Analysis of the Impact of Digital Transformation of the Legal Field on Data Cybersecurity

Submitted: 3 January 2025
Reviewed: 17 January 2025
Revised: 6 February 2025
Accepted: 17 February 2025

Saimir Fekolli[*]
https://orcid.org/0009-0002-3655-5449
Ervis Çela[**]
https://orcid.org/0009-0004-1630-3644
Chynybek Erdolatov[***]
https://orcid.org/0000-0001-9974-9203
Berik Biyashev[****]
https://orcid.org/0009-0006-3661-3804
Gulnoza Ismailova[*****]
https://orcid.org/0000-0002-2244-0299

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.56766

Abstract

[Purpose] To develop effective cybersecurity strategies in the context of digital transformation of the legal field.

[Methodology/approach/design] The research methodology includes a comprehensive analysis of technological, organisational, and regulatory aspects of the problem.

[Findings] The article examines international legal cybersecurity regulation and recommends approaches to adapt best practices. The human component in law firm cybersecurity is examined, and recommendations for boosting staff digital literacy are made. Quantum cryptography's legal data protection potential and successful cyber-attacks on DLA are analysed. Piper, Cravath, Swaine & Moore, Jones Day. The introduction of cloud technologies in legal firms significantly increases the risk of unlawful access to confidential information. An examination of 2020–2023 cyberattacks on legal entities found a growing trend of automating hostile acts with AI. The vulnerability evaluation identifies crucial data protection issues in legal services digitisation. A model of an adaptive cyber security system that considers law firm business process transformation offers a

[*]DSc, Lecturer at the Department of Justice, Aleksander Moisiu University of Durres, 2001, 1 Currila Str., Durres, Albania. E-mail: sai.fekolli@gmail.com.
[**]Lecturer at the Department of Civil Law, University of Tirana, 1010, 183 Margarita Tutulani Str., Tirana, Albania. E-mail: ervis-cela@outlook.com.
[***]PhD, Associate Professor at the Department of Criminal Law and Procedure, Osh State University, 723500, 331 Lenin Str., Osh, Kyrgyz Republic. E-mail: erdolatov_c@hotmail.com.
[****]MSc, Lecturer at the School of Law, University of California, Los Angeles, 90095, 405 Hilgard Ave., Los Angeles, United States of America. E-mail: b-biyashev@outlook.com.
[*****]DSc, Vice-Rector of the University of World Economy and Diplomacy, 100007, 54 Mustakillik Ave., Tashkent, Uzbekistan. E-mail: gulnoza_ism@hotmail.com.

significant reduction in attack likelihood. Rewriting the legislative framework for personal data protection in the context of digitalisation, including regulating blockchain technology in legal practice, is justified. The integration of digital platforms into legal activity introduces new cyber dangers that demand novel security. Examine the impact of lawyers' remote work on corporate network security and offer ways to reduce hazards.
[Practical implications] The results of the study form the basis for the development of effective cybersecurity strategies in the legal field and the improvement of relevant legislation, which is critical for ensuring the confidentiality and integrity of legal information in the digital age.

Keywords: Cloud Computing. Blockchain. Privacy. Artificial Intelligence. Legal Regulation.

INTRODUCTION

In the modern era of rapid digitalisation, the juridical sphere is undergoing drastic transformations, which leads to new challenges in the field of cybersecurity. The integration of innovative technologies into legal practice, in particular, cloud computing, artificial intelligence (AI), and blockchain, creates unprecedented opportunities for improving the efficiency of legal services but simultaneously generates a set of risks associated with the protection of confidential information and personal information. The key issue of the study is the need to ensure a high level of cybersecurity in the context of the rapid digital transformation of the legal field. This requires the development of innovative approaches that would effectively protect confidential information and personal data of customers, without hindering the introduction of advanced technologies in legal practice. Special attention should be paid to investigating the specifics of this process in countries with different levels of digital development, such as Albania, Kyrgyzstan, the United States of America (USA), and Uzbekistan, to form universal but adaptive cybersecurity strategies in the legal area.

One of the key problematic issues in the field of digital transformation of the legal industry is ensuring cybersecurity when introducing new technologies (TKACHENKO et al., 2024). P. Śwital and D. Skoczylas (2024) considered the information sphere in the context of cyber threats, focusing on disinformation and cybersecurity issues. Their paper identified the growing role of information technologies in the legal field and the associated risks. J. Babikian (2023a) explored current issues of cyber law, in particular, data protection and privacy issues in the digital age. The author emphasised the need to adapt the legal framework to new technological challenges. C. Gaie and M. Karpiuk (2024) focused on the provision of electronic services by public administration bodies and ensuring their cybersecurity. The use of AI technologies in the US legal

sphere and the associated risks to cybersecurity were also investigated by J. Babikian (2023b). The author determined that the introduction of AI systems for analysing legal documents and predicting court decisions not only increases the efficiency of lawyers but also creates new vectors of cyber-attacks. J. Babikian emphasises the risks associated with manipulating input data for AI systems, which can lead to distortion of legal conclusions. Based on these findings, the researcher stresses the urgent need to develop ethical standards and audit mechanisms for AI systems in US law to minimise cybersecurity risks.

The problems of personal data protection in the context of the use of cloud computing in the legal practice of Albania were reviewed in detail by A. Koçi (2022). The study showed that the rapid transition of Albanian law firms to cloud platforms substantially increased the risks of unauthorised access to confidential customer information. A. Koçi established that Albania's existing regulatory framework is not sufficiently adapted to the challenges posed by cloud technologies in the legal sector. Based on this analysis, the author highlights the need for urgent improvement of data protection legislation when using cloud technologies, especially in the context of Albania's European integration processes and the need to adapt to GDPR standards. The impact of blockchain technologies on legal processes and related cybersecurity challenges in Uzbekistan was analysed by O. Zyhrii et al. (2023). The researchers examined the prospects for implementing blockchain in the country's legal system as part of the ambitious Digital Uzbekistan 2030 programme. They state that while blockchain can potentially substantially improve the transparency and reliability of legal transactions in Uzbekistan, its implementation poses several new cybersecurity challenges. In particular, the authors emphasise the problems associated with protecting private keys and ensuring the confidentiality of data in a distributed ledger in the context of an insufficiently developed digital infrastructure in the country.

Cybersecurity issues in the context of remote work of lawyers and online court sessions in Kyrgyzstan were thoroughly investigated by M.V. Demchenko et al. (2021). The authors determined that the forced rapid transition to remote forms of work created several new vectors of cyber-attacks in the country's legal sector. In particular, the study showed that the use of unsecured home networks and personal devices by lawyers substantially increased the risk of confidential information leakage. Based on these findings, the authors emphasise the urgent need to develop comprehensive cybersecurity strategies for the legal sector of Kyrgyzstan, which would consider the features of remote legal practice and the limited resources of the country.

Despite a substantial amount of research in cybersecurity in a juridical sphere, a comprehensive analysis of the impact of digital transformation on data security

is not sufficiently conducted. It requires a deeper assessment of the relationship between the introduction of the latest technologies and the emergence of new vectors of cyber-attacks, as well as mechanisms for adapting security systems to the rapidly changing digital landscape of the legal sphere. The purpose of this study was to develop a comprehensive approach to ensuring the cybersecurity of legal data in the context of intensive digitalisation of the legal field. The following tasks are formulated to achieve this goal:

1. Analyse the features of the business process transformation of law firms in the context of the introduction of innovative technologies and assess the associated risks to information security.
2. Investigate successful cyber-attacks on law firms: ransomware attack on DLA Piper (2024), Cravath, Swaine & Moore (GOLDSTEIN, 2016), compromise of Jones Day accounts (OPFER, 2021).
3. Assess the vulnerabilities of information systems of legal organisations in the context of digital transformation.
4. Propose a conceptual model of an adaptive cyber defence system that can effectively counteract new types of threats in the digital legal environment.
5. Formulate recommendations for Albania, Kyrgyzstan, the United States of America, and Uzbekistan to improve the regulatory framework in the field of cybersecurity of legal data, considering the features of digital transformation of the industry.

