DIGITAL LAW NEXUS 2025

Conference Proceedings

Published by

Uzbek Journal of Law and Digital Policy

EDITORIAL TEAM

Republic of Uzbekistan

DIGITAL LAW NEXUS 2025

Edited by

Dr. Naeem AllahRakha

IRSHAD

Table of Contents

A Concept of Center of Excellence in Cybernetic Law

Prof. Said Gulyamov **(DSc)**
Tashkent State University of Law

The concept of establishing a Center of Excellence in Cybernetic Law based on the existing Cyber Law Department at Tashkent State University of Law. The study analyzes institutional models of international cyber law centers, opportunities for integration into international research networks, functional components, and mechanisms to ensure the center's sustainability. The paper proposes a multilevel structure with research, educational, and consulting components; a public–private partnership funding model; a "digital ambassadors" program; and the creation of a digital platform for expert collaboration. The research findings demonstrate that this concept can transform Uzbekistan into a regional hub of expertise in cyber law.

Modern digital transformation of society and the economy creates unprecedented challenges for the legal system and legal education. A world where algorithms make decisions and cyberattacks pose threats to national security requires a fundamentally new approach to training lawyers and developing legal science (BARANOV et al., 2024). Research shows a critical shortage of specialists capable of working effectively at the intersection of law and technology: less than 8% of European law schools teach algorithm regulation, 88% of graduates acknowledge unpreparedness for digital era challenges, 93% of legal departments in technology companies cannot find technically competent lawyers, and EU law enforcement agencies face a 76% staff shortage for cybercrime investigations. In Uzbekistan, as in many other countries, there is an urgent need to form an ecosystem that could ensure the training of a new generation of lawyers with competencies to work in the digital economy (Enkova et al., 2021).

The study is based on comparative analysis of existing models of centers of excellence in cyber law across various jurisdictions. Structural and functional features of the European Cybersecurity Competence Centre (ECCC) in Bucharest, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, and Berkeley Center for Law & Technology (BCLT) in the USA were examined. The analysis included studying the organizational and legal forms of the centers, funding models, mechanisms of interaction with partners and stakeholders, and evaluation of their performance effectiveness. To enhance the validity of conclusions, a systematic analysis of scientific literature on institutional development of academic centers and knowledge hubs was conducted using Ostrom's Institutional Analysis and Development Framework, which revealed key factors for sustainability of such centers and enabled adaptation of best practices to the Uzbekistan context.

An inductive research method was applied to generalize the practical experience of the Cyber Law Department at Tashkent State University of Law and to

formulate a concept for scaling up to the level of a regional center of excellence. This approach allowed for consideration of local context specifics and available resources, which is critical for ensuring the realism and feasibility of the proposed concept. The methodology included detailed analysis of educational programs, research projects, and international partnerships of the department for qualitative data analysis. Special attention was paid to evaluating the triadic methodology of competence formation used at the department and the possibilities for scaling it within the Center. The obtained results were validated through discussions with international experts in cyber law and representatives of potential Center partners (Williamson et al., 2002).

The research resulted in the development of a comprehensive concept for a Center of Excellence in Cybernetic Law, based on scaling the existing ecosystem of the Cyber Law Department at Tashkent State University of Law. The Center's structure includes three interconnected components: an educational consortium, a research hub, and a consulting center. The educational consortium represents a network of cyber law educational programs at various levels, implemented in partnership with leading foreign universities. An important element of the educational consortium is a system of credit transfer and mutual recognition of qualifications, which ensures academic mobility and access to diverse expertise. Educational programs are built on a triadic methodology of competence formation, including writing structured analytical essays, creating compendiums with specific implementation proposals, and completing internships in partner organizations.

The Center's research hub will focus on developing four key areas: legal aspects of cybersecurity, regulation of artificial intelligence, digital rights, and legal support for the digital economy. The organizational structure of the research hub includes thematic research groups uniting scholars from different countries, a scientific laboratory for legal analysis of cyber threats equipped with specialized software for monitoring and analyzing cyber incidents, and the editorial office of the scientific journal "Digital Law Review". An important element of the Center's research activities is the development of analytical materials for government authorities, international organizations, and businesses. Currently, the Cyber Law Department already demonstrates high publication activity: 5+ articles in Scopus-indexed journals, 2+ in Web of Science, 2+ in Springer publications, and 5 monographs co-authored with international partners during the current academic year. Scaling research activities within the Center involves expanding the international network of coauthors and creating mechanisms for grant support of joint research projects (Garov et al., 2013).

The consulting center will become a practice-oriented component of the Center, providing connection with the real sector and developing expert potential. The structure of the consulting center includes specialized units in key areas: cybersecurity consulting, legal support for digital transformation, regulatory expertise in digital technology regulation, and training programs for practicing specialists. The consulting center will operate on a social entrepreneurship model, ensuring sustainable funding for the Center's activities as a whole. Key clients of the

consulting center will include government agencies responsible for digital transformation and cybersecurity, technology companies, banks and financial institutions, and law enforcement agencies. The consulting center will also implement a "digital ambassadors" program, under which trained Center experts will conduct educational events and consultations in countries of the region, contributing to the dissemination of best practices in the legal regulation of digital technologies.

The Center will be managed through a balanced structure including a Supervisory Board of representatives from partner universities, an Executive Director, an Academic Council, and an International Advisory Board of global experts. This management model will ensure consideration of all stakeholders' interests and high quality of decision-making. The Center's financial sustainability is ensured through diversification of funding sources: basic state funding, grants from international organizations (EU, World Bank, UNDP), income from consulting activities and educational programs, sponsorship support from technology companies, and the creation of an endowment fund. A roadmap has been developed for the Center's institutionalization, providing for three stages: formation of the legal framework and organizational structure (2025-2026), development of educational programs and research projects (2026-2027), scaling activities and achieving full functionality (2027-2028). Specific performance indicators are provided for each stage to assess the progress of concept implementation.

An important component of the concept is the creation of the Center's digital platform, providing remote interaction of experts, access to educational resources and research materials. The platform is being developed based on international interoperability standards and includes learning management systems (Moodle), research data management (Dataverse), online event hosting (BigBlueButton), and collaborative document work (GitLab). The Center's digital platform will integrate with existing national information systems in education and science, as well as with international databases and repositories. Platform security is ensured through the implementation of a multi-level protection system and regular security audits. The digital platform is a key tool for scaling the Center's activities and ensuring its accessibility to a wide range of users, including partners from other countries in the region.

Analysis of the legal aspects of establishing the Center showed the need to develop a special legal regime ensuring flexibility in management, international mobility of staff and students, intellectual property protection, and efficient use of resources. As a model, it is proposed to use the experience of creating international scientific and educational centers, such as the Skolkovo Institute of Science and Technology in Russia or Nazarbayev University in Kazakhstan, with adaptation to the specifics of Uzbekistan. The legal status of the Center can be established in a special resolution of the Cabinet of Ministers of the Republic of Uzbekistan, defining the features of its functioning, including tax benefits, simplified procedures for attracting foreign specialists, public-private partnership mechanisms, and procedures for participation in international projects. For effective integration into the international

scientific and educational space, the Center needs to ensure compliance with international standards of quality and transparency, such as the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG) and the principles of the Berlin Declaration on Open Access to Scientific Knowledge.

The proposed concept of a Center of Excellence in Cybernetic Law represents an innovative approach to the development of legal education and science in the context of digital transformation. A key advantage of the concept is its evolutionary nature: the Center is created not from scratch, but as a scaling of the existing ecosystem of the Cyber Law Department at Tashkent State University of Law, which increases the realism of the project and reduces its implementation time. Another important advantage is the integrated approach combining educational, research, and consulting components, which allows for a synergistic effect and long-term sustainability of the Center. However, potential challenges in implementing the concept should also be considered, among which are insufficient qualified personnel, bureaucratic barriers, competition with existing international centers, and issues of sustainable funding. To overcome these challenges, the concept provides special mechanisms: a targeted training program for specialists in leading global centers, creation of a special legal regime for the Center, focus on regional specifics and unique competencies, diversification of income sources, and establishment of an endowment fund.

Comparative analysis of the proposed concept with similar initiatives in other countries shows that the Center of Excellence in Cybernetic Law has the potential to become a unique model for developing countries seeking to build legal infrastructure for the digital economy. Unlike most existing centers, which focus primarily on educational or research functions, the proposed concept provides a comprehensive approach with an emphasis on practical application of knowledge through the consulting component. This approach is particularly relevant for countries with developing economies, where there is an acute need for expertise in forming the legal framework for digital transformation. Moreover, an important aspect of the concept is its regional dimension – the Center is positioned as a hub for Central Asian countries, which corresponds to Uzbekistan's strategic priorities for strengthening regional cooperation and integration.

The conducted research confirms the relevance and feasibility of the concept of a Center of Excellence in Cybernetic Law based on the existing Cyber Law Department at Tashkent State University of Law. The proposed multi-level structure with research, educational, and consulting components creates a foundation for transforming Uzbekistan into a regional hub of expertise in cyber law. The public-private partnership model for funding, the "digital ambassadors" program, and the creation of a digital platform for expert interaction ensure the sustainability and scalability of the Center. Expected effects from implementing the concept include increased scientific productivity in digital law, attraction of international grants and investments, improved quality of legislation in the digital sphere, and formation of a

new generation of specialists capable of working effectively at the intersection of law and technology (Susskind & Susskind, 2015).

For successful implementation of the concept, it is necessary to ensure coordination of efforts among various stakeholders: government bodies responsible for digital transformation, education and science; international organizations and foreign partners; technology companies and financial institutions. It is also important to develop a detailed implementation plan that includes specific performance indicators at each stage of concept realization. Creating a Center of Excellence in Cybernetic Law can become a model for developing other innovative educational and scientific initiatives in Uzbekistan, demonstrating the effectiveness of an integrated approach to building competencies in strategically important areas. In the future, the Center can also become a platform for regional dialogue on issues of legal regulation of digital technologies, contributing to the harmonization of legislation in Central Asian countries and their integration into the global digital space.

