of the General Data Protection Regulation on technology venture investment", Marketing Science, 40(4), 2021, pp. 593–812. https://doi.org/10.1287/mksc.2020.1271

JULIUSSEN, B.A., KOZYRI, E., JOHANSEN, D. and RUI, J.P. "The third country problem under the GDPR: Enhancing protection of data transfers with technology", International Data Privacy Law, 13(3), 2023, pp. 225–243. https://doi.org/10.1093/idpl/ipad013

KOULIERAKIS, E. "Certification as guidance for data protection by design", International Review of Law, Computers & Technology, 38(2), 2024, pp. 245–263. https://doi.org/10.1080/13600869.2023.2269498

KRÄMER, J. "Personal data portability in the platform economy: Economic implications and policy recommendations", Journal of Competition Law & Economics, 17(2), 2021, pp. 263–308. https://doi.org/10.1093/joclec/nhaa030

KRETSCHMER, M., PENNEKAMP, J. and WEHRLE, K. "Cookie banners and privacy policies: Measuring the impact of the GDPR on the Web", ACM Transactions on the Web, 15(4), 2021, Article 20, pp. 1–42. https://doi.org/10.1145/3466722

LABADIE, C. and LEGNER, C. "Building data management capabilities to address data protection regulations: Learnings from EU–GDPR", Journal of Information Technology, 38(1), 2023, pp. 23–45. https://doi.org/10.1177/02683962221141456

MARKOPOULOU, D., PAPAKONSTANTINOU, V. and DE HERT, P. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", Computer Law & Security Review, 35(6), 2019, 105336. https://doi.org/10.1016/j.clsr.2019.06.007

MARTIN, N., MATT, C., NIEBEL, C. and BLIND, K. "How data protection regulation affects startup innovation", Information Systems Frontiers, 21, 2019, pp. 1307–1324. https://doi.org/10.1007/s10796-019-09974-2

Mone V., Thommandru A., Maratovich F.F., Khurramovich K.F., Mirziyatovna A.K. "AI price tags and privacy: When your data sets your price", WIREs Data Mining and Knowledge Discovery, 2026. https://doi.org/10.1002/widm.70070

MONE, V.; MITHARWAL, S. "Guardians of privacy: Exploring the viability of a United Nations-backed global data governance", International Journal of Intellectual Property Management, 14(2), 2024, pp. 194–216. https://doi.org/10.1504/IJIPM.2024.137220

MONE, V.; SADIKOV, M. A.; YOUNAS, A.; PETIKAM, S. "Data warfare and creating a global legal and regulatory landscape: Challenges and solutions", International Journal of Legal Information, 2024. https://doi.org/10.1017/jli.2024.22

MONE, V.; TILWANI, R.; SIVAKUMAR, C. L.; FAYZULLAEVA, S. "Evaluating the prospects of a UN-backed global data protection authority: A Third World perspective", International Organizations Law Review, 2025. https://doi.org/10.1163/15723747-22010002

MS LAW. TAX. GDPR Enforcement Tracker: Statistics – fines imposed over time. Available at: https://www.enforcementtracker.com/ (accessed on 6 March 2026).

MULDER, T. and TUDORICA, M. "Privacy policies, cross-border health data and the GDPR", Information & Communications Technology Law, 28(3), 2019, pp. 261–274. https://doi.org/10.1080/13600834.2019.1644068

MURPHY, M.H. "Assessing the implications of Schrems II for EU–US data flow", International & Comparative Law Quarterly, 71(1), 2022, pp. 245–262. https://doi.org/10.1017/S0020589321000348

PEUKERT, C., BECHTOLD, S., BÁTIKAS, M. and KRETSCHMER, T. "Regulatory spillovers and data governance: Evidence from the GDPR", Marketing Science, 41(4), 2022, pp. 746–768. https://doi.org/10.1287/mksc.2021.1339

PRESIDENT OF UKRAINE. Decree No. 685/2021 on the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 on the Information Security Strategy, Ukraine, 2021. Available at: https://www.rnbo.gov.ua/ua/Ukazy/5203.html (accessed on 6 March 2026).

