Artigo original

http://dx.doi.org/10.18623/rvd.v23.5572

THE LEGAL SECURITY OF DIGITAL ECOSYSTEMS

A SEGURANÇA JURÍDICA DOS ECOSSISTEMAS DIGITAIS

Article received on: 11/10/2025
Article accepted on: 2/6/2026

Denis Gabriela Ghervase*
*Universitatea Andrei Şaguna din Constanța, Constanța, Constanța, Romênia
Orcid: https://orcid.org/0009-0000-9638-8537
denis.ghervase@yahoo.com

Andreea Mihaela Ilincuța*
*Universitatea Andrei Şaguna din Constanța, Constanța, Constanța, Romênia
Orcid: https://orcid.org/0009-0001-9657-6981
cabavilincuta@yahoo.com

Nicoleta Raina Geamalinga*
*Universitatea Andrei Şaguna din Constanța, Constanța, Constanța, Romênia
Orcid: https://orcid.org/0009-0004-3849-5157
geamalinga@societate-notariala.ro

The authors declare that there is no conflict of interest

Abstract
This article analyzes the legal mutations induced by the accelerated digitalization across various fields of activity, with a specific focus on the transition from traditional IT security to the concept of digital operational resilience. In the context of the full implementation of Regulation (EU) 2022/2554 (DORA) starting in 2025, the paper explores the reconfiguration of civil and prudential liability of the institutions involved in relation to emerging threats (AI, DDoS attacks, Ransomware). By analyzing recent CJEU case law (Case C-340/21) and due diligence standards in proactive cost allocation (EDR, SIEM, SOC), this research proposes an integrated vision of cyber governance as a pillar of social, economic, and financial stability.

Keywords: Cybersecurity. Operational Resilience. Financial Law. Artificial Intelligence. Legal Liability.

Resumo
Este artigo analisa as mudanças jurídicas provocadas pela digitalização acelerada em diversos setores de atividade, com foco específico na transição da segurança de TI tradicional para o conceito de resiliência operacional digital. No contexto da plena implementação do Regulamento (UE) 2022/2554 (DORA) a partir de 2025, o artigo explora a reconfiguração da responsabilidade civil e prudencial das instituições envolvidas em relação às ameaças emergentes (IA, ataques DDoS, ransomware). Ao analisar a jurisprudência recente do TJUE (Processo C-340/21) e os padrões de due diligence na alocação proativa de custos (EDR, SIEM, SOC), esta pesquisa propõe uma visão integrada da governança cibernética como um pilar da estabilidade social, econômica e financeira.

Palavras-chave: *Segurança Cibernética. Resiliência Operacional. Direito Financeiro. Inteligência Artificial. Responsabilidade Legal.*

1 INTRODUCTION

The digital transformation of the financial sector, driven by FinTech ecosystems and Artificial Intelligence, has transcended the sphere of economic optimization, becoming a matter of public-order stability.[1]

From a legal perspective, cybersecurity has evolved from a mere obligation of technical diligence into an obligation of result with regard to operational resilience, a development confirmed by the new prudential compliance standards.[2]

The adoption of Regulation (EU) 2022/2554 (DORA) marks the transition toward a model of "security through regulation," in which ICT incidents are treated as risks capable of generating cascading failures across the entire Union.[3]

The judgment of the Court of Justice of the European Union (CJEU) in Case C-340/21 (VB v. National Revenue Agency of Bulgaria)[4] provides essential clarifications regarding the interpretation of Article 82 of the GDPR in the context of cybersecurity incidents, in relation to the legal issue under analysis, following a cyberattack on the Bulgarian National Revenue Agency (NRA), during which the personal data of millions of citizens were published online.

The Court held that the mere occurrence of a security breach does not automatically mean that the controller's technical and organizational measures were inadequate; however, the burden of proof lies with the controller, who must demonstrate that its measures were "appropriate" in relation to the risk (Articles 24 and 32 GDPR).

Furthermore, the Court clarified that the controller (a public institution) is not exempt from liability solely because the damage was caused by an external attacker, where it is established that deficiencies in the controller's security measures facilitated the attack.