Bibliography

BARANOV, O., KOSTENKO, O., DUBNIAK, M., & GOLOVKO, O. (2024). *DIGITAL TRANSFORMATIONS OF SOCIETY: PROBLEMS OF LAW*. RS Global Sp. z O.O. https://doi.org/10.31435/rsglobal/057

Enkova, E., Ershova, I., & Trofimova, E. (2021). Application of digital technologies in the training of lawyers for the business sector. *SHS Web of Conferences*, *106*, 03006. https://doi.org/10.1051/shsconf/202110603006

Garov, S., Dencheva, M., & Kisselova, A. (2013). ORGANIZATIONAL STRUCTURE OF RESEARCH PROJECT ACTIVITIES PERFORMED AT MEDICAL UNIVERSITIES IN BULGARIA. *Journal of IMAB - Annual Proceeding (Scientific Papers)*, *19*(4), 340–344. https://doi.org/10.5272/jimab.2013194.340

Susskind, R., & Susskind, D. (2015). *The Future of the Professions*. Oxford University Press. https://doi.org/10.1093/oso/9780198713395.001.0001

Williamson, K., Burstein, F., & McKemmish, S. (2002). The two major traditions of research. In *Research Methods for Students, Academics and Professionals* (pp. 25–47). Elsevier. https://doi.org/10.1016/B978-1-876938-42-0.50009-5

Cross-Border Data Protection and Exchange in EV-CRM Value Chains

Dr. Naeem AllahRakha
Tashkent State University of Law

This article examines legal mechanisms for cross-border data transfer in electric vehicle (EV) value chains and customer relationship management (CRM) systems. It analyzes legal frameworks for cross-border data transfer, jurisdictional conflicts in data processing, protection standards in the automotive industry, and the balance between data localization and free information flow. The research proposes recommendations for Uzbekistan, including developing legal mechanisms for participation in international data chains, creating special legal regimes for technological projects, implementing data protection standards, and concluding bilateral agreements. The results demonstrate Uzbekistan's potential for integration into global value chains.

The digitalization of the automotive industry, particularly in electric vehicle (EV) and customer relationship management (CRM) sectors, generates unprecedented volumes of data circulating across national borders. A modern electric vehicle generates up to 25 gigabytes of data per hour, which is used to optimize production, manage supply chains, improve user experience, and develop innovative services. The integration of this data with CRM systems forms complex cross-border value chains involving manufacturers, component suppliers, service companies, and consumers from different jurisdictions. According to research by the Institute of Value Chains (New Delhi, India), the volume of data transferred within global EV-CRM chains increased from 1.7 petabytes in 2020 to 8.4 petabytes in 2023, with projected growth to 27 petabytes by 2026 (Llopis-Albert et al., 2021).

This intensive cross-border circulation of data faces growing fragmentation of data protection regimes: while only 35 countries had specialized data protection legislation in 2010, by 2023 this number reached 137, with many jurisdictions imposing restrictions on cross-border transfers. In these conditions, legal mechanisms that balance data protection with free cross-border exchange become a critical factor for integration into global value chains. For Uzbekistan, which aims to develop its national automotive industry and attract investment in electric vehicle production, an effective legal framework for cross-border data transfer represents a strategic interest in the context of integration into global high-tech value chains.

The analysis of legal mechanisms for cross-border data transfer in EV-CRM value chains revealed the formation of three main regulatory models. The first model "adequacy approach," implemented in the EU through an adequacy decision mechanism, recognizing the equivalence of data protection levels in third countries. The second model "contractualization approach," dominant in the USA and several Asian countries, based on the use of contractual mechanisms (standard contractual clauses, binding corporate rules) to ensure protection during data transfer. The third model “localization approach," characteristic of China, Russia, and some developing countries, establishing requirements for storing certain types of data on national territory. Each of these models creates specific challenges for global data chains in the automotive industry.

For example, electric vehicle manufacturers exporting to the EU must comply with GDPR requirements, which necessitates substantial adaptation of CRM systems

and data processing procedures (Williamson & Prybutok, 2024). The study showed that the most successful automakers apply a multi-level compliance strategy combining various legal mechanisms. Tesla, for instance, uses a combination of standard contractual clauses, binding corporate rules, and Privacy Shield 2.0 certifications to ensure the legality of cross-border data flows between the USA, EU, and Asia. Similarly, Volkswagen Group has implemented a global data management system based on "privacy by design" and a differentiated approach to various data categories, with separate protocols for customers' personal data, vehicle technical data, and aggregated analytical data.

Jurisdictional conflicts in data processing within international supply chains present a serious challenge for the automotive industry, especially in the electric vehicle sector, where data plays a critical role in optimizing production, battery management, and service development. The study identified four main types of jurisdictional conflicts. The first type extraterritorial effects of national legislation, when requirements of one jurisdiction (such as EU GDPR) extend to data processing beyond its borders. The second type conflicting localization requirements, when different countries require storage of the same data on their territory. The third type – conflicts in defining the legal status of data, when some jurisdictions consider certain data as personal, while others classify it as nonpersonal or industrial. The fourth type differences in procedural requirements, such as consent forms, retention periods, and reporting requirements (Jeong et al., 2024).

These conflicts create significant legal and operational risks for companies in EV-CRM chains. For example, Chinese manufacturer BYD, when entering the European market, faced the need to restructure its data flows due to conflicts between PIPL requirements (requiring Chinese regulator permission for exporting certain data) and GDPR (requiring the possibility to transfer data to the subject upon request). To resolve such conflicts, companies develop complex legal constructs, including creating local data centers in key jurisdictions, structuring corporate architecture considering regulatory requirements, and developing specialized inter-corporate data transfer agreements.

Data protection standards in the automotive industry are actively evolving, reflecting the unique characteristics of electric vehicle data and integrated CRM systems. The research identified the formation of three levels of standardization. At the international level, key roles are played by ISO/SAE 21434 (automotive systems cybersecurity), ISO 27701 (personal data management), and UNECE WP.29 recommendations on cybersecurity and data protection in vehicles. At the regional level, industry standards such as VDA TISAX in Europe (information security standard for the automotive industry) and Auto-ISAC in the USA (platform for sharing information about cyber threats) are significant. At the corporate level, leading automakers develop their own standards, often exceeding regulatory requirements (Roy et al., 2022).

Notably, in the electric vehicle sector, special attention is paid to protecting battery-related data (technical parameters, charging data, telemetry), which is

considered critical for intellectual property and safety. The study showed that the most successful electric vehicle manufacturers, such as Tesla and BYD, apply a multi-level data protection model, differentiating requirements depending on data type, geographic location, and regulatory context. This approach allows balancing between compliance with various jurisdictional requirements and optimization of business processes. An important trend is the standardization of machine-to-machine data exchange (M2M) in electric vehicle ecosystems, including data exchange protocols between vehicles, charging stations, and service centers, which requires harmonization of technical and legal standards (Villa-Salazar et al., 2024).

The data localization and free information flow represents one of the central dilemmas of modern data regulation, especially relevant for global value chains in the automotive industry. The study identified three dominant approaches to this dilemma. The first approach "free flow priority," characteristic of Japan, Singapore, and New Zealand, minimizes restrictions on cross border data transfer and promotes international agreements on free data flow, such as the DFFT (Data Free Flow with Trust) initiative and the CPTPP agreement. The second approach "digital sovereignty," implemented by the EU, China, and Russia, establishes various forms of localization requirements and control mechanisms for cross-border data flows. The third approach "sectoral differentiation," applied in the USA, South Korea, and India, provides different regimes for different types of data and economic sectors (Taylor, 2020).

In the context of EV-CRM chains, these approaches create a complex regulatory landscape requiring companies to carefully structure data flows. For example, sales and customer data are often subject to stricter restrictions than technical data on vehicle performance. The study showed that successful electric vehicle manufacturers develop data architectures that consider various regulatory requirements: they localize the most sensitive data in the respective jurisdictions, create mechanisms for local processing with limited cross-border transfer, and implement technologies minimizing the need to transfer raw data such as federated learning and edge computing (Schäfer et al., 2023).

Based on the analysis of international experience, specific adaptation recommendations have been developed for Uzbekistan, aimed at creating an effective legal framework for participation in global EV-CRM data chains. The first recommendation involves developing legal mechanisms for participation in international data chains, including updating the Law "On Personal Data" with the introduction of detailed provisions on cross-border data transfer, corresponding to international standards but considering national specifics. A differentiated approach to various data categories is recommended, with stricter requirements for personal data and a more flexible regime for technical and industrial data (Comandè & Schneider, 2022).

The second recommendation is to create special legal regimes for international technological projects, including "regulatory sandboxes" and experimental legal regimes for the automotive industry, allowing testing of innovative approaches to data

exchange in a controlled environment. The third recommendation involves implementing data protection standards compatible with global requirements, including adaptation of international standards (ISO/SAE 21434, ISO 27701) to the national context and developing industry guidelines on data protection for the automotive industry. The fourth recommendation relates to concluding bilateral data protection agreements with major trading partners, including mechanisms for mutual recognition of data protection adequacy, which will facilitate the integration of Uzbek companies into global EV-CRM chains.

The expected effect from implementing the proposed recommendations includes integrating Uzbekistan into global high-tech value chains, increasing investment attractiveness for international technology companies, ensuring data security for citizens while developing the digital economy, and creating new highly qualified jobs. According to expert estimates, developing an effective legal framework for cross-border data transfer can increase foreign direct investment in high-tech sectors by 23-28% over five years and create an additional 15,000-20,000 jobs in sectors related to electric vehicle production and digital services.

The experience of countries such as Singapore, South Korea, and the UAE shows that creating legal certainty in the field of cross-border data transfer becomes a significant factor in attracting investments in high-tech industries. Notably, the effect of implementing the proposed recommendations is not limited to the automotive industry but extends to other sectors dependent on cross-border data exchange, including telecommunications, financial services, and logistics. It is important to consider potential challenges that Uzbekistan may face when implementing these recommendations, including the contradiction between localization requirements and international standards, technical limitations of infrastructure for big data processing, shortage of data management specialists, and risks of unauthorized access to sensitive data.

The analysis of legal mechanisms for cross-border data transfer in EV-CRM value chains reveals a fundamental contradiction between the need for free data exchange to develop innovations and global value chains and the necessity to protect national interests, personal data, and intellectual property. This contradiction is especially relevant for countries seeking to integrate into global high-tech chains, such as Uzbekistan. On one hand, an overly restrictive approach to cross-border data transfer can isolate the country from global innovation processes and limit access to international markets and technologies. On the other hand, excessive openness without adequate protection mechanisms can create threats to national security, citizens' privacy, and data sovereignty. The proposed recommendations aim to find an optimal balance between these opposing requirements, considering both international standards and best practices, as well as Uzbekistan's national specifics and strategic priorities.

