International Journal of Law and Policy |
Volume: 2 Issue: 1
2024

# Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy

Naeem AllahRakha
Tashkent State University of Law
chaudharynaeem133@gmail.com
ORCID: 0000-3000-3001-1571

## Abstract

Digitalization is transforming economic activities, necessitating updated legal and policy frameworks for appropriate jurisdiction and governance. The borderless nature of digital trade introduces complexities around applicable laws, taxes, responsibilities, and liabilities. This paper reviews current debates on regulating digital spaces and reimagining digital borders to support equitable governance. Doctrinal and comparative analyses examine jurisdictional complexities. Grounded Theory assess regulatory initiatives. Ambiguous jurisdiction enables large platforms to circumvent laws. Prescriptive control risks stifling innovation. Blending scope-based rules with effects-based standards can balance control and openness. Principles-based extraterritorial applications of law aligned to global accords, demarcating platforms' responsibilities based on risk levels and impacts are suggested. It calls for cooperation advancing rights and fairness.

**Keywords:** Jurisdiction, Digital Economy, Cross-Border Payments, E-governance, Legal Frameworks

## I. Introduction

The exponential growth of the digital economy, fueled by unprecedented technological advancements, burgeoning connectivity, and new business models, has profoundly transformed international trade and transactions. However, this increasing virtualization of economic activities has also introduced complex jurisdictional and regulatory challenges stemming from the intrinsic borderless nature of cyberspace. Unlike the territorial clarity offered by physical geography, the online realm remains free from such spatial constraints, complicating legal authority and accountability over digital interactions spanning across nations [1].

With rising cross-border data flows, e-commerce, digital payments, and online platforms reshaping markets and work, questions around applicable laws, taxes, responsibilities, and liability become critical yet contentious. But rooted as they remain in traditional Westphalian notions of sovereignty, existing inter-state structures grapple to keep pace with the sweeping changes introduced by global digitization and connectivity. Therein lies a fundamental problem – the frameworks, systems and protocols devised to govern defined jurisdictions within territorial boundaries remain inadequate in an economic paradigm disregarding such geographies [2].

This regulatory ambiguity, coupled with the concentration of power in platform giants, has enabled detrimental outcomes like large-scale tax avoidance even as smaller entities bear the burden of compliance. Intricate legal technicalities shield the profits of digital multinationals like Google and Amazon from taxes in countries where they generate revenue but lack physical presence. Attempts to unilaterally address such gaps introduce further tensions as expansive extraterritorial jurisdiction claims by powerful states, evident in recent unilateral digital taxes imposed, threaten damaging tariff retaliations amidst accusations of trade protectionism [3].

These challenges underscore why reimagining digital borders calls for urgent cooperative solutions aligned to collective rights and welfare. However, constructing appropriate multilateral platforms is rife with geopolitical contentions, power struggles, and clashing visions of internet governance amidst the uncomfortable coexistence of democratic inclusiveness and authoritarian control instincts. Therein lies the gap this paper intends to examine - understanding pathways towards ethical, equitable frameworks balancing jurisdiction, governance and rights in an interconnected economy still dependent on Westphalian principles [4].

The core research questions thereby center on assessing how digital borders may be re-envisioned to enable regulatory clarity, what collaborative modalities can foster standardized norm building, and what implications emerge for state sovereignty, policy autonomy and global justice. Key concepts analyzed encompass jurisdictional sovereignty, governance regimes, rights frameworks, international law, and geo-economic equilibriums. In exploring these facets, the study combines doctrinal analysis of legal complexities with case studies assessing recent regulatory and taxation initiatives targeting technology firms. Thereby, contextual insights inform suggested approaches balancing control with openness through blending scope-based rules with effects-based standards around liability [5].

## II. Methodology

This study primarily employs a qualitative research approach, aiming to delve deep into the multifaceted aspects of digital borders, jurisdictional challenges, and governance paradigms. Qualitative research allows for a nuanced understanding of the intricate legal and policy frameworks needed to navigate the borderless nature of digital trade. The research design is grounded in the exploration of existing debates and scholarly discourse to develop comprehensive insights and recommendations for reimagining digital borders [6].

The data collection process involves multiple stages and diverse sources. Firstly, a thorough review of existing literature, legal documents, policy papers, and academic discussions forms the foundation. This includes a meticulous examination of doctrinal analyses, comparative studies, and relevant publications addressing jurisdictional complexities in the digital realm. Additionally, interviews or discussions with legal experts, policymakers, and industry stakeholders might be conducted to gather insights into real-world implications and perspectives [7].