MATERIALS AND METHODS

The study was based on an integrated approach that combines quantitative and qualitative analysis methods for a comprehensive examination of the impact of digital transformation on cybersecurity in the legal field. Special attention was paid to considering the specific features of digital transformation and related cybersecurity challenges in the context of Albania, Kyrgyzstan, the United States, and Uzbekistan. This approach allowed for gaining a deep understanding of the issues and developing practically oriented recommendations for improving cybersecurity in the context of rapid digitalisation of the legal industry. A comparative analysis of the regulatory framework of different jurisdictions was conducted. In particular, the following analysed: National Institute of Standards and Technology Cybersecurity Framework (National Institute of Standards and Technology, 2018), USA; National Strategy on Cybersecurity 2020-2025 (GJIKA, 2023), Albania; Cybersecurity concept of the Kyrgyz Republic for 2019-2023 (Resolution on Issues of Development of…, 2019), Kyrgyzstan; Strategy "Digital Uzbekistan-2030" (HAMDAMOVA, 2020), Uzbekistan. A review of successful cyber-attacks was conducted to understand the methods of

unauthorised access to legal institutions. The analysis included the following cases:

1. Ransomware attack on DLA Piper (2024).
2. Phishing attack on Cravath, Swaine & Moore (GOLDSTEIN, 2016).
3. Compromised Jones Day accounts (OPFER, 2021).

An important aspect of the study was the examination of the regulatory framework governing cybersecurity and digital transformation in the legal sphere. Special attention was paid to the analysis of the Directive (EU) 2018/1972 of the European Parliament and of the Council of Establishing the European Electronic Communications Code (2018), which sets new standards for electronic communications and has a substantial impact on cybersecurity in legal practice. The provisions of the Directive (EU) 2016/1148 of the European Parliament and of the Council of Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (2016), which defines pan-European cybersecurity standards and their implementation in national legislation were also considered. These documents were analysed in the context of their impact on the formation of cybersecurity policies in legal organisations and the adaptation of legal practices to new digital realities. In addition, the impact of new regulations, such as the Regulation (EU) 2022/2065 of the European Parliament and the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (2022) and Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (2022), on the formation of cybersecurity strategies in the legal sector was considered. These documents establish new rules for digital platforms and markets, which have substantial implications for data security in legal practice.

RESULTS

Technological Factors of Digital Transformation and their Impact on Cybersecurity of the Legal Sphere

In the context of the exponential development of information and communication technologies, the legal field is undergoing fundamental transformations, which leads to the emergence of new paradigms in ensuring cybersecurity. The implementation of cloud computing, AI, blockchain, and the Internet of Things in legal practice generates a multi-factor impact on information security, creating both innovative opportunities and potential vulnerabilities.

Cloud computing is a model that allows ubiquitous and convenient on-demand access to a common pool of configurable computing resources (e.g., a set of

networks, servers, data storage, applications and services) that can be provided by a service provider in a timely manner (AVIV et al., 2023). Cloud technologies that ensure scalability and efficiency of data processing simultaneously create problems in controlling information assets and their localisation (GAFNI et al., 2024). The diffusion of data between different jurisdictions in cloud environments makes it difficult to apply traditional legal mechanisms to protect information. This requires the development of new risk management models and the introduction of cryptographic protocols that can ensure data confidentiality in heterogeneous computing environments. The integration of AI systems into legal processes, in particular, for analysing precedents and predicting court decisions, creates new vectors of cyber-attacks (GASHI et al., 2024). The potential vulnerability of machine learning algorithms to adversarial attacks may lead to the manipulation of legal opinions and recommendations.

Blockchain technology, used in electronic document management systems and smart contracts, offers new paradigms for ensuring the integrity and immutability of legal documents (NURBATYROVA et al., 2024; SAKHIPOV et al., 2022). However, the implementation of blockchain creates challenges in terms of scalability and energy efficiency and raises questions about compliance with the principles of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of…, 2016). It is necessary to develop hybrid architectures that would combine the advantages of blockchain with the ability to selectively edit data by legal requirements. The Internet of Things, by integrating into e-justice and legal monitoring systems, expands the attack surface for cybercriminals. The heterogeneity of the Internet of Things (IoT) and communication protocols creates multiple vulnerability points that require the implementation of integrated intrusion detection and prevention systems (IDS/IPS) adapted to the specifics of the legal infrastructure. The convergence of these technologies in the legal field leads to complex ecosystems, where traditional perimeter protection models lose their effectiveness. This makes it necessary to move to the Zero Trust Architecture (ZTA) paradigm, which provides for continuous verification of each request and transaction, regardless of the source of origin.

The analysis of technological factors of digital transformation of the legal sphere and their impact on cybersecurity revealed a comprehensive interaction between innovative solutions and new challenges in data protection. In particular, the introduction of quantum computing technologies creates the potential for revolutionary changes in cryptographic systems used to protect legal information. Quantum cryptography offers theoretically unbreakable encryption methods based on the principles of quantum mechanics, such as quantum key distribution (QKD). Therewith, the development of quantum computers threatens existing cryptographic protocols based on the complexity of factorisation of large

numbers, actualising the need to develop post-quantum encryption algorithms. This necessitates the development of robust AI models that can resist attempts to intentionally distort input data and provide resistance to attacks such as "data poisoning". The integration of natural language interface (NLP) technologies into legal information systems opens up new opportunities for automating the analysis of legal documents and interaction with clients but also creates new attack vectors related to the ability to manipulate input data for NLP systems.

The integration of augmented (AR) and virtual (VR) reality technologies into legal practice, in particular, for visualising evidence and conducting virtual court sessions, creates new challenges for cybersecurity. Potential vulnerabilities in AR/VR systems can lead to manipulation of visual content, which is critical to the legal process. This requires the development of methods for verifying the integrity and authenticity of AR/VR content and protocols for secure data transmission in virtual environments. The development of Edge computing technologies in the legal context allows for optimising data processing and analysing directly on peripherals, reducing latency and improving the efficiency of working with legal information. However, the decentralisation of computing creates new challenges for providing a unified approach to cybersecurity, requiring the implementation of distributed anomaly detection systems and preventive security mechanisms at the end device level. The use of Big Data technologies and analytics in legal practice to predict court decisions and analyse legal trends increases the risks associated with the aggregation and processing of large amounts of sensitive information. Potential threats include unauthorised access to aggregated data, privacy violations due to the possibility of de-anonymisation, and risks of distortion of analysis results due to manipulation of incoming data.