It is important to note that implementing the proposed recommendations requires a comprehensive approach that goes beyond purely regulatory changes. The development of technical infrastructure for secure data processing and transfer is of

critical importance, including modern data centers, secure communication channels, and cybersecurity monitoring systems. Equally important is human capital development training specialists in data management, information security, international data law, and digital diplomacy. International cooperation also plays a key role, including active participation in global and regional initiatives for standardization and harmonization of approaches to data regulation. Only a combination of regulatory changes, technological development, investments in human capital, and international cooperation can ensure Uzbekistan's successful integration into global data chains and the digital economy.

Implementing these recommendations opens opportunities for strengthening Uzbekistan's position in high-tech sectors of the global economy, including electric vehicle production and digital services, attracting investments, and creating new jobs. A phased and adaptive approach is of key importance, considering both long-term strategic goals and the current level of digital infrastructure and competency development. Experience shows that the most successful countries in regulating cross-border data flows combine commitment to international standards with developing national competitive advantages and protecting strategic interests. Uzbekistan, with its strategic position at the intersection of various regions and traditions of balancing between different centers of influence, has the potential to create an innovative model for regulating cross-border data transfer, contributing to the sustainable development of the national digital economy and integration into global value chains.

Bibliography

Comandè, G., & Schneider, G. (2022). Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal*, *23*(4), 559–596. https://doi.org/10.1017/glj.2022.30

Jeong, J. H., Kim, C., & Jo, H. J. (2024). Three major challenges in the shift to electric vehicles: Industrial organization, industrial policy, and a just transition. *Sociology Compass*, *18*(5). https://doi.org/10.1111/soc4.13218

Llopis-Albert, C., Rubio, F., & Valero, F. (2021). Impact of digital transformation on the automotive industry. *Technological Forecasting and Social Change*, *162*, 120343. https://doi.org/10.1016/j.techfore.2020.120343

Roy, H., Roy, B. N., Hasanuzzaman, Md., Islam, Md. S., Abdel-Khalik, A. S., Hamad, M. S., & Ahmed, S. (2022). Global Advancements and Current Challenges of Electric Vehicle Batteries and Their Prospects: A Comprehensive Review. *Sustainability*, *14*(24), 16684. https://doi.org/10.3390/su142416684

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, *66*(4), 493–504. https://doi.org/10.1016/j.bushor.2022.10.002

Taylor, R. D. (2020). “Data localization”: The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Villa-Salazar, A. F., Gomez-Miranda, I. N., Romero-Maya, A. F., Velásquez-Gómez, J. D., & Lemmel-Vélez, K. (2024). Optimizing Electric Racing Car Performance through Telemetry-Integrated Battery Charging: A Response Surface Analysis Approach. *World Electric Vehicle Journal*, *15*(7), 317. https://doi.org/10.3390/wevj15070317

Williamson, S. M., & Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences*, *14*(2), 675. https://doi.org/10.3390/app14020675

Victims of Corruption

Ahmadjonov Murodullo Nurali ogli
Assistant Prosecutor

Corruption negatively affects communities and undermines the global economy as a whole. It deters business growth, restricts foreign aid and investment, and worsens social disparity. The most vulnerable and marginalized individuals often suffer the most, as corruption limits their access to basic services and reduces their chances of escaping poverty and exclusion. For instance, in sectors like construction and healthcare, corruption can even result in loss of life. When public funds are misused, there is less investment in essential public services such as education and environmental protection. When corruption involves organized crime connected to powerful political or economic figures, it can lead to greater instability and violence, threatening both national and international peace and security on the whole (Spyromitros & Panagiotidis, 2022).

In recent years, there has been growing recognition of the link between corruption and human rights, demonstrated by two resolutions passed by the UN Human Rights Council in 2021. Corruption undermines social, economic, and cultural rights by compromising the delivery and quality of essential services. It also affects civil and political rights by weakening institutions, eroding the rule of law, and diminishing public trust in government legitimacy. Despite increasing awareness and ongoing research to collect data, corruption remains difficult to quantify due to its hidden nature and far-reaching effects. Identifying victims is often challenging, as in the case of environmental crimes, where those affected may be unaware of the harm caused. While combating corruption has become a political priority, there is growing consensus that both preventive and punitive measures are insufficient unless the harm caused is also effectively handled (Luna-Pla & Nicolás-Carlock, 2020) .

Further and even more importantly, the principle of repairing harm is a core concept found across all legal systems. In both common law and civil law traditions, it refers to addressing harm prompted by illegal actions in a way that aims to restore the situation to what it would have been had the harm not occurred. Different

jurisdictions may use varying terms such as recovery, restitution, reparation, compensation, remedy, or redress with potentially different interpretations.

When it comes to corruption-related damages, there are two key legal frameworks that provide a foundation for recovery: the anti-corruption framework and human rights law. Human rights are defined as internationally recognized legal entitlements individuals hold in relation to the state. In this regard, this foundation supports a victim-centered, claims-based approach that gives attention to securing reparations for those who have suffered harm, whether as individuals or communities. In contrast, the anti-corruption framework traditionally centers on prosecuting wrongdoers and ensuring they are held accountable. Despite their different focal points, both approaches are rooted in the rule of law the idea that all individuals and institutions, public or private, are subject to laws that are transparently established and fairly enforced as a whole (Guo, 2023).

In addition, the United Nations Convention against Corruption (UNCAC) the only universally binding international anti-corruption treaty accounts for measures encouraging national legal systems to enable victims and legitimate owners to reclaim damages and recover assets tied to corruption. Notably, Chapter V of the UNCAC is associated with asset recovery. This extends beyond merely punishing corrupt actors, emphasizing the return of stolen assets to rightful owners, constituting countries from which the assets were unlawfully taken. Although UNCAC's references to victim compensation are limited and somewhat general, their presence illustrates the intersection and mutual reinforcement of the anti-corruption and human rights approaches. In turn, the integration of concepts still like “victim” into anti-corruption treaties entails a shift in focus. Rather than solely aiming to avert impunity and enforce accountability, this shift highlights the importance of repairing the harm suffered by victims whether they are individuals, social groups, or entire nations (Davis, 2019).

Wide range of international and regional anti-corruption treaties, along with human rights instruments and non-binding declarations, contain provisions and references regarding the recovery of damages stemmed from corruption. Over recent decades, these instruments have helped establish shared principles and general mechanisms alongside measures through which countries have committed to ensuring their legal systems allow victims to reclaim losses caused by corrupt practices as a whole. Below, we delve into a concise overview of the critical international obligations and commitments that States have undertaken in this area, including:

- The United Nations Convention against Corruption (UNCAC);
- The Political Declaration adopted at the United Nations General Assembly Special Session;
- The Council of Europe Civil Law Convention on Corruption;
- The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism;

- The European Union (EU) Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the EU;
- Relevant human rights treaties that establish the right to a remedy

In turn, the aforementioned obligations and commitments do play a critical role in providing the victims of corruption-related offences with rights and remedies on the whole. It is a glaring example that the United Nations Convention against Corruption (UNCAC) adopted by the UN General Assembly in 2003 and came into force in 2005 is the only universally binding international treaty dedicated to combating corruption. The Convention sheds light on obligations and sets standards that must be pursued by its 190 State parties. Notably, four out of the five key provisions outlined below use binding language, creating a legal duty for all State parties to introduce the particular measures and approaches.

A distinctive feature of the UNCAC is its Implementation Review Mechanism, a peer-review system designed to help countries implement the Convention's core provisions into their legislations. In this regard, this mechanism facilitates the identification of challenges, setbacks, best practices, and areas where technical support is needed broadly. It, in turn, enables countries to identify weaknesses along with loopholes in their legal and institutional frameworks, while also offering the wider anti-corruption community both practitioners and scholars' insight into trends in implementation initiatives. To be obvious, the first relevant provision on victim compensation appears in Article 32 the UNCAC, which underscores the protection of witnesses, experts, and victims as well. While most of its paragraphs deal with protective measures, the final paragraph specifically requires States to allow victims' concerns and perspectives to be taken into account during criminal proceedings. Additionally, Article 34, titled "Consequences of Corruption," obliges States to take decisive measures and actions to iron out the effects of corrupt acts as well.

Furthermore, corruption remains a pervasive global challenge that undermines effective governance, distorts economic systems, and weakens institutional integrity on the whole. Historically, anti-corruption measures have largely emphasized the prevention of misconduct and the prosecution of offenders. However, there is a yawning awareness of grasping of the importance of addressing the human impact of corruption. Adopting a victim-oriented approach centered on identifying those affected, understanding the harm they suffer, and ensuring relevant remedies is essential for crafting more inclusive and effective anti-corruption policies and approaches.

To understanding who the victims are, it is worthwhile to point out that the phrase "victims of corruption" typically refers to individuals or groups who experience harm either directly or indirectly as a result of corrupt behavior. This harm may manifest in various forms, consisting of physical or psychological injury, emotional distress, financial losses, or significant violations of basic rights. These consequences often result from actions or omissions that breach criminal laws, particularly those concerning the misuse of power for private gain on the whole. In

contrast to more traditional offences where victims are readily identifiable, the harm prompted by corruption is often ubiquitous and not immediately visible. Its impact can take time to become apparent and frequently affects the populace on the large scale. For instance, when government funds are misappropriated or mismanaged, entire communities may face diminished access to essential services such as education, clean water, or healthcare without recognizing that corruption is the underlying cause (Pozsgai-Alvarez, 2024).

Further and even more importantly, corruption gives rise to plethora of forms of harm across socio-economic, and political spheres. From an economic standpoint, it misallocates public resources, resulting in underfunded infrastructure, deteriorating services, and deepening social inequality. In the health sector, corruption may result in inflated costs for services and goods, reduced quality of care, or the circulation of unsafe medications, putting lives at risk. Similarly, in education, bribery and theft of funds can undermine quality educating and deny equal access to education, contributing to entrenched poverty as a whole. In addition, from a social and political perspective, corruption damages trust in public institutions and weakens the rule of law. Its ramifications are particularly severe on vulnerable and marginalized groups, who often lack the means to seek justice while corruption poses a threat to democratic values, manipulating judicial systems and reinforcing systemic inequality and exclusion, all of which contribute to long-term political instability on the whole.