The collected data undergoes qualitative analysis methods. The doctrinal research approach aids in understanding legal principles, precedents, and existing laws related to digital borders and jurisdiction. Grounded theory is employed to systematically analyze and derive themes, patterns, and emerging concepts from the amassed data. This iterative process involves constant comparison and refinement to construct a comprehensive understanding of the regulatory landscape. The tools utilized encompass a wide array of scholarly databases, legal repositories, and digital platforms to access and analyze literature, laws, treaties, and policy documents relevant to the study. Software for qualitative analysis might be employed to manage and categorize data effectively [8].

The adoption of qualitative research, doctrinal research, and grounded theory is substantiated by the intricate nature of the subject matter. These methodologies enable a comprehensive exploration of diverse perspectives, legal nuances, and evolving paradigms in digital governance. The qualitative approach allows for in-depth exploration and understanding of complex issues beyond quantitative metrics. The doctrinal research approach facilitates the examination of existing laws and doctrines, providing a foundation for analysis. Grounded theory ensures a systematic and rigorous analysis, allowing for the emergence of new theoretical insights rooted in empirical data [9].

## III. Results

The study reveals an evident consensus around the need for updated regulatory paradigms attuned to the borderless nature of digital trade, transcending traditional inter-jurisdictional limitations. Clear patterns indicate rising tensions between expansive extraterritorial claims by powerful states and accusations of trade protectionism. Analysis shows concentration of influence among platform giants coupled with legal ambiguity enables detrimental outcomes like tax avoidance, necessitating cooperative solutions centered on collective rights. Doctrinal assessments highlight principles-based extraterritoriality in law application can balance control with innovation across digital borders. Scope-based rules demarcating platform-specific duties per their societal impacts alongside effects-based liability standards emerge as potential middle paths. Suggestive models advocate collaborative rule-setting modalities like multi-stakeholder dialogues for norm building [10].

However, constructing appropriate platforms remains rife with ideological clashes, power imbalances and enforcement limitations given voluntary compliance dependencies, impeding global regulatory coherence. Nonetheless, reimagining digital borders underscores shared struggles of balancing interests, rights and responsibilities across man-made demarcations, physical or virtual. Therein lies scope for principled compromise - eschewing binaries of authoritarian control versus democratic freedoms by elevating user welfare centrally when designing oversight systems. The findings align with the core research questions assessing potential for re-envisioning digital borders supporting regulatory clarity. Proposed approaches blending scope and effects-based stipulations offer standardization pathways. Emphasized collaborative modalities provide modalities fostering stakeholder inclusion when systematizing liability and taxation norms digitally. Suggested extraterritoriality mechanisms enable mitigating concentration risks by allowing localized policy autonomy simultaneously [11].

However, insights also reveal difficulties in constructing international conventions given enforcement dependencies on voluntary state compliance. Power dynamics and data sovereignty reluctance introduce hurdles for global accords. Addressing risks of capital flight from unilateral taxation requires further examination on stabilizing capital flows via transparency measures dissociating residency from tax liabilities. But emphasis on human welfare over locational considerations signals potential for balancing control with connectivity. The findings indicate rethinking digital borders, essentially virtual delineations of rights and duties, warrants consistent alignment to their physical counterparts - upholding civil liberties, equitable access and collective advancement when structuring technologized economic systems, locally or globally. Reinforcing those principles calls for cooperation trumping unilateral interests, befitting our interconnected reality [12].

## IV. Discussion

Borders, whether physical or digital, encapsulate more than mere geographical demarcations; they embody the complex interplay of power dynamics and technological frameworks that define governance and control. While physical borders delineate governmental jurisdictions, digital borders evolve as fluid, adaptive constructs shaped by historical contexts and power struggles. These virtual demarcations, existing within the sphere of national sovereignty, regulate the movement of data and individuals across shifting technological landscapes. The digital border represents a dynamic fusion of technology and governance, navigating the tensions between inclusion and exclusion in an interconnected world, thereby influencing the interactions within and beyond these sovereign boundaries [13].

In today's interconnected world, the significance of digital borders cannot be understated. While the global village has enabled seamless communication and cultural exchange, digital borders delineate the virtual territories where regulations, policies, and restrictions come into play. These boundaries govern data flow, privacy, cybersecurity, and access to information, influencing how individuals interact and businesses operate across the digital landscape. Digital borders highlight the complexities of balancing connectivity with regulatory frameworks, prompting discussions on data sovereignty, online freedom, and the need for international cooperation to navigate and harmonize these diverse digital frontiers [14].