---

[1] M. Constantinescu, Dreptul Securității Cibernetice: Provocări în Spațiul Financiar European, Ed. C.H. Beck, București, 2024, p. 45.
[2] C. Radu, Securitatea informației în instituțiile de credit. Abordări juridice și tehnice, Ed. Universul Juridic, București, 2023, pp. 89-92.
[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), Official Journal of the European Union, L 333/1, accessed on 25 February 2026.
[4] CJUE, Marea Cameră, Hotărârea din 14 decembrie 2023, VB împotriva Agenția Națională pentru Venituri (Bulgaria), C-340/21, EU:C:2023:986.

Starting from Case C-340/21 (VB v. National Revenue Agency of Bulgaria), it can be argued that Regulation (EU) 2022/2554, known by the acronym DORA (Digital Operational Resilience Act), represents a turning point in European legislation, being fully applicable as of 17 January 2025.[5]

From a legal standpoint, DORA is not merely a set of technical rules, but an instrument of maximum harmonization aimed at eliminating legislative fragmentation among Member States with regard to ICT (Information and Communication Technology) risk.[6]

Moreover, unlike previous directives, DORA is directly and bindingly applicable, imposing a uniform set of rules on more than 20 types of financial entities. Its legal essence lies in the shift from a "risk management" model to a "resilience assurance" model, which entails that entities must not only prevent attacks, but also demonstrate the legal and operational capacity to absorb cyber shocks and ensure the continuity of essential services.

An element of absolute novelty is the regulation of contractual relationships with third-party ICT service providers (e.g., cloud providers), in that the Regulation imposes mandatory minimum contractual clauses and grants the European Supervisory Authorities (EBA, ESMA, EIOPA) direct powers to oversee "critical" providers.[7] This legal shift blurs the traditional distinction between the regulated financial sector and the technology sector, bringing major technology companies under a form of indirect prudential supervision.

The DORA Regulation clarifies the responsibility of governing bodies (top management), in the sense that, from a legal standpoint, members of the board of directors are subject to an obligation of active oversight and may incur personal liability for deficiencies in ICT risk management, thereby emphasizing that cybersecurity has become an intrinsic component of fiduciary duties in financial corporate law.

[5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, OJ L 333, 27.12.2022, accessed on 27 February 2026.
[6] A. Z. Rusu, „Implicațiile DORA asupra contractelor de externalizare TIC", în Analele Universității din București – Seria Drept, 2024, p. 45-47.
[7] M. B. Ghica, „Supravegherea furnizorilor critici de servicii TIC: o nouă frontieră a dreptului administrativ european", în Revista Română de Drept European, nr. 1/2025, p. 32.

In conclusion, in the field of civil liability, the case-law of the CJEU has evolved toward enhanced protection of data subjects, establishing in Case C-340/21 that the mere state of fear relating to the potential misuse of data following an incident constitutes compensable non-material damage. This interpretation reshapes risk management for financial institutions, transforming cybersecurity from a formal obligation into a central pillar of both patrimonial and non-patrimonial protection of clients.[8]

The current global context is defined by an accelerated digital transformation, a phenomenon that has fundamentally reshaped the financial sector through the adoption of FinTech platforms, robo-advisory services, and instant payment systems. However, from a legal perspective, this transition has generated a shift in risk: a major disruption within a single institution can now trigger systemic risk, affecting regional or even global economic stability.

Consequently, cybersecurity has transcended the technical sphere, becoming a top-management priority and a national security imperative, rigorously regulated through prudential supervisory mechanisms.[9]

It may also be argued that the cornerstone of this revolution is Artificial Intelligence (AI) and the processing of massive volumes of data (Big Data), given that not only banking institutions, but also other public authorities and institutions, make intensive use of Machine Learning algorithms for critical tasks such as fraud detection and risk analysis.