Additionally, a victim-centered approach to combating corruption emphasizes the rights, needs, and lived experiences of those who have suffered harm as a result of corrupt practices. In contrast to conventional anti-corruption strategies that focus mainly on uncovering wrongdoing and punishing perpetrator, this approach, in turn, acknowledges that corruption inflicts tangible damage on individuals, communities, and even entire countries as well. In this regard, it calls for a sudden shift in focus by posing key questions: Who has been harmed by corruption? In what ways have they suffered? And how can justice and redress be ensured?

This type of strategy includes several core components, two of which are the formal and social recognition of victims, accounting for those indirectly harmed, and the acknowledgment of variety forms of damage - whether physical, psychological, economic, or violations of fundamental rights. Another critically vital element is ensuring that victims have meaningful access to justice and redress mechanisms, which may include financial compensation, the return of stolen assets, or social and psychological support. Victims must also be given opportunities to partake in legal proceedings, be made aware of their rights, and receive the necessary assistance to seek justice effectively.

Additionally, a victim-centered model encourages active participation of victims in legal processes. This consists of mechanisms such as victim impact statements, where individuals can articulate how corruption has affected them personally. The strategy also promotes prevention of possible future harms through institutional reforms, improved transparency, and greater public involvement in decision-making processes. A critical aspect is the provision of protection and

support services for victims such as legal assistance, mental health care, and safeguards against retaliation, particularly in cases constituting whistleblowers or key witnesses on the whole (Holder & Englezos, 2024).

In practical terms, this strategy might be implemented through state-funded compensation schemes for communities impacted by corrupt resource extraction or by judicial orders mandating the return of misappropriated public funds. It may also involve partnerships between anti-corruption agencies and civil society organizations to identify victims and ensure they receive adequate support and legal guidance. The importance of this approach lies in its ability to consolidate justice, accountability, and public trust. It not only handles the consequences of corruption but also affirms the dignity and rights of those harmed. By focusing on restoration rather than punishment alone, a victim-focused approach promotes more inclusive, fair, and people-centered governance on the whole.

Bibliography

Davis, K. E. (2019). *Between Impunity and Imperialism*. Oxford University PressNew York. https://doi.org/10.1093/oso/9780190070809.001.0001

Guo, Z. (2023). Anti-corruption mechanisms in China after the supervision law. *Journal of Economic Criminology*, *1*, 100002. https://doi.org/10.1016/j.jeconc.2023.100002

Holder, R. L., & Englezos, E. (2024). Victim participation in criminal justice: A quantitative systematic and critical literature review. *International Review of Victimology*, *30*(1), 25–49. https://doi.org/10.1177/02697580231151207

Luna-Pla, I., & Nicolás-Carlock, J. R. (2020). Corruption and complexity: a scientific framework for the analysis of corruption networks. *Applied Network Science*, *5*(1), 13. https://doi.org/10.1007/s41109-020-00258-2

Pozsgai-Alvarez, J. (2024). Three-Dimensional Corruption Metrics: A Proposal for Integrating Frequency, Cost, and Significance. *Social Indicators Research*. https://doi.org/10.1007/s11205-024-03473-x

Spyromitros, E., & Panagiotidis, M. (2022). The impact of corruption on economic growth in developing countries and a comparative analysis of corruption measurement indicators. *Cogent Economics & Finance*, *10*(1). https://doi.org/10.1080/23322039.2022.2129368

AI-generated works and copyright: is there a need for new approaches?

Sanjar Shomurodov
Tashkent State University of Law

AI systems can now produce news articles, videos, images, and blog posts with minimal human input, blurring traditional notions of authorship and ownership. We analyze uncertainties about who (if anyone) can claim copyright in AI-generated works, given that copyright laws usually recognize only human creators. The discussion highlights a growing tension between existing legal frameworks designed for human creativity and the realities of AI-driven content creation. At the same time, the proliferation of AI-generated media raises risks of manipulation and provocation, such as deepfake videos and synthetic news used to misinform or defame, which current laws struggle to address. Through a legal-analytical and critical lens, and with international examples (from the United States, Europe, and Asia) and references to Uzbekistan's legislation, we evaluate whether existing copyright frameworks are adequate. We find that while some jurisdictions attempt to fit AI creations into current rules, significant gaps remain in authorship attribution and in controlling malicious AI-derived content.

Rapid advances in artificial intelligence have enabled algorithms to generate creative content that was once the exclusive domain of human authors. From news articles written by AI to computer generated artwork and deepfake videos, these AI-produced works test the limits of current copyright law. At the core of the issue is authorship: copyright traditionally vests in the author of a work, assuming the author is a human being exercising creative skill. Most national laws reflect this principle. For example, Uzbekistan's Law on Copyright and Related Rights defines an “Author” as “a natural person, whose creative labor created the work”. Similarly, U.S. courts and the Copyright Office have consistently held that only human beings can be authors under copyright law (GAFFAR & ALBARASHDI, 2025).

In the notable 2023 U.S. case Thaler v. Perlmutter, a federal judge reaffirmed that an AI-generated image with no human involvement could not be protected by copyright, emphasizing that human creativity is a fundamental requirement for copyright eligibility. AI-generated media complicates the picture of human involvement. Many AI systems generate content in response to human prompts or data inputs. Is the person who enters a text prompt or curates the training data the “author” of the resulting work? Or is the AI itself the creator, leaving no human author to claim rights? Under present law, an AI cannot be an author, it lacks legal personhood and the human creativity required by statutes and case law.

Some jurisdictions have tried to bridge this gap by attributing authorship to a human associated with the AI's output. Notably, the United Kingdom's Copyright, Designs and Patents Act 1988 provides that for a “computer-generated” work with no human author, the author is deemed to be “the person who made the arrangements necessary for the creation of the work”. Internationally, most countries have sided with the view that human creativity is indispensable. Merely providing a text prompt to an AI is not enough to claim authorship; there must be human selection, arrangement, editing, or other creative choices reflected in the work. This requirement aligns with copyright's fundamental purpose as articulated by scholars

like Boyden, who emphasizes that copyright aims to incentivize human creativity, not mechanical production (Mazzi, 2024).

Another significant challenge lies in the inputs and processes behind AI-generated media. Generative AI models are typically trained on massive datasets of existing works: millions of copyrighted articles, books, images, videos, and audio recordings are ingested to teach the AI how to produce similar content. This practice has sparked a wave of concern and litigation. In late 2023, numerous lawsuits were filed by artists, authors, and media companies against AI developers, alleging that the unlicensed use of copyrighted material to train AI models violates intellectual property rights. Some jurisdictions, like the EU, introduced text and data mining (TDM) exceptions in copyright law to allow data analysis of works, at least for research or under certain conditions. The EU's 2019 Copyright Directive permits data mining of legally accessed content, and rights holders can opt out for commercial uses. This was meant to strike a balance between innovation and rights. However, critics argue that these exceptions have been stretched by AI companies.

Perhaps the most troubling aspect of AI-generated media is its capacity for manipulation and provocation on a societal scale. “Deepfakes” hyper-realistic fake videos or audio and algorithmically generated fake news are now common enough to pose serious risks to privacy, reputation, public order, and even national security. From fabricated video speeches by public figures to AI-generated news reports that spread disinformation, the potential for harm is evident. Copyright law, however, is largely unconcerned with truth or falsity; it cares only about protecting creative expression. In fact, as U.S. jurisprudence emphasizes, copyright does not protect an individual's image, likeness, or identity per se (Kharvi, 2024).

This means that if someone uses an AI to create a fake video of a celebrity or a politician saying things they never said, the primary legal issue is not copyright (unless the video copied parts of a pre-existing copyrighted video). The person depicted has no automatic copyright claim over that synthetic video, because it's not a use of their copyrighted work, it's a use of their persona or likeness, which falls under privacy, data protection, or “personality rights” laws rather than copyright. This is a crucial gap: malicious actors can create and distribute AI-generated false media without infringing copyright, thereby avoiding one possible avenue of content control.

Moreover, in countries like Uzbekistan, while general legal provisions exist regarding defamation, dissemination of false information, and online provocation, there is no specific legislation that addresses deepfakes or AI-generated impersonations. The current legal framework criminalizes the spread of “deliberately false information” that could damage public order or an individual's reputation, but it does not account for the unique characteristics of synthetic media. As such, if an AI-generated fake video damages a public figure’s image without directly copying any copyrighted material, legal remedies may be unclear or delayed. This creates a potential regulatory vacuum where harmful content may circulate widely before authorities can intervene, especially in digital media and social networks. Thus, just

as copyright law alone is insufficient to manage AI-generated manipulation, general criminal or civil codes may also fall short unless updated to address emerging technologies.

To fill this gap, legal scholars and policymakers have suggested implementing transparency obligations for AI-generated media. These could include requirements that deepfake content be clearly labeled as artificially generated, or that creators obtain consent before using someone's likeness for synthetic media. Similar measures have already been adopted in China, and provisions in the European Union's AI Act and Digital Services Act mandate platform-level responsibility for clearly identifying manipulated content (Felzmann et al., 2019). For Uzbekistan and other developing jurisdictions, these approaches could serve as models. Furthermore, collaborative mechanisms, such as regional agreements or coordination with global IP institutions like WIPO, may assist in harmonizing standards and building a legal infrastructure capable of mitigating the risks of AI-generated manipulation, while preserving freedom of expression and technological innovation.

From the analysis above, it becomes clear that current copyright frameworks, both in Uzbekistan and internationally, are under significant pressure in the age of AI-generated content. On the issue of authorship and ownership of AI creations, the law either denies protection (as in U.S. and Uzbek practice) or extends protection through legal fictions (as in the U.K.), but neither approach fully resolves the dilemma. There is a strong case that new approaches are needed to address the legal issues posed by AI-generated media content. In the realm of copyright, this might involve clarifying laws to confirm how human creativity can be blended with AI assistance for example, providing guidance on the threshold of human contribution required for a work to be protected. Legislatures may consider explicit provisions on "AI-generated works," whether to exclude them from protection (as pure machine output) or to create a tailored protection regime. International organizations like WIPO are already facilitating discussions on AI and IP, which could lead to soft law recommendations or treaty updates in the future (Atilla, 2024).