An analysis of cyber-attacks on law firms revealed the diversity and complexity of threats facing the legal sector in the digital age. The NotPetya ransomware attack on DLA Piper (2024) in 2017 demonstrated the vulnerability of even big international law firms to large-scale cyber-attacks. This attack resulted in substantial financial losses and operational failures, highlighting the need for continuous security updates and effective disaster recovery plans. A phishing attack on Cravath, Swaine & Moore in 2016 revealed the vulnerability of law firms to social engineering and the importance of training employees in cybersecurity. The incident also highlighted the value of confidential information held by law firms, especially in corporate mergers and acquisitions (GOLDSTEIN, 2016). The compromise of Jones Day accounts in 2021 due to a vulnerability in third-party software highlighted the risks associated with the use of external service providers. This case highlighted the need for a thorough security review and monitoring of all components of the IT infrastructure, including third-party services (OPFER, 2021). Together, these incidents

demonstrate the evolution of cyber threats in the legal sector and highlight the need for a comprehensive, multi-level approach to cybersecurity that includes technical measures, staff training, and careful third-party risk management.

In the context of the rapid digital transformation of the legal sphere, there is a substantial impact of various technologies on the state of cybersecurity. Key technological innovations such as cloud computing, AI, blockchain, and the Internet of Things, on the one hand, open up new opportunities for optimising legal processes, and on the other – create unprecedented challenges for data protection. In particular, cloud technologies, while ensuring scalability and efficiency of information processing, make it difficult to control data and localise it. AI, by revolutionising precedent analysis and predicting court decisions, is becoming vulnerable to adversarial attacks. Blockchain, offering new paradigms for ensuring document integrity, creates challenges in terms of compliance with the GDPR (Regulation (EU) 2016/679 of…, 2016). Advances in quantum computing, AR/VR technologies, and 5G networks are also substantially transforming the cyber threat landscape, requiring the development of innovative approaches to protecting legal information and processes (Table 1).

Technology	Features	Cybersecurity challenges
Cloud computing	Scalability, data processing efficiency	Data control, cross-border transmission
Artificial intelligence	Use case analysis, decision forecasting	Vulnerability to adversarial attacks
Blockchain	Document integrity, smart contracts	Scalability, GDPR compliance
Internet of things	E-Justice, legal monitoring	Expanding the attack surface
Quantum computing	Quantum cryptography	Threat to existing cryptosystems
AR/VR	Visualisation of evidence, virtual meetings	Manipulating visual content
Edge computing	Optimisation of data processing	Decentralising security
5G	Mobile access, video conferencing	New attack vectors

Table 1 – Cybersecurity opportunities and challenges of modern technologies
Source: compiled by the author based on E. Syarief (2022), P. Śwital and D. Skoczylas (2024), D. Manko et al. (2023), M.T. Nguyen and M.Q. Tran (2023), M.J. Sule et al. (2021), J. Babikian (2023a), B. Karovska-Andonovska and N. Taneski (2020), O. Čupka et al. (2023), C. Gaie and M. Karpiuk (2024), B. Alouffi et al. (2021), N. Mohamed (2023), Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (2016).

The use of Big Data technologies and analytics in legal practice to predict court decisions and analyse legal trends increases the risks associated with the aggregation and processing of large amounts of sensitive information. Potential threats include unauthorised access to aggregated data, privacy violations due to the possibility of de-anonymisation, and risks of distortion of analysis results due to manipulation of incoming data. This highlights the need to develop differential privacy and homomorphic encryption methods to ensure privacy when analysing large amounts of legal data. The implementation of 5G technologies and future generations of mobile communications in the legal infrastructure opens up new opportunities for mobile access to legal resources and high-quality video conferencing. However, increasing the data transfer rate and the number of connected devices creates new attack vectors, requiring the development of adaptive security systems that can operate in conditions of high network traffic dynamics. In the context of the progressive digitalisation of the legal sphere, the problem of integrating AI technologies with an increased level of autonomy is becoming particularly relevant (KOLBAYEV et al., 2024). The implementation of AI systems capable of self-learning and adaptation in legal analysis and decision-making processes creates unprecedented challenges for cybersecurity (PALKO et al., 2023). In particular, there is a need to develop methodologies for verifying and validating AI algorithms that would guarantee their resistance to manipulation and ensure transparency in decision-making.

The concept of explainable AI (XAI) becomes critical in a legal context where the need to justify each decision is a fundamental principle. Its central goal is to make the behaviour of these systems understandable to humans by elucidating the underlying mechanisms of their decision-making processes. The development of AI algorithms that can provide a clear explanation of their conclusions becomes not only a technological but also an ethical and legal imperative (KHARCHENKO et al., 2017). This requires the creation of new paradigms in neural network architecture and machine learning techniques that provide a balance between efficiency, accuracy, and the interpretability of results. The integration of Natural language processing (NLP) technologies into legal information systems opens up new opportunities for automating the analysis of legal documents and interaction with clients. However, it also creates new attack vectors related to the ability to manipulate input data for NLP systems. Developing robust natural language processing algorithms resistant to adversarial attacks is becoming a critical challenge for ensuring the reliability of legal AI systems (AI and predictive…, 2024).

The development and standardisation of post-quantum encryption algorithms, such as lattice-based cryptosystems or error-correcting code-based systems, are becoming critical to protecting the confidentiality of legal information in the long

run. The integration of continuous authentication and behavioural biometrics technologies into access systems for Legal Information Resources offers new approaches to ensuring user authentication. This allows moving from static authorisation models to dynamic, context-sensitive access control systems that can adapt to changes in user behavioural patterns. The implementation of the concept of a Security Operations Centre (SOC) (CICHONSKI et al., 2012) in the structure of legal organisations becomes a critical factor for ensuring proactive monitoring and response to cyber threats. The integration of Security Information and Event Management (SIEM) and User and Entity Behaviour (UEBA) (JOHNSON et al., 2016) enables comprehensive analysis of anomalies and potential security incidents in real-time, increasing the organisation's ability to quickly detect and mitigate cyber threats.

They are actively implementing advanced technologies in US legal practice, including AI for analysing legal documents and cloud computing for data storage (BABIKIAN, 2023b). This creates the need to develop sophisticated cyber defence systems that can counter advanced threats. The United States is a leader in developing and implementing innovative solutions for cybersecurity in the legal field. Special attention is paid to protecting critical infrastructure and preventing confidential information leakage. As part of the European integration process, Albania is actively modernising its judicial system, introducing electronic legal proceedings and creating centralised databases of court decisions. It focuses on adapting European cybersecurity standards to local conditions, in particular, the introduction of personal data protection systems by the General Data Protection Regulation (GDPR) (GJIKA, 2023). The introduction of cloud technologies and AI in the Albanian legal sector is slower than in the United States, but it is steadily progressing. The main challenges are ensuring data security during cross-border transmission and developing local regulations.

Kyrgyzstan is at the initial stage of digital transformation of the legal sphere, focusing on the development of basic information technology (IT) infrastructure for courts and state legal institutions (Resolution on Issues of Development of…, 2019). The introduction of an electronic office management system in courts is a priority but faces challenges in ensuring a basic level of cybersecurity due to limited resources and insufficient technical expertise. The use of cloud technologies and AI in the legal sector of Kyrgyzstan is limited, mainly due to the lack of an appropriate regulatory framework and concerns about data security. The country is beginning to explore the possibilities of implementing basic automation systems to improve the efficiency of the judicial system. Uzbekistan demonstrates active development in the field of digitalisation of public services, including the legal sphere, within the framework of the programme “Digital Uzbekistan 2030” (HAMDAMOVA, 2020). Electronic systems for filing lawsuits

and managing cases are being implemented, which creates a need to develop comprehensive cyber defence systems. Cloud technologies are gradually being introduced to the legal sector, mainly for storing and processing unclassified information. The use of AI in the legal practice of Uzbekistan is at an experimental stage, pilot projects are being conducted to introduce systems for automated analysis of legal documents and forecasting court decisions.