However, although the use of AI is regarded by 77% of professionals as the determining factor of operational success, it significantly expands the legal and technical "attack surface." In this context, threats are not merely evolving but are being amplified by techniques such as deepfakes and advanced spear-phishing, thereby compelling the legislator to redefine the standards for safeguarding data integrity.[10]

Moreover, the integration of AI introduces subtle internal risks, such as algorithmic bias and the lack of transparency ("black box" systems), which may compromise the integrity of financial decision-making. In modern financial law, striking

[8] S. Popescu, „Evoluția conceptului de prejudiciu moral în era atacurilor cibernetice masive", în Revista de Drept Comercial, nr. 1/2024, pp. 56-60
[9] M. P. Mathen, A. Paul, „Toward an evolving framework for responsible AI for credit scoring in the banking industry", în Journal of Information, Communication & Ethics in Society, 2025, p. 25
[10] Idem

a balance between innovation and cyber resilience thus represents the strategic challenge of the decade.

Accordingly, dependence on interconnected ecosystems elevates cybersecurity to the level of systemic risk, generating new vulnerabilities related to data confidentiality and ethical governance—developments that are constantly monitored by key bodies, which report an unprecedented escalation of attacks on critical infrastructures.[11]

2 THE ROLE AND IMPORTANCE OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

The CIA Triad: Confidentiality, Integrity, and Availability represents the foundational framework of information security, defining the essential objectives of any defense system. While their applicability and relative weight vary depending on the sector, compliance with these principles is indispensable for maintaining trust and operational stability.

Confidentiality refers to ensuring that information is accessible only to authorized entities. In the current context, this principle entails the protection of sensitive personal data (PII – Personally Identifiable Information) and banking secrecy through encryption mechanisms and strict access control, particularly given the volume and sensitivity of the data processed. Accordingly, a breach of confidentiality (for example, data theft through ransomware or the exploitation of a vulnerability) leads directly to litigation and severe sanctions (notably under DORA), as well as to the irreversible loss of trust in the respective institution.

Availability guarantees that systems and resources are accessible to authorized users whenever necessary. Considering the nature of financial services, any disruption (for example, a DDoS attack) may result in immediate financial losses and a massive erosion of trust, directly affecting market stability and, potentially, public order.[12]

[11] ENISA, Threat Landscape for the Financial Sector, 2024, p. 27

[12] Chatterjee, P., Das, D., & Rawat, D. B. (2024). A generative AI approach for ensuring data integrity security resilience in FinTech systems. In 2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops. IEEE. https://doi.org/10.1109/CCGridW63211.2024.00027 – accessed on 16.11.2025

Moreover, a lack of availability (caused by DDoS attacks, hardware failures, or system errors) generates disruptions to essential services and may directly affect even the resolution of cases within a reasonable time. In this context, the current DORA Regulation places digital operational resilience—and, implicitly, availability—at the very core of its regulatory architecture.

Integrity represents the property of data to be complete, accurate, and not altered or destroyed in an unauthorized manner. In many systems, integrity is often regarded as the most critical pillar, since the modification of a single record within an application may produce significant adverse consequences, leading to social imbalances and undermining trust in automated systems.

Compromising integrity (for example, through data poisoning attacks targeting AI models or through the injection of malicious code)[13] may result in erroneous decisions, false reporting, and systemic loss of confidence. Accordingly, the use of hashing functions and digital signatures to verify data authenticity, version control mechanisms, and the implementation of input–output validation and verification procedures constitute essential data integrity safeguards.

3 TYPOLOGY OF CYBER THREATS: AN ANALYSIS FROM THE PERSPECTIVE OF INTERNATIONAL CRIMINAL AND FINANCIAL LAW

In the current legal landscape, cyberattacks are no longer viewed merely as technical incidents, but as forms of aggression against the financial public order. Their classification generally follows the CIA triad—referenced above—yet each component entails a distinct regime of legal liability.

Threats to Availability (the critical component of operational resilience) predominantly manifest through Distributed Denial of Service (DDoS) attacks. From a legal standpoint, however, the use of botnet networks constitutes a form of computer

[13] Barile, D., Secundo, G., & Bussoli, C. (2024). Exploring artificial intelligence robo-advisors in the banking industry: A platform model. Management Decision. Advance online publication. https://doi.org/10.1108/MD-08-2023-1324 - accessed on 16.11.2025.

sabotage, criminalized at the international level under the Convention on Cybercrime (Budapest Convention on Cybercrime)[14].

In the financial sector, the impact of a DDoS attack extends beyond the technical sphere, generating a breach of the service continuity obligations imposed under Pillar II of the DORA Regulation. In this regard, the paralysis of interbank payment systems such as SWIFT and TARGET2, or of FinTech APIs, directly affects market liquidity.