RASAII, A., GOSAIN, D. and GASSER, O. "Thou shalt not reject: Analyzing accept-or-pay cookie banners on the Web", in Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23), Association for Computing Machinery, 2023, pp. 154–161. https://doi.org/10.1145/3618257.3624846

RUNTE C.; KAMPS M. "Record broken: GDPR fines exceed EUR 5 billion for the first time", 2025. Available at: https://cms.law/en/ukr/news-information/record-broken-gdpr-fines-exceed-eur-5-billion-for-the-first-time (accessed on 6 March 2026).

RUOHONEN, J. and HJERPPE, K. "The GDPR enforcement fines at glance", Information Systems, 106, 2022, 101876. https://doi.org/10.1016/j.is.2021.101876

SCHMITZ-BERNDT, S. "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive", Journal of Cybersecurity, 9(1), 2023, tyad009. https://doi.org/10.1093/cybsec/tyad009

SHASTRI, S., WASSERMAN, M. and CHIDAMBARAM, V. "GDPR anti-patterns", Communications of the ACM, 64(2), 2021, pp. 59–65. https://doi.org/10.1145/3378061

THOMMANDRU A., MONE V., SHOKHIJAKHON F., MIRZAYEV G. "Algorithmic profiling and facial recognition in EU border control: Examining ETIAS decision-making, privacy and law", WIREs Data Mining and Knowledge Discovery, 2025. https://doi.org/10.1002/widm.70013

TURAN, F., ROY, S.S. and VERBAUWHEDE, I. "HEAWS: An accelerator for homomorphic encryption on the Amazon AWS FPGA", IEEE Transactions on Computers, 69(8), 2020, pp. 1185–1196. https://doi.org/10.1109/TC.2020.2988765

UK PARLIAMENT. Data Protection Act 2018, United Kingdom, 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents (accessed on 6 March 2026).

UK PARLIAMENT. Online Safety Act 2023, United Kingdom, 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/50/contents (accessed on 6 March 2026).

VANBERG, A.D. "Informational privacy post GDPR – end of the road or the start of a long journey?", The International Journal of Human Rights, 25(1), 2021, pp. 52–78. https://doi.org/10.1080/13642987.2020.1789109

VERKHOVNA RADA OF UKRAINE. Constitution of Ukraine (adopted June 28, 1996, as amended), Ukraine, 1996. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (accessed on 6 March 2026).

VERKHOVNA RADA OF UKRAINE. On Amendments to Certain Laws of Ukraine Regarding the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure (Law of Ukraine No. 4336-IX, March 27, 2025), Ukraine, 2025. Available at: https://zakon.rada.gov.ua/laws/show/4336-20 (accessed on 6 March 2026).

VERKHOVNA RADA OF UKRAINE. On National Security of Ukraine (Law of Ukraine No. 2469-VIII, June 21, 2018, as amended), Ukraine, 2018. Available at: https://zakon.rada.gov.ua/laws/show/2469-19 (accessed on 6 March 2026).

VERKHOVNA RADA OF UKRAINE. On Personal Data Protection (Law of Ukraine No. 2297-VI, December 1, 2010, as amended June 14, 2025), Ukraine, 2010. Available at: https://zakon.rada.gov.ua/laws/show/2297-17?lang=en (accessed on 6 March 2026).

VERKHOVNA RADA OF UKRAINE. On Protection of Information in Information and Communication Systems (Law of Ukraine No. 80/94-VR, July 5, 1994, as amended April 20, 2025), Ukraine, 1994. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (accessed on 6 March 2026).

VERKHOVNA RADA OF UKRAINE. On the Basic Principles of Ensuring Cybersecurity of Ukraine (Law of Ukraine No. 2163-VIII, October 5, 2017, as amended October 19, 2025), Ukraine, 2017. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed on 6 March 2026).

WEITZENBOECK, E.M., LISON, P., CYNDECKA, M. and LANGFORD, M. "The GDPR and unstructured data: Is anonymization possible?", International Data Privacy Law, 12(3), 2022, pp. 184–206. https://doi.org/10.1093/idpl/ipac008