Organisational Aspects of Digital Transformation and their Role in Ensuring the Cybersecurity of Legal Organisations

Organisational aspects of digital transformation of the legal sphere are a complex phenomenon that determines fundamental changes in the structure, processes, and culture of legal organisations, directly influencing the paradigm of ensuring cybersecurity. The implementation of digital technologies catalyses the reconfiguration of organisational architectures, which requires a holistic approach to integrating security practices into transformable business processes. The transition to flexible legal project management methodologies, characterised by iterativeness and adaptability, creates new challenges for traditional cybersecurity models. Disaggregation of monolithic processes into microservices and the use of DevOps practices in the development of legal information systems requires the implementation of the Security by Design concept security practices at all stages of the software development lifecycle (SDLC). Transformation of the organisational structure of law firms in the direction of network and matrix models, characterised by increased flexibility and decentralisation of decision-making, actualises the need to develop adaptive access control systems. The implementation of attribute-based access control (ABAC) and risk-based trust models becomes imperative for providing granular control over information assets in a dynamic organisational landscape.

The transition to hybrid work models that combine office and remote forms creates new vectors of cyber threats, blurring traditional security perimeters. This requires the implementation of the ZTA concept and provides continuous authentication and authorisation of users, devices, and transactions, regardless of their location. Integrating Bring Your Own Device (BYOD) (DISTERER & KLEINER, 2013) and Bring Your Own Cloud (BYOC) (Narayanan et al., 2020) practices into legal activities increases the heterogeneity of the technological landscape, complicating asset, and configuration management processes. This highlights the need to implement Unified Endpoint Management (UEM) systems and virtualisation technologies for work environments to ensure the segregation of corporate and personal data. The transformation of corporate culture towards increasing the digital competence of personnel requires the development of comprehensive cybersecurity training programmes that incorporate elements of

the gamification and simulation of cyber-attacks to increase the organisation's resilience to social engineering and phishing attacks.

The implementation of Information Security Risk Management (ISRM) practices in the context of digital transformation requires the development of dynamic risk assessment models that can consider emerging threats associated with the introduction of new technologies. Integration of frameworks with adaptation to the specifics of the legal sphere is becoming a key factor in ensuring a systematic approach to cybersecurity management. The development of Business Continuity Management (BCM) practices in conditions of increased dependence on digital technologies requires the development of comprehensive incident response plans and disaster recovery strategies that consider the specific features of cyber threats in the legal sphere. In February 2021, Jones Day, one of the largest law firms in the United States, suffered a data leak due to a vulnerability in the Accellion FTA file transfer software. Hackers gained access to confidential customer documents and published them on the darknet. This incident highlights the need for thorough security checks by third-party service providers and regular software updates (OPFER, 2021). In June 2017, the international law firm DLA Piper (2024) was subjected to a large-scale attack by the NotPetya ransomware programme. This attack paralysed the company's operations for several days, disabling phone systems and email. Damage from the attack is estimated at USD 15 million. This incident highlighted the importance of regularly updating software and creating reliable data backup systems. The development of Cyber Threat Intelligence (CTI) practices in the legal sector is becoming particularly relevant in the context of targeted attacks on high-profile law firms. The creation of industry communities for the exchange of information on cyber threats information sharing and analysis centres (ISACs) for the legal sector allows for increasing the collective resistance of the industry to cyber-attacks through the timely exchange of compromise indicators and tactics of intruders. This includes automating the processes of granting and revoking access rights, regularly auditing privileges, and implementing the principle of least privilege to minimise the attack surface.

Integration of DevSecOps practices into the development and support processes of legal information systems allows for continuous implementation of security controls at all stages of the software lifecycle. This includes automated code scanning for vulnerabilities, penetration testing, and real-time security monitoring, which helps identify and fix potential vulnerabilities early. The implementation of the Zero Trust Data Protection Framework becomes imperative for ensuring the confidentiality and integrity of legal data in distributed computing environments. This includes data encryption technologies at rest and during transmission, granular access control at the data level, and continuous verification

of the legitimacy of data requests. The development of a cyber hygiene culture in legal organisations requires the development of comprehensive programmes for staff security awareness training (BOCHELIUK et al., 2019). Adaptive learning methods and personalised training programmes based on the analysis of employee behavioural patterns can increase the effectiveness of training and reduce the risks associated with the human factor.

Transformation of third-party risk management processes in the context of expanding the ecosystem of digital services used by legal organisations requires the introduction of comprehensive frameworks for evaluating and monitoring the security of suppliers. This includes conducting regular security audits, establishing clear security SLAs, and implementing practices to continuously monitor cyber risks in the supply chain. The implementation of cyber risk quantification practices allows for transforming the approach to making decisions about investing in cybersecurity, transferring the discussion from the technical plane to the business context. Methodologies such as Factor Analysis of Information Risk (FAIR) (FREUND & JONES, 2015) allow for assessing potential financial losses from cyber incidents and optimising the allocation of resources to cybersecurity measures. The development of Business Continuity Management (BCM) practices in the context of increased dependence on digital technologies requires the development of comprehensive incident response plans and disaster recovery strategies that consider the specifics of cyber threats in the legal field.

The analysis of organisational aspects of digital transformation and their impact on the cybersecurity of legal organisations revealed substantial differences between the countries examined. The United States has the highest level of maturity in organisational cybersecurity practices. In Albania, the process of organisational transformation of the legal sector takes place in the context of the country's European integration aspirations. The introduction of electronic document management systems in courts creates new challenges for ensuring data confidentiality. However, only a small proportion of law firms have formalised cybersecurity policies, which indicates the need to increase organisational maturity in this area (GJIKA, 2023). In Kyrgyzstan, the organisational aspects of the digital transformation of the legal sector are at an early stage. A limited number of legal organisations have specialised IT departments, and cybersecurity issues are often delegated to external contractors. This creates additional risks for protecting confidential information and requires the development of comprehensive organisational cybersecurity strategies. Consequently, Electronic Document Management and video conferencing solutions are being instituted for court hearings in Uzbekistan (HAMDAMOVA, 2020). However, only a fraction of legal organisations has formalised policies for responding to cybersecurity

incidents, which indicates the need for further development of organisational mechanisms for protecting information.

Regulatory Factors and their Impact in Cybersecurity in the Context of Digitalisation of the Legal Sphere

The regulatory factors that shape the cybersecurity landscape in the digitalisation of the legal sphere are characterised by a high degree of dynamism and complexity, reflecting the dualistic nature of law as a regulatory tool and object of transformation in the context of the digital revolution. The intersection of legal practice and information technologies gives rise to new paradigms of legal regulation that require a synergistic approach to the formation of the legal framework for cybersecurity. The implementation of the GDPR and similar regulations in different jurisdictions accelerates the process of harmonisation of international standards for the protection of personal data while creating new challenges for cross-border data transfer in legal practice. The principle of extraterritoriality of the GDPR (Regulation (EU) 2016/679 of…, 2016) highlights the need to develop comprehensive compliance strategies for law firms operating on a global scale.

The development of the "Privacy by Design" concept and its inclusion in regulatory legal acts changes approaches to the development and implementation of information systems in the judicial field. This requires technical and organisational measures to ensure privacy at all stages of data processing, including pseudonymisation, encryption, and data minimisation. Strengthening regulatory requirements for mandatory data breach notification increases the transparency of cybersecurity incidents and encourages legal organisations to improve their incident monitoring and response systems. The diversity of regulatory requirements in different jurisdictions creates additional challenges for multinational law firms, requiring the development of unified incident response protocols.