In recent case-law and supervisory practice, such disruptions have been characterized as a form of "market vulnerability," capable of triggering substantial prudential sanctions from supervisory authorities such as the National Bank of Romania and the European Central Bank.[15]

However, the use of DDoS attacks by state actors or hacktivist groups in the context of ongoing regional conflicts has led to their reclassification as instruments of "hybrid warfare." This development has compelled EU Member States to strengthen the protection of critical infrastructures through the adoption of the Directive (EU) 2022/2555 (NIS2 Directive).[16]

The compromise of data integrity and confidentiality constitutes one of the most serious breaches of the trust-based relationship between an institution and the individuals concerned. Such tactics (data encryption followed by threats of publication on the Dark Web)[17] represent a convergence between the criminal offense of extortion and a personal data breach within the meaning of the GDPR.

From a legal perspective, the unauthorized alteration of financial records or credit scores amounts to computer forgery, with irreparable consequences for the evidentiary value of electronic documents.[18]

It may also be observed that, unlike opportunistic attacks, Advanced Persistent Threat (APT) campaigns constitute long-term cyber-espionage operations. From a

[14] S. G. Pop, Criminalitatea informatică. Analiză teoretică și practică, Ed. Hamangiu, București, 2024, p. 112.
[15] ENISA, Threat Landscape 2024, p. 28.
[16] S. Popescu, „Răspunderea membrilor consiliului de administrație pentru breșe de securitate cibernetică în lumina Directivei NIS2 și a Regulamentului DORA", in *Revista de Drept Comercial*, nr. 1/2025, p. 44. The author argues that the proactive underfunding of the Security Operations Center (SOC) may be interpreted as a breach of the duty of prudence.
[17] U.S. Department of the Treasury, Report on Cybersecurity in the Financial Services Sector, published in March 2024.
[18] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, p. 12.

compliance perspective, the existence of such threats obliges institutions to implement the Zero Trust model, which is no longer merely a recommendation but has evolved into a due diligence requirement under U.S. regulatory practice (e.g., the Office of the Comptroller of the Currency's supervisory guidance) and within the technical standards framework established by DORA.[19]

4 LEGAL ASSESSMENT OF PROACTIVE COSTS IN CYBERSECURITY

At present, the decision to invest in cybersecurity has ceased to constitute a mere cost–benefit economic analysis, evolving instead into an imperative of normative compliance. In banking law, a clear distinction is emerging between proactive costs (investments in resilience architectures) and reactive costs (financial losses, administrative sanctions, and damages).

Recent studies demonstrate that a preventive approach, grounded in emerging technologies such as generative AI, provides not only a positive return on investment but also a structural guarantee of data integrity and resilience within FinTech systems.[20]

In the context of Advanced Persistent Threat (APT) campaigns, traditional security architectures are increasingly regarded, also from a legal standpoint[21], as insufficient to meet the duty of diligence. Effective budgeting today entails the strategic allocation of capital toward solutions that ensure internal visibility and behavioral detection capabilities.

This "decoding of digital synergies" through mechatronic systems and AI-based infrastructures is essential for compliance with prudential supervisory standards[22]. From

[19] L. Dumitrescu, „Reziliența operațională digitală: standarde și sancțiuni sub imperiul DORA", in *Dreptul*, nr. 4/2024, p. 55.
[20] P. Chatterjee, D. Das, & D. B. Rawat, „A generative AI approach for ensuring data integrity security resilience in FinTech systems", în *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops*, IEEE, 2024, accessed on 18.01.2026.
[21] I. G. Tofan, „Răspunderea civilă pentru deciziile sistemelor autonome în sectorul financiar-bancar", în *Revista de Drept Bancar și Financiar*, no 1/2025, p. 34.
[22] L. F. Manta, A. G. Manta, & C. Gherțescu, „Decoding digital synergies: How mechatronic systems and artificial intelligence shape banking performance through quantile-driven method of moments", în *Applied Sciences*, 15(10), 5282, 2025. p. 11

the perspective of evidence and liability, three technological solutions form the backbone of modern defense:

a) Endpoint Detection and Response (EDR)