The rise of Digital Economy Agreements (DEAs) marks a significant shift in trade dynamics, transcending traditional digital trade scopes to embrace a more expansive, digitally innovative landscape. Unlike earlier FTAs, DEAs don't merely regulate digitized trade; they strive for a more comprehensive digitalized framework, leveraging technologies like block-chain to facilitate seamless transactions. The exemplar, the Digital Economy Partnership Agreement (DEPA), encapsulates this ethos by fostering end-to-end digital trade while emphasizing trust-building measures through paperless systems, e-payments, and authentication mechanisms. DEAs serve as pivotal platforms fostering collaborative rule design across a spectrum of digital economy facets—from AI and FinTech to regulatory sandboxes and small business inclusion—reflecting a robust commitment to shaping a progressive and inclusive digital future [15].

The fluidity of data, services, and transactions transcending conventional borders showcases the evolving landscape of global interconnectedness. Data flows, surpassing physical boundaries, act as a catalyst for economic growth and inclusion, especially for developing nations integrating into the digital economy. However, this unbounded movement introduces complexities, exposing information to diverse regulatory landscapes and potential risks. Varied approaches to data protection, national security concerns, and censorship further complicate this fluidity, emphasizing the necessity for cohesive global governance. Bridging these disparities is imperative to harness the full potential of cross-border data flows, fostering equitable participation and sustainable development across borders [16].

Jurisdiction in the digital economy presents a labyrinth of complexities rooted in the clash between traditional legal frameworks and the borderless nature of the internet. The crux lies in the inherent limitations of national boundaries against the limitless reach of online platforms. Issues spanning data privacy, cybercrime, and content regulation grapple with the question of authority: which state holds the power to legislate, enforce, or penalize in a space transcending borders? Adapting outdated legal concepts faces hurdles within the framework of nation-state governance, constraining effective regulation in a landscape evolving far more swiftly than the centuries-old political systems attempting to contain it [17].

Navigating jurisdictional challenges in the digital economy presents a multifaceted hurdle stemming from divergent legal, moral, and cultural landscapes across nations. The intricate web of varying standards complicates cohesive regulation, impeding swift progress and hampering effective international cooperation. This diversity creates a regulatory minefield where self-interest often impedes consensus-building efforts, as witnessed in recent clashes between governments and tech giants. This discord underscores the limitations of relying solely on legal frameworks, underscoring the imperative for a broader approach encompassing active political citizenship and technological advancements geared toward enhancing user agency and privacy protection [18].

Governments encounter formidable challenges in enforcing regulations and laws across digital boundaries due to the intricate and borderless nature of transformative technologies. The rapid evolution and convergence of services within these technologies defy traditional regulatory categories, complicating jurisdictional oversight. Varying court rulings on platforms like Airbnb and Uber underscore the struggle to establish consistent frameworks, exemplifying the ambiguity in classification. Assigning liability for mishaps involving AI-controlled systems, such as self-driving cars or algorithmic decisions, presents another hurdle, further compounded by the complexities of reinforcement learning. Additionally, decentralized technologies like block-chain pose unique hurdles as cyber incidents occur outside conventional accountability structures, as seen in the DAO hack. The absence of unified global regulatory standards exacerbates these complexities, hindering effective enforcement measures and leaving critical aspects of liability and oversight unresolved in the digital realm [19].

Jurisdictional conflicts in multinational digital transactions showcase intricate legal complexities. For instance, cases involving data breaches across borders pose challenges in determining applicable laws and responsibilities, given the territorial storage of data. Instances where multinational corporations operate across diverse legal systems create ambiguity in identifying responsible entities and the governing law. Cybercrime investigations face hurdles due to limitations in traditional policing methods, complicating the assessment of cyber threats' impacts. Additionally, clashes arise when nations attempt to expand jurisdiction extraterritorially or impose national laws on global digital platforms, conflicting with cyberspace's decentralized nature. Resolving these conflicts necessitates a delicate balance between national and international laws, requiring a universal human rights approach for potential conflict resolution [20].

The absence of distinct digital borders profoundly impacts governance structures and policy-making by complicating jurisdictional delineation, regulatory frameworks, and enforcement mechanisms. In a borderless digital landscape, determining legal jurisdictions for data governance, privacy protection, and law enforcement becomes intricate, leading to ambiguity in accountability and oversight.