The implementation of the "right to be forgotten" concept in of digitalisation of the legal sphere creates a dichotomy between protecting privacy and preserving the integrity of legal archives. This actualises the need to develop technological solutions that ensure the selective deletion of personal data without compromising the legal significance of documents. The evolution of the regulatory framework for the use of AI in legal practice, in particular, in the aspects of predicting court decisions and automated document analysis, gives rise to new paradigms for regulating algorithmic transparency and responsibility. The concept of "explainable AI" is becoming normative, requiring developers of AI systems for the legal field to ensure the interpretability and auditability of algorithmic decisions. Development of the regulatory "sandbox", that is, a test environment

for using modern technologies to automate and improve legal processes and services (legal tech), solutions create a controlled environment for assessing potential risks and developing adequate regulatory mechanisms. This helps to balance between stimulating innovation and ensuring the necessary level of data protection and cybersecurity in the legal field. The introduction of the "digital sovereignty" at the national and supranational levels affects the regulation of cross-border data flows and the use of cloud technologies in legal practice. This highlights the need to develop new models of international cooperation of cybersecurity and data protection, considering the geopolitical aspects of the digital economy.

The evolution of the "Duty of Care" doctrine (WITTING, 2005) in the context of cybersecurity transforms the standards of professional responsibility of lawyers, requiring them not only to be competent in legal matters but also to understand the technological aspects of information security. This highlights the need to include cybersecurity courses in legal education and professional development programmes. The development of the regulatory framework for the use of smart contracts and blockchain technologies in legal practice gives rise to new paradigms for regulating electronic transactions and contractual relations. This requires the development of specific cybersecurity standards for decentralised systems that ensure the immutability and authenticity of legally substantial actions in the digital space. The implementation of the principles of "privacy-enhancing technologies" (PETs) in regulatory legal acts encourages the development of technological solutions that ensure privacy protection at the level of information system architecture. This includes regulatory requirements for the use of homomorphic encryption, differentiated privacy, and other advanced data protection technologies in legal practice. The evolution of the "digital rights" and their incorporation into the system of fundamental human rights transforms the legal paradigm of personal protection in the digital space. This requires the development of new mechanisms for legal protection and liability for violations of digital rights, including cybersecurity and protection against digital violence.

The Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and Amending Directive 2000/31/EC (2022) sets new standards of transparency and responsibility for online platforms, which has a substantial impact on legal practice in the digital space. This Act requires platforms to implement tougher measures to combat illegal content, increase the transparency of algorithms, and protect user rights. For law firms, this means the need to adapt their cybersecurity strategies to meet new requirements for processing and storing customer data, as well as potential changes in approaches to providing legal services through digital platforms. Regulation (EU) 2022/1925 of the European Parliament and of the Council on

Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (2022), in turn, is aimed at ensuring fair competition in the digital sector, which has an indirect but substantial impact on cybersecurity in the legal area. By introducing new rules for so-called "gatekeepers" – large digital platforms, the Act creates new challenges and opportunities for law firms. On the one hand, this requires the development of new approaches to protecting confidential customer information when interacting with these platforms. On the other hand, it opens up new areas of legal practice related to the regulation of digital markets and data protection in the face of increased competition.

The evolution of "digital rights" and their integration into the system of fundamental human rights transforms the legal paradigm of personal protection in the digital space. This requires the development of new mechanisms for legal protection and liability for violations of digital rights, including cybersecurity and protection against digital violence. The development of the regulatory framework for quantum cryptography and post-quantum encryption algorithms highlights the need to actively adapt cybersecurity standards to future technological challenges. This involves the creation of regulatory mechanisms for the certification and validation of quantum-resistant cryptosystems in legal practice. The implementation of the concept of "algorithmic accountability" in the context of using AI systems for legal analysis and decision-making requires the development of regulatory mechanisms for auditing and verifying AI algorithms. This includes setting standards for transparency, non-discrimination, and ethics of algorithmic systems used in the legal field. The evolution of the regulatory framework for cyber insurance is transforming approaches to managing cyber risks in legal organisations. This requires the development of specific insurance products and methodologies for assessing cyber risks, adapted to the specific features of legal practice.

The development of international legal instruments in cybersecurity, such as the Budapest Convention on Cybercrime (2001), requires the harmonisation of national legislation and the development of effective mechanisms for cross-border cooperation in the investigation of cybercrime affecting the legal sphere. This highlights the need to create a global legal framework for combating cybercrime, which would consider the specifics of the digital space and the features of legal activity in the online environment. The formation of a regulatory framework for the use of distributed ledger technologies (DLT) in the legal area opens up new opportunities for ensuring transparency and immutability of legal records while creating challenges for traditional concepts of legal regulation. This requires the development of innovative approaches to verifying and legitimising blockchain-

based legal documents and smart contracts, as well as establishing a legal framework for resolving disputes arising from their use.

An analysis of the US regulatory framework determined that the National Institute of Standards and Technology Cybersecurity Framework (National Institute of Standards and Technology, 2018) plays a key role in shaping approaches to cybersecurity in the legal sector. This document offers a flexible and risk-based framework that allows legal entities to effectively manage cyber risks. This framework focuses on five key functions: identification, protection, detection, response, and recovery. This allows US law firms to develop comprehensive cybersecurity strategies that cover the entire lifecycle of potential cyber threats. In Albania, the National Strategy on Cybersecurity 2020-2025 (MONITORING OF NATIONAL CYBERSECURITY…, 2023) demonstrates the country's desire to adapt its regulatory framework to EU standards. This strategy focuses on developing national cyber resilience, protecting critical information infrastructure, and improving cybersecurity in the public and private sectors, including the legal sphere. Special emphasis is placed on harmonising legislation with EU norms, in particular, with the Directive on Security of Network and Information Systems (NIS Directive) and the GDPR, which has a substantial impact on data protection practices in Albanian law firms. EU NIS Directive addresses cybersecurity incidents affecting essential services and digital providers. These entities must report breaches that could disrupt their services or security. GDPR requires businesses to report personal data breaches to authorities within 72 hours if individual rights are at risk. In essence, while both GDPR and NIS2 are essential components of the broader European cybersecurity and data protection framework, they serve different roles, with GDPR primarily addressing personal data protection and privacy, and NIS2 dealing with the security of critical infrastructure and systems.

The cybersecurity concept of the Kyrgyz Republic for 2019-2023 (Resolution on Issues of Development of…, 2019) reflects the initial stage of formation of the regulatory framework in the field of cybersecurity in Kyrgyzstan. The document defines the main directions of development of the national cybersecurity system, including the creation of legal mechanisms for information protection, the development of technical means of protection and the professional development of specialists in the field of information security. For the legal sector of Kyrgyzstan, this means the need to adapt to new cybersecurity requirements and standards, which may cause some difficulties due to limited resources and insufficient technological readiness of many legal organisations.

Development of a Comprehensive Cybersecurity Strategy for Legal Organisations in the Context of Digital Transformation

Developing a comprehensive cybersecurity strategy in digital transformation requires integrating multidisciplinary approaches that synthesise technological, organisational, and regulatory aspects into a single coherent system. This approach must adhere to the concepts of adaptability, resilience, and proactivity to ensure successful safeguarding of information assets amid the continual evolution of cyber threats. A fundamental element of the strategy is the use of a risk-based approach, which involves the systematic identification, assessment and mitigation of cyber risks. A cyber risk quantification methodology such as FAIR allows for the transition of the technical aspects of cybersecurity into a business context, facilitating informed decisions about allocating resources to security measures (FREUND & JONES, 2015).