EDR represents the evolution of the traditional antivirus model toward continuous monitoring. From a legal standpoint, it serves as a damage-limitation instrument through its capacity to automatically isolate compromised systems, thereby preventing the propagation of harm across the entire network and safeguarding the integrity of informational assets.

b) Security Information and Event Management (SIEM)

SIEM functions as the analytical engine that transforms "informational noise" into actionable legal evidence (actionable threat intelligence). By correlating large-scale data streams in real time, it enables the identification of multi-stage attacks (such as unauthorized access followed by data exfiltration), providing critical decision-support in crisis management scenarios.[23]

c) Security Operations Center (SOC)

A SOC represents not merely a technological solution, but an organizational governance structure. A mature SOC is indispensable for fulfilling the rapid incident-reporting obligations imposed by DORA, ensuring the maintenance of service availability and compliance with Recovery Time Objectives (RTO) established in Business Continuity Plans (BCP).[24]

5 CONCLUSIONS

The present analysis demonstrates that cybersecurity in digital systems has ceased to be a mere technical attribute, becoming instead a fundamental component of state stability and global economic security. The transition from a "perimeter security" model

[23] In international judicial practice, event logs centralized through SIEM systems are fundamental for establishing the chronology of an attack and for substantiating criminal complaints in cases of cyber fraud. See, in this regard, the Europol, *Electronic Evidence Guide*, 2024.

[24] Regulation (EU) 2022/2554 (DORA), Articles 17–23, impose stringent standards for the detection, classification, and reporting of major ICT-related incidents, thereby transforming the operation of a Security Operations Center (SOC) into an implicit legal requirement for critical financial entities.

to one of "operational resilience," enshrined in Regulation (EU) 2022/2554 (DORA), marks the beginning of a new era in European financial law.

Recent case-law, in particular Case C-340/21 of the Court of Justice of the European Union, indicates a clear trend toward expanding the concept of non-material damage in the field of data breaches. From a legal standpoint, financial institutions must understand that investment in solutions such as EDR, SIEM, and SOC is not merely a matter of operational efficiency, but also an evidentiary instrument demonstrating professional diligence.[25] Their absence may lead to a presumption of fault in risk management, with severe pecuniary and reputational consequences.

In light of DORA and recent European jurisprudence, we are witnessing an "objectification" of institutional liability. In litigation concerning a security breach, mere formal compliance is no longer sufficient for exoneration. The institution bears the legal burden of proving not only that it possessed protective technology, but that it implemented a genuine "culture of resilience."

From a legal perspective, insufficient investment in solutions such as EDR or SOC may be interpreted as evidence of organizational fault, potentially reversing the burden of proof against the bank at an early stage of the proceedings.

Furthermore, the strict regulation of third-party ICT service providers under DORA establishes a new regime of joint liability. Outsourcing to cloud services no longer constitutes a transfer of risk, but rather an extension of the bank's supervisory perimeter.

It may reasonably be anticipated that courts will, by analogy, apply the doctrine of vicarious liability—holding the principal (the financial institution) liable for the acts of its agent (the ICT service provider). This development would compel banks to exercise quasi-sovereign control over the security posture of subcontractors, under the sanction of invalidating contractual clauses that limit liability within outsourcing agreements.

[25] L. Dumitrescu, „Responsabilitatea organelor de conducere în contextul DORA: o nouă dimensiune a bunei guvernanțe corporative", in Dreptul Afacerilor, nr. 3/2024, p. 12-15

5.1 De lege ferenda perspectives

Digital resilience is not a destination, but a continuous process of legal and technological adaptation. In the era of Artificial Intelligence and advanced mechatronic systems, the law must provide not only sanctions, but also an ethical and normative framework capable of safeguarding the pillars of integrity and confidentiality, thereby ensuring the long-term viability of the digital financial ecosystem.