For Uzbekistan, keeping pace with these developments is crucial. The country's existing copyright law provides a solid foundation by aligning with international norms on authorship, but it may need augmentation to explicitly handle AI-created works and to protect creators and the public from new forms of misuse. Policymakers should evaluate whether amendments are needed to the Copyright Act or related legislation to define the status of AI-generated works (possibly declaring them unprotected unless a human contributor is identified, to avoid ambiguity). Additionally, as Uzbekistan continues to digitalize, consideration could be given to laws ensuring transparency of AI-generated media and protecting individuals from unauthorized digital impersonation. In a global context where AI technology evolves faster than law, the need for new approaches is evident – not necessarily a wholesale replacement of copyright principles, but targeted adaptations and supplementary laws.

Bibliography

Atilla, S. (2024). Dealing with AI-generated works: lessons from the CDPA section 9(3). *Journal of Intellectual Property Law and Practice*, *19*(1), 43–54. https://doi.org/10.1093/jiplp/jpad102

Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951719860542

GAFFAR, H., & ALBARASHDI, S. (2025). Copyright Protection for AI-Generated Works: Exploring Originality and Ownership in a Digital Landscape. *Asian Journal of International Law*, *15*(1), 23–46. https://doi.org/10.1017/S2044251323000735

Kharvi, P. L. (2024). Understanding the Impact of AI-Generated Deepfakes on Public Opinion, Political Discourse, and Personal Security in Social Media. *IEEE Security & Privacy*, *22*(4), 115–122. https://doi.org/10.1109/MSEC.2024.3405963

Mazzi, F. (2024). Authorship in artificial intelligence-generated works: Exploring originality in text prompts and artificial intelligence outputs through philosophical foundations of copyright and collage protection. *The Journal of World Intellectual Property*, *27*(3), 410–427. https://doi.org/10.1111/jwip.12310

Artificial Intelligence and Autonomous Vehicles: Issues of Legal Personality in the Digital Age

Inoyatov Nodirbek Xayitboy ugli
Tashkent State University of Law

Modern society is experiencing a rapid integration of artificial intelligence systems and autonomous vehicles into daily life. According to Boston Consulting Group, autonomous vehicles are projected to constitute 25% of the global automotive market by 2035 (Noviati et al., 2024). Artificial intelligence and autonomous vehicles represent not only a transportation revolution but also a paradigm shift for legal systems. This technological transformation raises fundamental questions for legal theory and practice. The legal status of AI systems and autonomous vehicles remains undefined in most countries' legislation. The question of legal personality is one of the most important and complex legal issues in the field of artificial intelligence. The ambiguity surrounding liability, insurance systems, and legal subjectivity issues underscores the urgency of addressing these questions.

This research aims to comprehensively study the legal personality issues of artificial intelligence, particularly autonomous vehicles, analyze international experience, and develop scientifically-based proposals for legislative improvement. The question of legal personality for AI systems has not found uniform solutions in national legislation, each state faces the necessity of detailed legal regulation based

on the characteristics of its legal system. The concept of legal personality and its historical evolution provides essential context for understanding AI's potential legal status (Novelli et al., 2022). The concept of legal personality has historically been variable, encompassing new types with the development of society and technology. This evolution has previously accommodated non-human entities like corporations and governmental bodies (Hárs, 2022).

Different scholars approach the legal subjectivity of AI systems from varying perspectives. AI systems as merely objects of civil law are insufficient because they possess autonomy and unique decision-making abilities. The necessity of a special legal regime for autonomous vehicles. The research also monitors existing legislative frameworks in national contexts, analyzing civil codes and transportation laws. Statistical data regarding autonomous vehicle accidents, their causes, and liability determination mechanisms provide empirical grounding for the analysis.

The global autonomous vehicle market is growing rapidly. It projects that by 2030, autonomous vehicles will reach 40% of the global automotive market. This trend intensifies the need for legal regulation in this area. International legal standards for AI are developing quickly. Studies show a 320% increase in legal documents related to AI between 2015-2022. The adoption of ISO/IEC 22989 standards represents a significant step toward global regulation of AI systems. Research indicates an increasing number of legal violations involving autonomous vehicles, with 273 autonomous driving-related accidents recorded in the US alone in 2022. More than 45 countries worldwide have adopted special legislation regulating AI, with the European Union, United States, China, South Korea, and Singapore leading in this field (Chougule et al., 2024).

Through analysis of international experience and legal frameworks, two potential categorizations for autonomous vehicles emerge. Firstly, autonomous vehicles as property objects requiring special legal regimes due to technological complexity Secondly, “Electronic persons” as a new type of legal construction with elements of limited legal subjectivity. Considering that modern autonomous vehicles lack fully independent decision-making capabilities, recognizing them as full legal subjects appears premature. However, implementing the “electronic person” construction could effectively address liability issues. The practical necessity of the “electronic person” concept remains contested. To granting AI «electronic person» status based on their autonomy and decision-making capabilities provides a clear mechanism for establishing liability when harm occurs (Custers et al., 2025).

However, granting full legal subjectivity to AI could become an artificial legal fiction rather than addressing practical necessity. Such fiction might serve as a convenient mechanism for avoiding responsibility without effectively protecting the rights of injured parties. Studies suggest that in autonomous vehicle accidents, liability should ultimately rest with either insurance companies or manufacturers. The creation of a special legal regime for autonomous vehicles appears more promising. Based on research, regulating autonomous vehicles as objects with special legal regimes rather than full legal subjects offers several advantages. For example,

ensures legal clarity, clearly defines liability issues, strengthens protection of injured parties' rights, does not impede innovation development. A “electronic person fund” concept merits further development. This model offers a mechanism for distributing liability for damage caused by autonomous vehicles and pre-accumulating financial resources for compensation.

Based on the research findings, a gradual improvement of legislation following these principles is recommended: Firstly, technological neutrality (legislation should be adaptable to rapidly changing technologies), secondly, priority of safety (ensuring autonomous vehicle safety must be the primary task), thirdly, clear definition of the liability system, fourthly, consideration of international experience and standards.

The «electronic person fund» concept should be adapted to specific national contexts as a mechanism for distributing liability for damage caused by autonomous vehicles and pre-accumulating financial resources. The research identifies several challenges in the scientific field: terminological inconsistency, lack of empirical data, complexity of interdisciplinary approaches, and balancing legal regulation with innovation. The ambiguity of legal concepts leads to serious problems in norm-creation. These challenges can be addressed through clearly defining the conceptual apparatus in scientific research, studying foreign experience, taking a complex approach involving specialists from various fields, and proposing soft legal regulation instruments.

Artificial intelligence, particularly autonomous vehicles, occupies a unique position in the modern legal system. While they are considered property objects, their autonomy necessitates a special legal regime. The “electronic person” concept implies limited rather than full legal subjectivity for AI and autonomous vehicles, reflecting their lack of self-awareness and genuine intelligence (Custers et al., 2025). The optimal way to address liability issues related to autonomous vehicles is applying the “risk chain” concept, which ensures reasonable distribution of liability among vehicle manufacturers, software developers, owners, and other subjects. Creating a special legal regime for autonomous vehicles is necessary to address liability, insurance, data security, and ethical-legal issues.

Improving national legislation should adhere to principles of technological neutrality, safety priority, clear definition of the liability system, and consideration of international experience and standards. The “electronic person fund” concept should be adapted to specific national contexts as a mechanism for distributing liability for damage caused by autonomous vehicles and pre-accumulating financial resources. The legal status of artificial intelligence and autonomous vehicles has strategic importance, requiring gradual improvement of legislation, studying international experience, and creating modern legal mechanisms that consider national legal system characteristics. Accelerating the adoption of international standards such as ISO/IEC 22989 (AI concepts and terminology) and ISO/PAS 21448 (road vehicle safety) is essential for effective regulation in this emerging field.

Bibliography

Chougule, A., Chamola, V., Sam, A., Yu, F. R., & Sikdar, B. (2024). A Comprehensive Review on Limitations of Autonomous Driving and Its Impact on Accidents and Collisions. *IEEE Open Journal of Vehicular Technology*, *5*, 142–161. https://doi.org/10.1109/OJVT.2023.3335180

Custers, B., Lahmann, H., & Scott, B. I. (2025). From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies. *AI & SOCIETY*. https://doi.org/10.1007/s00146-024-02137-1

Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, *62*(4), 320–344. https://doi.org/10.1556/2052.2022.00352

Novelli, C., Bongiovanni, G., & Sartor, G. (2022). A conceptual framework for legal personality and its application to AI. *Jurisprudence*, *13*(2), 194–219. https://doi.org/10.1080/20403313.2021.2010936

Noviati, N. D., Putra, F. E., Sadan, S., Ahsanitaqwim, R., Septiani, N., & Santoso, N. P. L. (2024). Artificial Intelligence in Autonomous Vehicles: Current Innovations and Future Trends. *International Journal of Cyber and IT Service Management*, *4*(2), 97–104. https://doi.org/10.34306/ijcitsm.v4i2.161

Money Laundering and Cryptocurrency. The Threats and Ways to Control

Bahodir Muzaffarov
Tashkent State University of Law

Money laundering is the process where individuals or organizations hide the illicit origins of their funds and make them appear as though they come from legitimate sources. If this kind of crime happens, it can give a chance to criminals to bring illegally obtained money into the legal financial system. At first glance, money laundering might seem similar to other financial crimes like tax evasion or fraud, however, the main difference lies in the origin of the funds. Money laundering specifically uses the money that were obtained through illegal activities, including drug trafficking, corruption, organized crime, or even terrorism financing. Laundering money can have a detrimental impact on economy, for example, in 2021 alone, cybercriminals laundered $8.6 billion in cryptocurrency, a 31% increase over the previous year(Korejo et al., 2021).

When it comes cryptocurrencies, they can be considered as a digital version of money, but they differ in terms of many aspects compared to printed money and the fund on our bank cards. Most importantly, they are unregulated, which means that the government has little to none influence on controlling it and at being aware of the crypto-transactions between certain people. Additionally, this type of digital money is not regulated nor ruled by any Central Banks.

Usually, criminals use money laundering techniques to make it harder to public and government officials to track it. This process typically involves three stages. First one is a Placement. This stage can be done through methods such as depositing cash into bank accounts or purchasing assets like real estate or luxury items. Second stage is called Layering and this might involve transferring money between multiple accounts, investing in various financial instruments, or converting funds into different currencies. Last one is Integration, in other words reintroducing the "cleaned" money into the economy as seemingly legitimate income. At this stage, the laundered funds can be used for any expenses (Cooke & Marshall, 2024).