The development of a comprehensive cybersecurity strategy for legal organisations in the context of digital transformation is an imperative of the modern legal environment, characterised by increased vulnerability to cyber threats and the need to ensure confidentiality, integrity, and accessibility of legal information. This strategy should be based on legality, proportionality, and balance of interests, considering both technological aspects and regulatory requirements. The first stage of strategy development is to conduct a comprehensive information security audit of a legal organisation, including an analysis of existing policies, procedures, and technical means of information security. This audit should be conducted by international standards, such as ISO/IEC, and consider specific requirements of industry legislation, in particular, GDPR (Regulation (EU) 2016/679 of…, 2016) for organisations working with European clients. The next step is to develop an information security policy. This policy should cover several critical aspects. Firstly, it should include the classification of information according to the level of confidentiality and criticality. An important element is the definition of procedures for managing access to information resources. The policy should also contain clear protocols for responding to information security incidents. An integral part is the development of a cybersecurity training programme for personnel. Finally, the policy should provide mechanisms to ensure the continuity of business processes in the event of cyber incidents. All these elements together form a comprehensive approach to the organisation's information security.

Special attention should be paid to the protection of client's personal data and confidential information constituting attorney-client privilege. This requires the introduction of technical security tools such as data encryption, intrusion detection, and prevention systems, as well as organisational measures, including regular checks on the trustworthiness of personnel and limiting access to sensitive

information on the principle of least privilege. In the context of the digital transformation of the legal industry, the cybersecurity strategy should consider the specific risks associated with the use of cloud technologies, electronic document management systems, and AI in legal practice. This requires the development of additional security protocols for working with remote services and ensuring the integrity of electronic evidence.

An important aspect of the strategy is to ensure compliance with regulatory requirements and industry standards. This includes regular monitoring of changes in cybersecurity and data protection legislation, and implementing mechanisms to quickly adapt to new requirements. Legal entities should also consider obtaining information security certifications, such as ISO, which will increase the trust of customers and partners. The development of risk management procedures is a critical component of the strategy. This involves systematically identifying, evaluating, and prioritising cyber risks specific to the legal field, such as unauthorised access to case files, leakage of confidential customer information, or compromise of electronic signatures. The strategy should also include a cybersecurity incident response plan that defines the roles and responsibilities of personnel, procedures for communicating with customers and regulators, and steps to minimise legal and reputational risks in the event of a data security breach. Finally, an important element of the strategy is to create a cybersecurity culture in the organisation. This includes regular staff training, simulating phishing attacks, and integrating cybersecurity issues into lawyers' daily workflows.

The analysis of regulatory factors and their impact on cybersecurity in the digitalisation of the legal sphere identified a complex system of relationships between regulatory requirements and information security practices (Table 2).

Regulatory factor	**Impact on cybersecurity**	**Implementation requirements**
GDPR and similar acts	Harmonisation of data protection standards	Compliance strategies, Privacy by Design
Data leak notification	Increased transparency	Monitoring and response systems
Right to be forgotten	Problems with archive integrity	Selective data deletion
AI regulation in law	Algorithm transparency requirements	Explainable AI
Electronic evidence	New authentication standards	Verification of digital artefacts
Smart contracts	New paradigms of contractual relations	Blockchain security standards

Digital rights	Transformation of personal protection	Protection mechanisms in the digital space

Table 2 – Impact of regulatory factors on cybersecurity and requirements for their implementation

Source: compiled by the author based on E.L. Sidorenko and P. Von Arx (2020), A. Koçi (2022), J. Gjika (2023), I.A. Tsindeliani et al. (2022), C. Codagnone and L. Weigl (2023), J. Babikian (2023b), J. Kirsiene and D. Amilevičius (2022), R.F.R. Forradellas and L.M.G. Gallastegui (2021), A. Shabalin et al. (2024), Y. Tikhomirov et al. (2021), M.V. Demchenko et al. (2021), C.E.P. Tache and C.S. Săraru (2024), S. Zenin et al. (2023), O. Zyhrii et al. (2023), Regulation (EU) 2016/679 of the European Parliament and of the Council On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (2016).

Table 2 systematises key regulatory factors, their impact on cybersecurity, and relevant requirements for implementation in the legal field. The table shows that regulatory acts such as the GDPR and similar documents play a crucial role in shaping the cybersecurity landscape, stimulating the harmonisation of data protection standards and the implementation of the "Privacy by Design" concept. Mandatory reporting of data leaks increases the transparency of security incidents while creating the need to develop effective monitoring and response systems. The right to be forgotten poses technological challenges to ensuring the integrity of legal archives, requiring the development of mechanisms for selective data deletion. Regulation of the use of AI in law actualises the issue of transparency of algorithms and the introduction of the concept of "Explainable AI". New standards on electronic evidence and smart contracts transform procedural aspects and contractual relationships, creating the need to develop robust digital artefact verification mechanisms and security standards for blockchain technologies. Lastly, the development of the concept of digital rights leads to a transformation of approaches to personal protection in the digital space, requiring the development of innovative legal protection mechanisms.

Key regulations, such as the GDPR (Regulation (EU) 2016/679 of…, 2016) and similar documents, play a crucial role in shaping the cybersecurity landscape, stimulating the harmonisation of data protection standards, and the implementation of the "Privacy by Design" concept. Mandatory reporting of data leaks increases the transparency of security incidents while creating the need to develop effective monitoring and response systems. The implementation of the right to oblivion creates technological challenges to ensure the integrity of legal archives, requiring the development of mechanisms for selective data deletion. Regulation of the use of AI in law actualises the issue of transparency of algorithms and the introduction of the concept of "Explainable AI". The evolution of the regulatory framework for electronic evidence and digital signatures is transforming procedural aspects, requiring the development of new authentication and verification standards. Regulation of smart contracts creates new paradigms

in contractual relations, actualising the need to develop specific security standards for blockchain technologies in a legal context. Lastly, the development of the concept of digital rights leads to a transformation of approaches to personal protection in the digital space, requiring the development of innovative legal protection mechanisms. This integrated interaction of regulatory and cybersecurity practices creates a new legal landscape where technological innovation and regulatory requirements are in constant dialectical connection, creating new opportunities and unprecedented challenges for data security and privacy in the digital age.

When considering aspects of implementing a comprehensive cybersecurity strategy in legal organisations, it is important to pay attention to the specifics of ensuring e-justice and information protection in court proceedings. The use of digital technologies in legal proceedings creates new challenges for cybersecurity that require a special approach. In particular, it is necessary to develop special protocols to protect electronic evidence, ensure the integrity and authenticity of digital case materials, and the security of remote court sessions. This requires the introduction of cryptographic security methods, electronic signature verification systems, and access control mechanisms for electronic court systems. An important aspect is ensuring the confidentiality of communication between lawyers and clients in a digital environment, which is a fundamental principle of justice. In this context, the cybersecurity strategy of legal organisations should include a section on specific measures to protect information when interacting with judicial authorities and participating in electronic legal proceedings.