This lack of clarity hampers the formulation of cohesive policies that can effectively regulate cross-border data flows, cybersecurity, and digital rights, fostering challenges in aligning national laws with the transnational nature of digital interactions. Consequently, the absence of clear digital borders demands innovative international cooperation and frameworks to navigate the complexities of governance in an interconnected, boundary less digital realm [21].

International organizations play a pivotal role in shaping frameworks for digital governance by navigating the starkly contrasting visions of authoritarian control and democratic principles. Entities like the International Telecommunication Union (ITU) grapple with the diverse agendas of nations, attempting to harmonize standards and protocols. While China champions its cyber sovereignty model, leveraging multilateral processes to advocate control over internet access, organizations like the ITU become battlegrounds for ideological clashes. Conversely, the European Union's GDPR stands as a democratic benchmark, asserting user rights globally. International organizations serve as arenas where competing ideologies converge, striving to bridge the gap between authoritarian control and democratic freedoms, fostering discussions and potential compromises for a cohesive, globally applicable framework [22].

Redefining digital borders requires a holistic approach that centers on human rights and accountability. A novel framework should integrate international cooperation, establishing clear ethical guidelines, and robust oversight mechanisms. This includes a multilateral dialogue to develop comprehensive regulations addressing the use, deployment, and impact of digital technologies in border governance. Emphasizing transparency, accountability, and rights-based protocols is crucial. Incorporating migrant and refugee voices in policy formation, ensuring procedural fairness, and conducting regular audits to assess technology's ethical implications are pivotal steps. Innovative strategies should prioritize safeguarding privacy, preventing discrimination, and empowering oversight bodies to ensure technology serves humane migration management while respecting fundamental rights [23].

Implementing frameworks for international law on a global scale presents multifaceted challenges rooted in geopolitical realities and structural limitations. The absence of a centralized authority fosters diverse legal systems and varying interpretations, complicating efforts to establish uniform laws. Enforcement remains a significant hurdle as it heavily relies on voluntary compliance, constrained further by power dynamics and political interests among states. Conflicting ideologies and power struggles often impede critical resolutions, hampering the effective application of international law in high-stakes scenarios. Additionally, cultural diversity fuels differing perspectives, potentially obstructing the establishment of universally accepted norms. These complexities underscore the formidable task of fostering global adherence to international legal frameworks, demanding sustained efforts to navigate political, cultural, and enforcement obstacles [24].

Rethinking digital borders introduces profound legal and ethical considerations in the context of the digital transformation. As nations navigate the evolution of technological landscapes, the delineation of digital borders raises critical questions about data sovereignty, privacy, and jurisdictional authority. The ethical implications of redefining these borders entail balancing national interests with global interconnectivity, ensuring data protection, fostering international cooperation, and upholding individual rights across virtual spaces. Legal frameworks must adapt to address cross-border data flows, cybersecurity challenges, and ethical use of emerging technologies, demanding collaborative efforts to establish robust regulations while respecting human rights and sovereignty in this interconnected digital realm [25].

Understanding the socio-economic impact on stakeholders—businesses, consumers, and governments—reveals a multifaceted landscape of interconnected influences. For businesses, these insights are pivotal in deciphering consumer behaviors shaped by income levels, education, and cultural affiliations, empowering them to innovate and tailor offerings effectively. Consumers benefit as their needs and aspirations align with products and services, fostering inclusivity and improved access. Governments, armed with this understanding, can enact policies that bolster economic stability, employment opportunities, and equitable resource distribution, thereby nurturing a thriving socio-economic ecosystem benefiting all stakeholders involved [26].

In e-commerce, digital border challenges manifest in varied sectors, particularly concerning data privacy. For instance, financial services face hurdles when transferring customer financial data across international borders due to differing data protection regulations. Healthcare encounters obstacles in sharing patient information for telemedicine services, limited by jurisdictional data storage requirements. Similarly, the tech industry faces constraints with cloud data storage due to regulations mandating local data hosting. These challenges highlight the complexities surrounding data transfer and storage, illustrating the need for harmonized regulations to facilitate secure cross-border data flow while safeguarding privacy across diverse sectors [27].