Tax evasion and falsified accounting records are two common types of money laundering. In addition, criminals often use shell companies and offshore accounts to hide illegal funds and make them appear legitimate. Shell companies are businesses that exist only on paper. They don't have real operations or employees. Criminals create them to hide the true ownership of assets and to make illegal money look clean. When it comes to offshore accounts, these are bank accounts opened in countries different from where the account holder lives. Often, these countries have strict privacy laws, which makes it hard to trace the money back to its source.

About 0.15% of all cryptocurrency transactions, roughly $14 billion annuall, are linked to illicit activities. Therefore, due to the risks associated with the use of cryptocurrencies related to money laundering, some countries have prohibited their use and imposed fines on their users (Sanz-Bas et al., 2021). One of the main threats is the high level of anonymity provided by cryptocurrencies. That's why cryptocurrencies have become a popular choice for criminals. For instance, weapons dealers, drug dealers, human traffickers, and child pornography distributors or even terrorist organisations make payments through cryptotransactions, because it makes their job easier because they can receive or send money while staying anonymous. The ISIL case can be real example:

The ISIL (Islamic State of Iraq and the Levant is a terrorist organization) can be seen while asking donations and giving their Bitcoin address (Press Release, 2020).

One of the methods where crypto-based money laundering occurs is a technique called cryptocurrency mixer, also known as a tumbler. Cryptocurrency tumblers make it hard to track specific coins by mixing funds from different sources over a random period before sending them to new addresses. These services exist because cryptocurrency transactions are recorded on a public ledger, and some users want to stay anonymous. However, tumblers have also been used to hide illegal money. A good example of this is the Sheep Marketplace case from December 2013. This online marketplace was mostly used for illegal activities like selling drugs, weapons, and stolen data. Another example is when hackers stole over $8 million worth of Bitcoin and in order to avoid getting caught, they used a service called Bitcoin Fog, which operated from 2011 to 2021.

Nowadays, services like Tornado Cash, YoMix offer mix transactions so that it becomes difficult to trace where the money come from or where it is going. Those services are famous among criminals. For example, TornadoCash has been a good tool for North Korea's Lazarus Group which stole $620 million Ronin Bridge hack while they later switched to using YoMix. Another method involves fiat-to-crypto exchanges. A fiat-to-crypto exchange is basically a place where you can trade regular money, like dollars or euros, for cryptocurrencies like Bitcoin and Ethereum. Platforms like Coinbase and Gemini offer people swaping their cash for digital coins. These exchanges act as a middleman between traditional finance and the crypto world. Also regulating these exchanges won't always be easy.

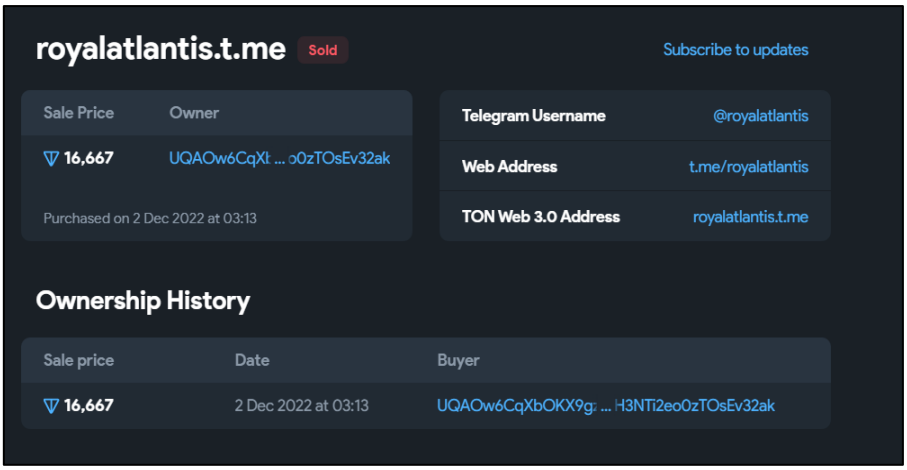
Last but not least, online gambling can be a method which people can exploit in order to make their "dirty" money "clean". Many online casinos and betting websites accept crypto, which lets people deposit large amounts of money without too many questions being asked. Someone who wants to launder money can put their illegal funds into a gambling site, place safe bets, and then take out their winnings as if they were legally earned. Gambling transactions usually seem normal, so they don't always raise suspicion. This makes it easier for criminals to hide where their money really came from. A lot of crypto gambling sites are also decentralized and don't require much personal information, which makes it even harder for authorities to track. This is why online gambling has become a popular way for people to hide illegal money in the crypto world (Fiedler, 2013).

Moreover, there is another method which, in my view, is always being neglected and ignored. That method involves Telegram and its marketplace, Fragment.com. No previous research has been done about that, so that's why I decided to take this matter into my own hands. So, Fragment.com is a website where people can buy and sell special usernames and anonymous numbers. In other words, it is a service used for Telegram. This site runs on The Open Network (TON) blockchain that helps transactions to be safe and clear. Also, users can participate in public auctions or buy usernames directly, so that they can use these names for their

personal accounts, groups, channels, or bots on Telegram. For the payments, the people must use Toncoin, which is the main cryptocurrency for the TON blockchain. Everything up to here might seem okay, but the problem is users can also buy their own NFTs, e.g. usernames. In order to list a username, that you own on Telegram, you must claim it earlier than others and wait about 15 days. Afterwards, you will have a chance to auction your username and turn it into NFT.

It was very hard to find a crime that has occurred on Fragment.com. However, this does not mean that criminals are not using this method, this high likely means that the criminals are not being detected and caught. I will just give one scenario. Let's say someone from Uzbekistan gambled his money and won a fair amount of money. The next thing a gambler must to do is to bring his "dirty" money into a regular financial system. He could use fragment.com because owning some random username on Telegram gives him a chance to buy his own username, the whole amount of money comes back to himself but fragment.com only takes 5 TONcoin and 5% of the last bid as a commission. Let's say, a gambler bid on his own NFT and the auction ended. Then a gambler can withdraw that remaining money, and now he is good to go because his money looks like "clean money". This tactic can used by any type of criminals such as a drug dealer, a scammer or a corrupted government official can easily exploit this method.

At this picture you can see that some random username was bought at 16,667 TONcoin which worth over $60,000 today.



The picture above was taken from fragment.com and it is just like a tip of iceberg. Because over thousands of usernames similar to given picture exist on this site and a person with a conscious mind will never buy this type of crap username for a large sum of money. It is clear that this auction is used for money laundering. The good news is that earlier this year Telegram and fragment.com introduced Know Your Customer (KYC) check to enhance security and prevent illegal activities. KYC procedure involves asking users their original IDs and confirming that the person is real. It helps in assessing risks and making sure that the user isn't involved in fraud or illegal activities. However, I'm pretty sure that the criminals can pass this stage without a doubt if they really want to do so by such as using a fake-ID or even by buying a passport and other personal information through Darkweb.

International cooperation's also play a crucial role in fighting cryptocurrency-based money laundering. The Financial Action Task Force (FATF) is a global organization that fights money laundering and terrorist financing. It sets international rules to stop these crimes and their negative effects on society. FATF has created 40 key recommendations that help countries work together to fight organized crime, corruption, and terrorism. These rules make it easier for authorities to track down criminals who profit from illegal activities like drug trafficking and human trafficking. One of the earlier recommendations says that countries should criminalize money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 also known as the Palermo Convention.

What it means is that money laundering must be considered as a crime across the world. Additionally, this intergovernmental organization urges countries to punish criminals who contribute to money laundering in many ways such as participation, association, planning with others, attempting, facilitating and giving advice on this crime. FATF has also a jurisdiction to check whether countries are following the rules properly through regular reviews and takes action against those that don't follow. From one side, it is true that cryptocurrencies have potential to make financial services more accessible and efficient. On the contrary, they can also provide criminals with new ways to launder money.

To minimize the risks of cryptocurrency-based money laundering, I suggest taking some measures. Firstly, improving and expanding blockchain analytics tools is crucial for tracking suspicious transactions and identifying crimes. Secondly, regulations must be consistent all over the world to prevent criminals from exploiting weak points in the system. Additionally, giving limited control to government over cryptocurrencies may be useful, because at this case criminals know that they're under control, so they may be refrain from doing it. Lastly, stronger partnerships between governments, financial institutions, and law enforcement agencies can be useful because exchanged data between them helps to tackle these challenges more effectively(Atlam et al., 2024) .

To conclude, developments in blockchain analytics can offer some hope. Machine learning and graph-based analysis can be life-changing factors in helping investigators to detect suspicious activity. For instance, graph algorithms and machine learning can help in analyzing large amounts of financial data because Graph Neural Networks (GNNs) are designed to find connections and patterns. These methods can learn from past data and recognize signs of money laundering. This makes it easier to detect suspicious activity more accurately. On the other hand, advancements in Artificial Intelligence can be helpful for criminals who want to launder the money. For instance, AI can create deepfake identities. After that, AI-generated fake IDs, documents, and even deepfake videos can be used to bypass Know Your Customer (KYC) checks.

Bibliography

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*, *13*(17), 3568. https://doi.org/10.3390/electronics13173568

Cooke, D., & Marshall, A. (2024). Money laundering through video games, a criminals' playground. *Forensic Science International: Digital Investigation*, *50*, 301802. https://doi.org/10.1016/j.fsidi.2024.301802

Fiedler, I. (2013). Online Gambling as a Game Changer to Money Laundering? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2261266

Korejo, M. S., Rajamanickam, R., & Md. Said, M. H. (2021). The concept of money laundering: a quest for legal definition. *Journal of Money Laundering Control*, *24*(4), 725–736. https://doi.org/10.1108/JMLC-05-2020-0045

Sanz-Bas, D., del Rosal, C., Náñez Alonso, S. L., & Echarte Fernández, M. Á. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws*, *10*(3), 57. https://doi.org/10.3390/laws10030057

Legal Regulation of the Digital Economy

Raximbayeva Sarvinoz
Tashkent State University of Law

In today's modern world, the digital economy is rapidly developing and has become a complex system encompassing various sectors. Therefore, the legal regulation of this sphere has become a pressing issue. Developing legal mechanisms related to the digital economy and implementing them in practice enables transparency in the use of technologies, protection of citizens' digital rights, and combating cybercrime. Legal regulation covers areas such as digital services, e-commerce, intellectual property, personal data protection, cryptocurrencies, and artificial intelligence. By creating clear and effective legal frameworks in each of these areas, states can achieve a stable digital transformation. The issues of legal regulation of the digital economy and their solutions are considered not separately, but within a single system in close connection with technological, economic, social, and legal aspects (Guliyeva et al., 2021). Based on the development dynamics of digital transformation processes in countries around the world, the needs and promising directions for the legal system have been forecasted.