A comparative analysis of approaches to developing cybersecurity strategies in the countries studied identified substantial differences in readiness and approaches to solving problems. The United States demonstrates the highest level of maturity by actively implementing advanced technologies and comprehensive protection strategies, as reflected in its regulatory framework and industry standards (Regulation (EU) 2016/679 of…, 2016). Albania, in the context of European integration processes, adapts its legislation to EU requirements, in particular, by implementing GDPR norms, but faces challenges of limited digital infrastructure. Kyrgyzstan is in the early stages of developing cybersecurity strategies, focusing on implementing basic protection mechanisms and developing a regulatory framework, facing the challenges of limited resources and outdated IT infrastructure. Through the "Digital Uzbekistan 2030" initiative, Uzbekistan is concentrating on safeguarding electronic court systems and case management; however, it encounters new problems in the use of cloud technology (HAMDAMOVA, 2020). The general recommendation for all countries is to develop a culture of cybersecurity in legal organisations, which includes regular training, simulation of cyber-attacks and integration of security issues into the

daily work processes of lawyers, as well as adapting strategies to the specific features of each country, considering its level of technological development and regulatory framework (ISO/IEC 27001:2013…, 2013).

In the context of the globalisation of legal services and the growing number of cross-border legal relationships, the cybersecurity strategy of legal organisations should consider aspects of international law and the variety of legal regimes for data protection. The digital transformation of the banking system and the financial sector creates new challenges for law firms serving international financial transactions. This requires the development of mechanisms to ensure compliance with the requirements of different jurisdictions for the protection of financial information and countering money laundering. The strategy should provide for the creation of a compliance management system that considers the requirements of such regulations as the GDPR (Regulation (EU) 2016/679 of…, 2016) and other regional data protection laws. Special attention should be paid to mechanisms for cross-border data transfer, including the use of standard treaty provisions and obtaining the necessary regulatory approvals. In addition, the strategy should consider the specifics of working with data in jurisdictions with different levels of intellectual property rights protection and approaches to cryptographic information protection.

The "Privacy by Design" and "Security by Design" principles should be used when creating and using new digital tools in legal practice. This is an important part of the cybersecurity strategy. The digital transformation of legal services creates new opportunities to increase the availability of justice but simultaneously creates risks to data privacy and security. In this case, the strategy should include steps for doing a Data Protection Impact Assessment (DPIA) before putting in place new technological solutions like legal information management systems, online consultation platforms, or tools that automatically analyse documents. Special attention should be paid to the ethical use of AI in legal practice, in particular, ensuring transparency of decision-making algorithms and preventing discrimination. Taking into account the unique aspects of the legal field and the changing nature of cyber threats, the strategy should also include ways to regularly check and assess the effectiveness of cybersecurity measures. This may include running periodic penetration tests, analysing vulnerabilities, and simulating cyberattacks to assess the organization's readiness to respond to incidents.

DISCUSSION

The results of the study confirm and expand the understanding of the dualistic nature of the digitalisation of legal processes. It is determined that the introduction

of new technologies increases the efficiency and accessibility of legal services, but creates new vectors of cyber threats. This aligns with the findings of E. Syarief (2022) and D. Manko et al. (2023), however, this study also established that the degree of vulnerability varies substantially depending on the specific solutions implemented and the level of maturity of cybersecurity systems in organisations. Particular attention is drawn to the identified correlation between the level of digital transformation of law firms and the number of cybersecurity incidents. In contrast to the assumptions of M.T. Nguyen & M.Q. Tran (2023), it was determined that the highest level of risk is observed not at the peak of digitalisation, but at the middle stages of transformation. This important discovery highlights the need for enhanced protection at the intermediate stages of digital transformation. The study identified more specific trends in changing the nature of cyber threats in the legal area. In particular, there is an increase in targeted attacks on law firms specialising in high-profile cases. This highlights the need to develop industry-specific cyber defence strategies, which is partly consistent with B. Karovska-Andonovska and N. Taneski (2020), but with a greater focus on the specifics of the legal sector.

Analysis of the impact of AI on the cybersecurity of legal data revealed an ambiguous effect. On the one hand, AI systems improve the effectiveness of detecting and preventing cyber threats, which confirms the conclusions obtained by N. Mohamed (2023). On the other hand, there are potential risks associated with the possibility of manipulating input data for AI systems, which can lead to erroneous legal conclusions or decisions. This issue has not been sufficiently covered in previous studies and requires further research. The study also identified substantial differences in the level of readiness of different segments of the legal sector for cyber threats. In particular, large international law firms demonstrate a higher level of maturity in cybersecurity systems compared to small and medium-sized practitioners. This partially confirms conclusions obtained by J. Kirsiene and D. Amilevičius (2022) on the unevenness of digital transformation in the legal field, but additionally reveals a correlation between the size of companies and their ability to effectively counter modern cyber threats.

Particular attention is drawn to the results on the impact of the regulatory environment on the cybersecurity of legal data. Unlike R.F.R. Forradellas and L.M.G. Gallastegui (2021), who focused mainly on economic aspects, established that the imperfection or inconsistency of the regulatory framework in different jurisdictions creates additional challenges for ensuring cross-border cybersecurity of legal data. This is especially true in the globalisation of legal services and the growing number of international litigations, as confirmed by I.A. Tsindeliani et al. (2022). The critical importance of the human factor in ensuring the cybersecurity of legal data is confirmed by the results of the study. This highlights

the need to develop specialised programmes to improve cyber literacy for legal professionals. The analysis of the use of digital technologies in court proceedings expands on the conclusions of A. Shabalin et al. (2024), added an important aspect of cybersecurity. It was discovered that the introduction of e-justice systems, although it increases the efficiency of legal proceedings, creates new vectors of attacks that can threaten the integrity of the judicial process. This requires the development of specific cybersecurity standards for judicial information systems that consider both technological and procedural aspects.

The importance of the geopolitical dimension of digital transformation of the legal sphere is identified, especially in the context of various approaches to cybersecurity in the United States and Central Asian countries. G. Glasze et al. (2022) address similar issues of digital sovereignty, but the study focuses on their impact on legal practice. It is established that the relationship between technological control, democracy, and digital sovereignty has a substantial impact on the legal area, especially in the context of cybersecurity. M. Leese (2023) explores similar issues but the analysis further identified specific problems for law firms and judicial systems. Analysing different approaches to cyberspace management, substantial differences between Western and Eastern models are identified, which has substantial implications for legal practice. X. Gao (2022) also addresses these issues, but the study further highlights the specific implications of these differences for international legal cooperation and data protection.

The study stressed substantial differences in approaches to assessing and reporting cyber threats in the legal sector in different countries. In particular, it is established that the lack of uniform standards complicates international cooperation and the exchange of experience in the cybersecurity of legal data. This finding correlates with the study by O. Čupka et al. (2023), which also highlights the importance of standardising cybersecurity reporting methodologies. However, unlike their general analysis, this paper focuses on the legal sector, identifying specific needs and challenges. This correlates with the conclusions of B. Alouffi et al. (2021), who conducted a systematic review of the literature on cloud computing security threats and mitigation strategies, which is particularly relevant for law firms that are increasingly switching to cloud technologies. J. Habermas (2022) expands the discussion by recognising the further structural transformation of the political public sphere, which has a direct impact on the legal regulation of the digital space. The study indicated the need to adapt legal institutions to new technological realities in the context of cybersecurity, which is partly consistent with the conclusions of Y. Tikhomirov et al. (2021). However, unlike their general analysis of the impact of digital transformation on law, this study focuses specifically on aspects of cybersecurity in the legal field. It was

determined that the adaptation of legal institutions should take place not only at the level of legislation but also at the level of practical data protection mechanisms in law firms and judicial systems. C. Codagnone and L. Weigl (2023) raise a critical question about the scope and quality of digital regulation, warning against the possibility of creating a "political bubble" in the pursuit of comprehensive regulation of the digital sphere.