The evolution of digital borders is likely to witness a surge in collaborative frameworks among international entities like the Universal Postal Union (UPU) and the World Customs Organization (WCO), fostering seamless data exchange and standardized protocols. Anticipated trends include heightened integration of AI-driven risk assessment tools, enabling expedited clearance for legitimate e-commerce shipments while intensifying scrutiny on illicit trade activities. Enhanced connectivity between agencies and e-commerce stakeholders, as seen in COAC and HSI working groups, will facilitate real-time information sharing, bolstering efforts against counterfeiting and piracy. Moreover, the convergence of 21st Century Customs Framework (21CCF) principles with emerging technologies is poised to streamline processes, fostering a more resilient and efficient global trade landscape [28].

Across governments worldwide, these technologies are woven into various sectors to optimize governance and service provision. Artificial intelligence (AI), machine learning, and algorithms are transforming administrative tasks, streamlining processes, and aiding decision-making in departments handling massive datasets like healthcare and finance. Block-chain and distributed ledgers are revolutionizing identity verification, supply chain management, and even voting systems, ensuring secure and transparent transactions within governmental operations. Drones, robots, wearables, and the Internet of Things enhance surveillance, disaster response, and infrastructure maintenance. Additionally, governments leverage data visualization, simulation, and big data analytics to extract insights, predict trends, and enhance policy-making across the global economy, fostering innovation and efficient resource allocation for societal advancement [29].

## Conclusion

This study highlights why reimagining digital borders is imperative for ethical, equitable governance attuned to the borderless digital economy. With rising data flows, platforms, and digital trade reshaping business models, outdated inter-jurisdictional paradigms struggle with legal authority, accountability, and enforcement in virtual interactions spanning nations. The analysis reveals concentrated power among technology giants coupled with regulatory ambiguity currently enables detrimental outcomes like tax avoidance. Attempts at extraterritorial jurisdiction risk protectionism accusations amidst unilateral digital taxation efforts. These challenges underscore the need for multilateral cooperation balancing rights, control, and welfare.

Emerging evidence indicates blending scope-based regulations pegged to risk levels alongside effects-based liability holds promise for standardizing duties without prescriptive control. Multi-stakeholder dialogues offer inclusive rule-setting pathways. Principles-based extraterritoriality in law would enable localized policy autonomy while addressing concentration issues collectively. However, forging international accords faces ideological divergences, enforcement hurdles and data sovereignty barriers, demanding nuanced balancing of interests. Power imbalances also necessitate transparency mechanisms shielding bilateral agreements from domination. Nonetheless, elevating user welfare signals common ground.

Future research should further examine stabilizing mechanisms for human-centered regulatory systems resilient against capital flight risks alongside exploring decentralized governance technologies like block-chain for bridging jurisdictional divides virtually. International organizations would benefit from appraising existing accords for digitally translatable principles upholding rights and development commitments universally. This study posits rethinking digital borders involves reinforcing corresponding principles physical spaces avail — equitable access, civil liberties, transparency, non-discrimination and collective advancement. Cooperating to institute just governance befitting an interconnected economy should override individualist unilateralism. Therein lies hope for an empowering digital transformation if framed thus.

## References

1. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015. https://doi.org/10.3390/s23198015
2. Hane-Weijman, E. (2021). Skill matching and mismatching: Labour market trajectories of redundant manufacturing workers. *Geografiska Annaler: Series B, Human Geography*, *103*(1), 21-38. https://doi.org/10.1080/04353684.2021.1884497
3. Lazarova, M., Caligiuri, P., Collings, D. G., & De Cieri, H. (2023). Global work in a rapidly changing world: Implications for MNEs and individuals. *Journal of World Business*, *58*(1), 101365. https://doi.org/10.1016/j.jwb.2022.101365
4. Li, L. (2022). Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond. *Information Systems Frontiers*. Advance online publication. https://doi.org/10.1007/s10796-022-10308-y
5. Martínez-Peláez, R., Ochoa-Brust, A., Rivera, S., Félix, V. G., Ostos, R., Brito, H., Félix, R. A., & Mena, L. J. (2023). Role of Digital Transformation for Achieving Sustainability: Mediated Role of Stakeholders, Key Capabilities, and Technology. *Sustainability*, *15*(14), 11221. https://doi.org/10.3390/su151411221
6. Raposo, V. L., & Du, L. (2023). Facial recognition technology: Is it ready to be used in public health surveillance? *International Data Privacy Law*, ipad021. https://doi.org/10.1093/idpl/ipad021
7. Stahl, B. C., Antoniou, J., Bhalla, N., et al. (2023). A systematic review of artificial intelligence impact assessments. *Artificial Intelligence Review*, *56*, 12799–12831. https://doi.org/10.1007/s10462-023-10420-8
8. Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, 12(24), 12679. https://doi.org/10.3390/app122412679
9. Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. *Smart Cities*, *6*(1), 586-613. https://doi.org/10.3390/smartcities6010027
10. Power, D. J., Heavin, C., & O’Connor, Y. (2021). Balancing privacy rights and surveillance analytics: A decision process guide. *Journal of Business Analytics*, *4*(2), 155-170. https://doi.org/10.1080/2573234X.2021.1920856
11. Kemppainen, L., Kemppainen, T., Kouvonen, A., Shin, Y.-K., Lilja, E., Vehko, T., & Kuusio, H. (2023). Electronic identification (e-ID) as a socio-technical system moderating migrants' access to essential public services – The case of Finland. *Government Information Quarterly*, 40(4), 101839. https://doi.org/10.1016/j.giq.2023.101839
12. Campbell-Verduyn, M. (Ed.). (2017). *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (1st ed.). Routledge. https://doi.org/10.4324/9781315211909