Before deeply analyzing this topic, it is necessary to understand the essence and meaning of several concepts. For example, without understanding the concept of the digital economy, it is not possible to talk about its legal regulation. The digital economy is a system of economic relations in which digitized data serve as the main

factor of production in all sectors. In other words, it is a network of all types of economic activities carried out through information and communication technologies (ICT) around the world. Here, the focus is not on software, but rather on services, goods, and activities conducted through electronic business. For reference, the term "digital economy" first appeared in 1994 when Don Tapscott published his book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence" (Bukht & Heeks, 2018).

The theory of the digital economy has not yet fully formed and is being studied in depth by many scholars and experts. In scientific literature, the modern digital economy is described using various terms. The growing importance of digital information technologies in economic processes and their crucial role in shaping the economy on a global scale. In today's world, the development of the digital economy is occurring at a rapid pace, and the reason for this is clear: the advantages of the new economy over the traditional one has become evident. Economic relations are virtual, digital documents eliminate the need for paper materials, goods are weightless, which in many cases eliminates the demand for large-scale packaging and transportation services (Irtyshcheva, 2021).

The possibilities for movement in the virtual space are limitless, new virtual currencies have emerged and are being actively used, and so on. The problem is that despite such rapid development and clear progress, the future directions of the digital economy are still uncertain. At the current stage, it is difficult to envision the future relationship between the digital and traditional economy, the economy that consumes material resources and requires labor. However, it is clear that the new relationships emerging within the digital economy must be properly formalized from a legal standpoint, because the legal vacuum in this area may negatively affect traditional ways of conducting business. To confirm the relevance of this issue, one can refer to the application of innovative technologies in the taxi services sector, in particular, the Uber service which uses digital technologies for smartphones. In some countries, particularly in India, the emergence of Uber services has led to serious negative changes in the traditional taxi service system, as the legal norms that had been in place in this sector were not compatible with the new conditions (Pepić, 2018).

The main characteristics of the traditional post-industrial economy and the digital economy differ significantly, which indicates the need to develop a new model of legal regulation to support new economic processes. Currently, there are various opinions about the normative and legal measures that should be implemented to regulate the development of the digital economy worldwide. Our studies have shown that the digital economy is more global compared to the traditional economy, meaning that the importance of harmonizing regulatory frameworks in this area is growing not only at the national but also at the international level. However, at present, the legal norms applied to the digital economy are not very clear, as approaches to this field vary across countries, which in turn creates risks for the successful development and implementation of innovations.

In addition, although the digital economy covers many areas of activity, it cannot yet be called a global economy, as not all economic sectors have the capacity to manage it. Therefore, legislative changes in this field should be implemented gradually. For example, in 2009, the Australian Government published a report on broadband communication and the digital economy, emphasizing the need for joint efforts by society, industry, and the state for the development of the digital economy in Australia. The report noted that the government's main role in the development of the digital economy is to regulate market issues, ensure effective and fair functioning in this field, reduce the negative consequences of social inequality in society, and support the most vulnerable segments. According to the report's authors, the primary goal of the state is to ensure that citizens, businesses, and households have access to all the services offered by the digital economy. For this, it is necessary to build and develop digital infrastructure, support the development of innovations, and develop an appropriate legal framework (Oloyede et al., 2023).

The report of the Digital Economy Commission of the World Trade Chamber emphasized that effective methods of regulation within the digital economy may be leadership-based approaches, as the previously used detailed regulatory documents for all types of activities are not capable of regulating new digital technologies in a timely manner. Moreover, in the rapidly evolving conditions of the digital economy, there is a risk that legislative methods may lose their relevance. According to some scholars, in order to successfully regulate activities in the digital economy, it is necessary to apply methods that regulate social relations after they arise, while also taking into account relevant data. At the same time, methods based on prior calculations and forecasting may not be effective in new conditions.

The Digital Economy is a global phenomenon that encompasses various aspects of the economies of many countries. Therefore, it is still too early to conclude whether there are or should be specific legal acts regulating this field. However, some countries have developed and implemented such documents. For example, in the Russian Federation, the official development of the digital economy began on December 1, 2016, after President Vladimir Putin's address to the Federal Assembly. In the address, the need to create a new web-economy was emphasized, aimed at increasing the efficiency of industrial sectors through the use of information technologies. Looking at the experience of the United Kingdom, in 2010 the "Digital Economy Act" was adopted, followed by another "Digital Economy Act" in 2017. The 2010 Act defined the functions of the UK's communication authority, established the internet domain registry, developed regulations related to online copyright infringement, and regulated the provision of radio and television services, as well as the use of the electromagnetic radiation spectrum.

The 2017 Act, adopted as a supplement to the previous one, aimed to regulate electronic communications services and infrastructure, define access regulations related to online pornography, identify systems for the protection of intellectual property related to electronic communications, regulate data sharing systems, prevent the use of communication devices for crimes such as drug trafficking, manage

the application of internet filters, and monitor the operation of payment systems. In France, the "Law on Confidence in the Digital Economy" has been adopted and is currently in effect. This regulatory legal document mainly provides for amendments to other laws. For instance, changes are made to electronic commerce activities and technical service provisions, as well as regulations related to digital economy security and the resolution of other issues. Another serious issue in developing the legal framework for the digital economy has been the challenge of ensuring competition, which is becoming increasingly important over time.

The rapid growth of innovation and the application of cutting-edge technologies in the digital economy often surpass traditional regulatory methods, making it difficult for the state to consistently monitor and consider rapidly evolving competition across various economic sectors. In today's digital economy, increasing competition requires the state to implement legal protection measures within the framework of intellectual property laws. Furthermore, regulation in this field demands approaches based on collaboration between intellectual property rights and competition law. It should be emphasized that the application of innovations and technical improvements even competition arising from potential failures in their operation is of great significance for the development of the digital economy (Oluka, 2024).

The main driving force behind the development of society in the field of digital technologies is the improvement in the quality of the global internet network and the expansion of communication technologies. As a result of these factors, it has become possible to quickly exchange, collect, and store large volumes of data. This, in turn, allows for in-depth analysis of existing information, accurate forecasting based on data, rational decision-making, and increased efficiency in various sectors. However, the formation of digital infrastructure namely, the creation of international-level information platforms and the ecosystems that support them is of significant importance. At the same time, this process brings about a number of challenges. It is essential to address these issues in a timely manner, as delays could lead to negative consequences in the process of digital transformation.

One of the most difficult issues to resolve in the digital economy is legal regulation. In the development of innovative technologies within the digital economy, the key factor is access to data. If third parties interested in such data are granted access rights, numerous questions arise regarding the protection of competition and rights. Thus, it can be understood that there are problems in the legal provision of data protection. Therefore, various approaches in the field of digital economy regulation converge on the idea that conditions should be created for the free development of technical innovations, while also taking into account potential risks. One of the most significant risks is the uncertainty about the future direction of digital economic development (Kumari, 2023). Hence, the legislation being developed must be sufficiently flexible and consider as much relevant data as possible.

The experience of various countries shows that an effective legal framework for the digital economy requires a comprehensive and integrated approach. Key areas include the protection of personal data, the strengthening of intellectual property

rights, ensuring cybersecurity, and fostering a competitive environment. Without the development of unified international approaches, differences in national legislation may hinder the growth of digital economic relations. Therefore, alongside the development of digital infrastructure, it is essential to continuously improve the regulatory and legal documents that define the legal status of entities operating based on modern technologies. Ultimately, the regulation of the digital economy should not become an obstacle to innovative development but should serve as a supporting and stimulating factor.

Bibliography

Bukht, R., & Heeks, R. (2018). Defining, Conceptualising and Measuring the Digital Economy. *International Organisations Research Journal*, *13*(2), 143–172. https://doi.org/10.17323/1996-7845-2018-02-07

Guliyeva, A., Korneeva, E., & Strielkowski, W. (2021). *An Introduction: Legal Regulation of the Digital Economy and Digital Relations in the 21 st Century*. https://doi.org/10.2991/aebmr.k.210318.001

Irtyshcheva, I. (2021). The effect of digital technology development on economic growth. *International Journal of Data and Network Science*, 25–36. https://doi.org/10.5267/j.ijdns.2020.11.006

Kumari, A. (2023). *Digital Transformation Risks and Uncertainties in European Union and Indian Industry* (pp. 150–166). https://doi.org/10.4018/979-8-3693-0458-7.ch006

Oloyede, A. A., Faruk, N., Noma, N., Tebepah, E., & Nwaulune, A. K. (2023). Measuring the impact of the digital economy in developing countries: A systematic review and meta- analysis. *Heliyon*, *9*(7), e17654. https://doi.org/10.1016/j.heliyon.2023.e17654

Oluka, A. (2024). The impact of digital platforms on traditional market structures. *Technology Audit and Production Reserves*, *2*(4(76)), 21–29. https://doi.org/10.15587/2706-5448.2024.303462

Pepić, L. (2018). The sharing economy: Uber and its effect on taxi companies. *ACTA ECONOMICA*, *16*(28). https://doi.org/10.7251/ACE1828123P

Legal Aspects of Cybersecurity Governance in Organizations

Rakhmatov Uktam

Tashkent State University of Law

Cybersecurity governance has become a central concern for organizations across all sectors, driven by the escalating frequency and sophistication of cyber threats. As digital transformation accelerates, organizations are increasingly reliant on complex information systems, making them attractive targets for cybercriminals and state-sponsored actors alike. The legal aspects of cybersecurity governance encompass the frameworks, statutes, and regulations that define how organizations

must protect their digital assets and operations. These legal frameworks are not only crucial for safeguarding sensitive data and maintaining business continuity but also for ensuring compliance with a growing array of national and international laws. The intersection of law and cybersecurity is characterized by a dynamic landscape, where legal requirements evolve in response to emerging threats and technological advancements (Olukunle Oladipupo Amoo et al., 2024). Precise legal definitions such as those pertaining to "cyber threat," "data breach," and "information security" are essential for providing clarity and consistency in both regulatory enforcement and judicial proceedings. However, the interpretation of these terms often varies across jurisdictions, posing significant challenges for organizations operating in multiple countries.