In order to consolidate the current framework, the following normative developments appear necessary:

a) Standardization of the "Cyber-Audit" Obligation

The introduction of a statutory obligation of external cybersecurity auditing—analogous to financial audit requirements—for all entities operating AI algorithms in credit scoring. Such a measure would mitigate risks of algorithmic bias and discrimination and strengthen accountability in automated decision-making.

b) Recognition of Artificial Intelligence as a High-Risk Agent

The classification of AI systems used in high-frequency trading under a regime of strict (objective) liability, given their structural complexity and the possibility that their operational dynamics may exceed immediate human control.

c) Global Harmonization of Reporting Mechanisms

The establishment of a real-time cross-border reporting mechanism (beyond EU borders), under the auspices of an international body, to counter Advanced Persistent Threat (APT) attacks that exploit legislative asymmetries between jurisdictions.

In conclusion, from a normative standpoint, high-risk AI systems should be subject to a regime of "mandatory decision traceability." This would require that any AI-generated financial decision be open to meaningful human review. The inability to explain the algorithmic logic (the "black box" problem) should result in the unenforceability of that decision vis-à-vis the client.

A major legal challenge—often overlooked—is the tension between European regulations such as Regulation (EU) 2022/2554 (DORA) and General Data Protection Regulation (GDPR), and the legislation of states hosting major technology providers (e.g., the CLOUD Act). For this reason, it appears imperative to create a **"legal neutrality status for critical financial infrastructure,"** aimed at protecting European data from

foreign jurisdictional interference, by treating servers hosting critical services under a regime functionally analogous to diplomatic archive immunity.

At present, courts face considerable difficulties in assessing digital evidence due to the absence of a standardized legal expertise framework for complex cyberattacks. Accordingly, a transition is proposed from empirical evaluation of technical witnesses toward an Automated Evidentiary Standard, based on electronically signed event logs stored within integrity-assured SIEM systems.

Furthermore, in commercial litigation, the "digital fingerprint" generated by a certified SOC system should be granted probative force comparable to that of an authentic instrument, thereby reducing judicial error margins and shortening the duration of civil liability proceedings.

REFERENCES

Chatterjee, P., Das, D., & Rawat, D. B. (2024). „A generative AI approach for ensuring data integrity security resilience in FinTech systems". *IEEE 24th International Symposium*, IEEE.

Constantinescu, M. (2024). *Dreptul Securității Cibernetice: Provocări în Spațiul Financiar European*, Ed. C.H. Beck, București.

Court of Justice of the European Union (Grand Chamber), Judgment of 14 December 2023, *VB v. National Revenue Agency (Bulgaria)*, Case C-340/21, EU:C:2023:986.

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

Dumitrescu, L. (2024). „Responsabilitatea organelor de conducere în contextul DORA: o nouă dimensiune a bunei guvernanțe corporative", in *Dreptul Afacerilor*, no 3.

ENISA, *Threat Landscape for the Financial Sector*, Report 2024.

Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*.

Ghica, M. B. (2025). „Impactul DORA asupra parteneriatelor FinTech și accesului la API-uri conform PSD3", în *Revista Română de Drept al Afacerilor*, nr. 1.

Manta, A. G., Bădîrcea, R. M., et al. (2024). „Industry 4.0 transformation: Analysing the impact of artificial intelligence on the banking sector through bibliometric trends". *Electronics*, 13(9).

Manta, L. F., Manta, A. G., & Gherțescu, C. (2025). „Decoding digital synergies: How mechatronic systems and artificial intelligence shape banking performance". *Applied Sciences*, 15(10).

Mathen, M. P., & Paul, A. (2025). „Toward an evolving framework for responsible AI for credit scoring in the banking industry". *Journal of Information, Communication & Ethics in Society*.

Pop, S. G. (2024). *Criminalitatea informatică. Analiză teoretică și practică*, Hamangiu, București.

Radu, C. (2023). *Securitatea informației în instituțiile de credit. Abordări juridice și tehnice*, Universul Juridic, București.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA).

Tofan, I. G. (2024). „Reziliența operațională digitală în sectorul bancar. Analiză din perspectiva noului Regulament DORA", in *Revista de Drept Bancar și Financiar*, no 2.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Ghervase, D. G., Ilincuţa, A. M., & Geamalinga, N. R. (2026). THE LEGAL SECURITY OF DIGITAL ECOSYSTEMS. *Veredas Do Direito*, 23(5), e235572. https://doi.org/10.18623/rvd.v23.5572