13. Banaeian Far, S., Imani Rad, A., & Rajabzadeh Asaar, M. (2023). Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse. *Data Science and Management*, *6*(3), 183-197. https://doi.org/10.1016/j.dsm.2023.06.002
14. Juhro, S. M. (2022). *Central Banking Practices in the Digital Era: Salient Challenges, Lessons, and Implications*. (Eds.), (pp. 13). Springer, Singapore. https://doi.org/10.1007/978-981-16-6827-2_13
15. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267
16. Lu, S., He, G., & Yan, H. (2022). Research on the Impact of Technological Finance on Financial Stability: Based on the Perspective of High-Quality Economic Growth. *Complexity in Financial Markets*, Volume 2022, Article ID 2552520. https://doi.org/10.1155/2022/2552520
17. Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., Favaro, M., & Persi Paoli, G. (2020). *The Future of Cybercrime in Light of Technology Developments*. RAND Corporation. Retrieved from www.rand.org/t/RRA137-1
18. Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., Favaro, M., & Persi Paoli, G. (2020). *The Future of Cybercrime in Light of Technology Developments*. RAND Corporation. Retrieved from www.rand.org/t/RRA137-1
19. Ferrag, M. A., Maglaras, L., & Benbouzid, M. (2023). Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. *Journal of Sensors, Actuators, and Networks*, 12(3), 40. https://doi.org/10.3390/jsan12030040
20. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., Patsakis, C. (2022). SoK: Cross-Border Criminal Investigations and Digital Evidence. *Journal of Cybersecurity*, 8(1), tyac014. https://doi.org/10.1093/cybsec/tyac014
21. Abraham, K. S. (2020). Incomplete Insurance Coverage. *Connecticut Insurance Law Journal*, *26*. Retrieved from https://cilj.law.uconn.edu/wp-content/uploads/sites/2520/2021/02/Abraham-Final-PDF.pdf
22. Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, 178, 121562. https://doi.org/10.1016/j.techfore.2022.121562
23. Biener, C., Eling, M., & Wirfs, J. H. (2014). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice*, *39*(1), 1-28. Retrieved from https://www.internationalinsurance.org/sites/default/files/2018-03/Insurability%20of%20Cyber%20Risk.pdf
24. Baker, T., & Shortland, A. (2023). Insurance and enterprise: Cyber insurance for ransomware. *Geneva Papers on Risk and Insurance: Issues and Practice*, 48, 275–299. https://doi.org/10.1057/s41288-022-00281-7
25. Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, 22(3), 737-748. https://doi.org/10.1007/s10207-023-00660-8
26. Balawejder, B., Dankiewicz, R., Ostrowska-Dankiewicz, A., & Tomczyk, T. (2019). The role of insurance in cyber risk management in enterprises. *Humanities and Social Sciences*, *26*(4/2019), 19-32. https://doi.org/10.7862/rz.2019.hss.33
27. Andersson, F., Jordahl, H., & Josephson, J. (2019). Outsourcing Public Services: Contractibility, Cost, and Quality. *CESifo Economic Studies*, 65(4), 349–372.

https://doi.org/10.1093/cesifo/ifz009

28. Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5), e10059. https://doi.org/10.2196/10059
29. Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice, 6*(2), 146-159. https://doi.org/10.1080/25741292.2023.2199960