The legal definitions that underpin cybersecurity governance are foundational to the development and enforcement of effective regulatory frameworks. A "cyber threat" is commonly understood as any potential event or action that exploits a vulnerability in an information system, with the potential to cause harm to an organization's data, systems, or operations. This broad definition encompasses a wide range of malicious activities, from ransomware attacks and phishing schemes to advanced persistent threats orchestrated by nation-states. "Data breach" refers to incidents involving unauthorized access to, or disclosure of, sensitive, protected, or confidential data. Such breaches can have far-reaching legal and reputational consequences, particularly in sectors handling personal or financial information (Safitra et al., 2023). The ISO/IEC 27001 standard, widely recognized in both legal and technical circles, defines "information security" as the preservation of confidentiality, integrity, and availability of information. Legal frameworks also address the concept of "cyber risk," which refers to the potential for loss, damage, or destruction of assets or data as a result of a cyber-attack or breach.

The legal framework for cyber risk management establishes the standards and obligations that organizations must adhere to in order to identify, assess, and mitigate cyber threats. Central to this framework is the concept of "reasonable security measures," which serves as the benchmark for evaluating an organization's cybersecurity posture. However, what constitutes "reasonable" varies significantly across legal systems and industries. In the United States, for example, the Federal Trade Commission's "Start with Security" guide provides practical recommendations that serve as a baseline for reasonable security practices. Failure to implement such measures can result in regulatory enforcement actions, civil liability, and reputational harm. Legal frameworks are increasingly moving towards risk-based approaches, requiring organizations to tailor their cybersecurity programs to the specific threats they face. This evolution reflects a growing recognition that proactive risk management is essential for mitigating cyber threats and protecting digital assets (Nurwanah, 2024).

The governance of cybersecurity within organizations has shifted from being a purely technical concern to a core issue of corporate governance. Regulatory bodies are increasingly holding boards of directors and senior executives accountable for

overseeing cybersecurity risks. In the United States, the Securities and Exchange Commission (SEC) has issued guidance emphasizing the need for board oversight of cybersecurity risks, reflecting a broader trend towards integrating cyber risk management into overall corporate governance structures. The New York Department of Financial Services' Cybersecurity Regulation, for instance, mandates that financial institutions implement specific governance requirements, including the appointment of a Chief Information Security Officer and the establishment of a formal cybersecurity program. These legal requirements underscore the importance of treating cybersecurity as a strategic business issue rather than a peripheral IT function. Boards are expected to be informed about the organization's cyber risk profile, to allocate adequate resources for cybersecurity, and to ensure that appropriate policies and controls are in place.

The development of international cybersecurity law is a rapidly evolving field, reflecting the global nature of cyber threats and the interconnectedness of digital infrastructure. Existing international legal principles, such as state sovereignty and non-intervention, are being tested by the unique challenges of cyberspace, including attribution, jurisdiction, and the use of offensive cyber capabilities. The Council of Europe's Budapest Convention on Cybercrime, ratified by over 65 countries, provides a common foundation for national cybercrime laws and facilitates international cooperation in prosecuting cybercrimes. However, significant gaps remain, particularly in terms of harmonizing legal definitions and enforcement mechanisms across jurisdictions. Ongoing debates center on whether new international instruments are needed to address issues such as state-sponsored cyber operations and the protection of critical infrastructure.

Legal definitions of cyber risks and threats vary significantly across jurisdictions, reflecting different regulatory philosophies and priorities (Kello, 2021). In the United States, the Cybersecurity Information Sharing Act (CISA) of 2015 defines "cyber threat indicators" in precise terms, focusing on information necessary to describe or identify malicious activities, vulnerabilities, and methods of defeating security controls. In contrast, the European Union's Network and Information Security (NIS) Directive adopts a broader approach, defining an "incident" as any event having an actual adverse effect on the security of network and information systems. These definitional differences have practical implications for reporting obligations, incident response, and cross-border data sharing. The rapid evolution of cyber threats, including the emergence of AI-powered attacks and sophisticated supply chain compromises, continually tests the adequacy of existing legal definitions.

The integration of cyber risks into broader enterprise risk management (ERM) frameworks has significant legal and practical implications. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has explicitly recognized cybersecurity as a critical component of ERM, underscoring the need for organizations to address cyber risks alongside traditional business risks such as financial, operational, and reputational risks. In the context of mergers and acquisitions, cyber risks have become a key due diligence consideration, with the

potential to materially affect transaction value. The Verizon-Yahoo deal, where the discovery of significant data breaches led to a $350 million reduction in the purchase price, serves as a stark illustration of the financial impact of cyber risks on corporate transactions. Legally, liability for cyber risks can arise under various theories, including negligence, breach of contract, and statutory liability. The concept of "reasonable security measures" is central to determining liability, with courts increasingly looking to industry standards and regulatory guidance to assess whether an organization's cybersecurity practices meet the required standard of care (Breaux & Baumer, 2011).

The legal framework addressing cybercrime is anchored by international agreements such as the Budapest Convention on Cybercrime, which establishes common definitions and procedures for investigating and prosecuting cyber offenses. This convention has been instrumental in fostering international cooperation, enabling law enforcement agencies to share information and coordinate investigations across borders. However, the transnational nature of cybercrime presents persistent challenges, including issues of jurisdiction, evidence collection, and extradition. The rapid pace of technological change further complicates enforcement, as lawmakers struggle to keep statutes up to date with new forms of cybercrime, such as ransomware-as-a-service and cryptocurrency-enabled money laundering. Legal frameworks must strike a balance between deterring criminal activity and fostering legitimate security research and innovation. Overly broad or vague laws risk criminalizing beneficial activities, while overly narrow statutes may leave gaps that cybercriminals can exploit. For organizations, the evolving legal landscape requires robust incident response plans and close collaboration with law enforcement to navigate the complexities of cybercrime investigations and enforcement actions.

Breach notification laws have become a critical component of the legal framework governing cybersecurity, imposing obligations on organizations to promptly disclose data breaches to affected individuals and regulatory authorities. The legal consequences of delayed or inadequate breach notifications can be severe, as demonstrated by high-profile cases such as Uber's 2016 data breach, where the company faced multiple lawsuits and regulatory actions for failing to promptly disclose the incident (De-Yolande et al., 2023). These laws often interact with other legal obligations, creating potential conflicts and complexities. For example, securities disclosure requirements may necessitate the public disclosure of breaches affecting publicly traded companies, as highlighted by the U.S. Securities and Exchange Commission's guidance on cybersecurity disclosures. The Equifax 2017 data breach is a notable case where breach notification laws and securities regulations intersected, resulting in both regulatory actions and shareholder lawsuits.

The concept of "fourth-party risk"-the risk posed by subcontractors of an organization's vendors-has emerged as a significant legal consideration in supply chain cybersecurity (Abdelmagid & Diaz, 2025). As organizations increasingly rely on complex, global supply chains, the potential for cyber threats to propagate through interconnected networks has grown. Some jurisdictions have responded by

introducing certification schemes for supply chain cybersecurity, such as the United Kingdom's Cyber Essentials program, which establishes baseline security requirements for suppliers and may impact liability assessments in the event of a breach. The global nature of supply chains presents challenges in applying and enforcing cybersecurity standards across different legal jurisdictions, particularly when suppliers are located in countries with varying levels of regulatory oversight. Legal frameworks are evolving to address issues such as software supply chain integrity, hardware backdoors, and the allocation of liability among parties in the event of a cyber incident.

Certain industries have developed specialized international cybersecurity standards to address their unique risks and regulatory requirements. In the financial sector, the SWIFT Customer Security Programme (CSP) mandates a comprehensive set of security controls for all SWIFT users, with significant legal implications for non-compliance, including potential disconnection from the SWIFT network. This program has set a global benchmark for cybersecurity in the banking sector, influencing both regulatory expectations and industry practices. The Basel Committee on Banking Supervision's guidance on cyber resilience provides a framework for regulators to assess banks' cybersecurity preparedness, and has been incorporated into national banking regulations, creating legally binding obligations for financial institutions. Similarly, the aviation industry has adopted the International Air Transport Association (IATA) Aviation Cyber Security Toolkit, which provides detailed guidance for airlines and airports and is referenced in civil aviation authorities' cybersecurity regulations. The IEC 62443 series, developed by the International Electrotechnical Commission, sets standards for industrial control systems security, with significant implications for the protection of critical infrastructure.

The legal aspects of cybersecurity governance in organizations are characterized by complexity, dynamism, and global interdependence. As cyber threats continue to evolve, so too must the legal frameworks that govern organizational responses (Del-Real & Díaz-Fernández, 2022). Organizations face an ongoing challenge to interpret and comply with a patchwork of national and international laws, sector-specific standards, and evolving regulatory expectations. Effective cybersecurity governance requires a proactive, risk-based approach that integrates legal, technical, and organizational measures. Boards of directors and senior executives must recognize cybersecurity as a core business issue, ensuring that adequate resources and oversight are dedicated to managing cyber risks. Legal counsel and compliance professionals play a critical role in navigating the evolving legal landscape, advising on the development and implementation of policies, procedures, and controls that meet both legal and business requirements. As the digital economy continues to expand, the importance of robust legal frameworks for cybersecurity governance will only grow, making it imperative for organizations to remain vigilant, adaptive, and informed.

Bibliography

Abdelmagid, A. M., & Diaz, R. (2025). Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems. *Risk Analysis*. https://doi.org/10.1111/risa.70026

Breaux, T. D., & Baumer, D. L. (2011). Legally "reasonable" security requirements: A 10-year FTC retrospective. *Computers & Security*, *30*(4), 178–193. https://doi.org/10.1016/j.cose.2010.11.003

Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. *International Cybersecurity Law Review*, *3*(2), 313–343. https://doi.org/10.1365/s43439-022-00069-4

De-Yolande, M. H., Doh-Djanhoundji, T., & Constant, G. Y. (2023). Breach Notification in the General Data Protection Regulation. *Voice of the Publisher*, *09*(04), 334–347. https://doi.org/10.4236/vp.2023.94026

Kello, L. (2021). Cyber legalism: why it fails and what to do about it. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab014

Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, & Benjamin Samson Ayinla. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369