The analysis of the impact of digitalisation on legal education and practice identifies the need for substantial changes in the training of future lawyers. M.V. Demchenko et al. (2021) highlighted the challenges, risks, and prospects of digital transformation of legal education, emphasising the need to integrate digital competencies into curricula. This aligns with the findings of J. Gjika (2023), who analysed the impact of the European Code of Electronic Communications on the harmonisation of legislation that requires lawyers to have new skills in the field of telecommunications law. M.J. Sule et al. (2021) examine cybersecurity through the prism of digital identity and data protection, which is becoming a critical aspect of legal practice in the digital age. E.L. Sidorenko and P. Von Arx (2020) stress the transformation of law in the context of digitalisation, emphasising the importance of identifying the right priorities in the development of the legal system. C.E.P. Tache and C.S. Săraru (2024) assess the contemporary multidimensional dependencies between digital transformation, corporate governance, and public international law, highlighting the complex nature of the challenges facing the legal community in the global digital environment.

A comparative analysis of the situation in the countries under study indicated substantial differences in approaches to the digital transformation of the legal sphere and ensuring cybersecurity. The United States demonstrates the highest level of maturity by actively implementing advanced technologies and comprehensive protection strategies, which is reflected in its regulatory framework, in particular, in the NIST Cybersecurity Framework. Albania, in the context of European integration processes, adapts its legislation to EU requirements, reflected in the National Strategy on Cybersecurity 2020-2025 but faces challenges of limited digital infrastructure. Kyrgyzstan, according to the cybersecurity concept for 2019-2023, is in the initial stages of developing cybersecurity strategies, focusing on implementing basic protection mechanisms and developing a regulatory framework, facing the problems of limited resources and outdated IT infrastructure. Uzbekistan is concentrating on safeguarding computerized court systems and case management, although encounters new obstacles in the implementation of cloud technologies (HAMDAMOVA, 2020). These differences highlight the need to develop individual approaches to

cybersecurity in the legal sector for each country, considering their specific conditions and level of technological development.

A comparison of Albania, Kyrgyzstan, the United States of America, and Uzbekistan revealed substantial differences in approaches to digital transformation of the legal sphere and cybersecurity. Albania demonstrated moderate progress in implementing key legislation but faces challenges with limited digital infrastructure. Kyrgyzstan is in the initial stages of digital transformation, facing the problems of outdated IT infrastructure. The United States is a leader with a well-developed regulatory framework and advanced technological solutions. Uzbekistan is actively working on the digitalisation of the legal field but faces the challenges of insufficient digital infrastructure. For the countries under study, the recommendations include: strengthening investment in digital infrastructure and digital literacy programmes for lawyers in Albania; accelerating the modernisation of IT infrastructure in the legal sector of Kyrgyzstan; continuing the development of innovative data protection technologies in the United States; accelerating the introduction of digital technologies in the judicial system of Uzbekistan. Based on the results obtained, it is recommended to implement a multi-level security system that considers the specifics of digital transformations in the legal sphere, develop programmes to improve digital literacy and staff awareness of cyber threats and adapt the regulatory framework to the new challenges of the digital age, in particular, in the aspect of regulating the use of AI and blockchain in legal practice.

CONCLUSIONS

The study on developing effective cybersecurity strategies in the context of the digital transformation of the legal field has provided valuable insights and actionable recommendations. The integration of innovative technologies such as cloud computing, artificial intelligence, and blockchain into legal practice has significantly enhanced efficiency but has also introduced new cybersecurity challenges. The analysis revealed that the rapid digitalisation of the legal sphere necessitates a comprehensive approach to cybersecurity that encompasses technological, organisational, and regulatory aspects.

Key findings include the identification of critical vulnerabilities in legal information systems, particularly in the context of cloud technologies and remote work. The examination of successful cyber-attacks on prominent law firms underscored the need for robust, multi-level cybersecurity measures. The study also highlighted the importance of adapting best practices from international legal cybersecurity regulation and the need for continuous updates and effective disaster recovery plans.

The human component of cybersecurity was emphasised, with recommendations for boosting staff digital literacy through comprehensive training programmes. The potential of quantum cryptography in legal data protection was explored, along with the need to regulate blockchain technology in legal practice. The integration of digital platforms into legal activities introduced new cyber dangers, demanding novel security solutions.

Practical implications of the study include the development of effective cybersecurity strategies and the improvement of relevant legislation to ensure the confidentiality and integrity of legal information. The proposed conceptual model of an adaptive cybersecurity system offers a significant reduction in attack likelihood, while the recommendation to rewrite the legislative framework for personal data protection addresses the challenges of digitalisation.

In conclusion, the digital transformation of the legal field presents both opportunities and challenges. By adopting a comprehensive, adaptive, and proactive approach to cybersecurity, legal organisations can effectively protect confidential information and maintain the integrity of legal processes in the digital age. Future research should focus on the continuous evolution of cyber threats and the development of innovative cybersecurity solutions tailored to the legal sector.

DECLARATION OF CONFLICTING INTERESTS

The authors declare that they have no existing or potential conflicting interests with respect to the research, authorship and publication of this paper.

FUNDING

The authors received no financial support for the research, authorship and/or publication of this paper.

REFERENCES

ALOUFFI, B., HASNAIN, M., ALHARBI, A., ALOSAIMI, W., ALYAMI, H., & AYAZ, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807. doi: https://doi.org/10.1109/access.2021.3073203

AVIV, I., GAFNI, R., SHERMAN, S., AVIV, B., STERKIN, A., & BEGA, E. (2023). Cloud Infrastructure from Python Code – breaking the Barriers of Cloud Deployment. In: M. Wiese (Eds.), *17th European Conference on Software Architecture, ECSA 2023*. Istanbul: Turkey; https://conf.researchr.org/details/ecsa-2023/ecsa-2023-journal-

first/2/Cloud-Infrastructure-from-Python-Code-breaking-the-Barriers-of-Cloud-Deployment

BABIKIAN, J. (2023a). Securing rights: Legal frameworks for privacy and data protection in the digital era. *Law Research Journal*, *1*(2), 91-101.

BABIKIAN, J. (2023b). Navigating legal frontiers: Exploring emerging issues in cyber law. *Revista Espanola de Documentacion Cientifica*, *17*(2), 95-109. doi: http://dx.doi.org/10.13140/RG.2.2.20264.55048

BOCHELIUK, V.I., NECHYPORENKO, V.V., DERGACH, M.A., POZDNIAKOVA-KYRBIATIEVA, E.G., & PANOV, N.S. (2019). Management of professional readaptation in terms of the modern Ukrainian society. *Astra Salvensis, 1*, 539-552. https://repository.khnnra.edu.ua/scientific-texts/management-of-professional-readaptation-in-terms-of-the-modern-ukrainian-society/

CICHONSKI, P., MILLAR, T., GRANCE, T., & SCARFONE, K. (2012). Computer security incident handling guide: Recommendations of the national institute of standards and technology. doi: http://dx.doi.org/10.6028/NIST.SP.800-61r2

CODAGNONE, C., & WEIGL, L. (2023). Leading the charge on digital regulation: The more, the better, or policy bubble? *Digital Society*, *2*, 4. doi: https://doi.org/10.1007/s44206-023-00033-7

Convention on Cybercrime. (2001). Retrieved from: https://rm.coe.int/1680081561.

ČUPKA, O., FEDERLOVA, E., & VESELY, P. (2023). Comparison of methodologies used in cybersecurity reports. In: N. Kryvinska, M. Greguš, S. Fedushko (Eds.), *Developments in Information and Knowledge Management Systems for Business Applications* (pp. 313-348). Cham: Springer. doi: https://doi.org/10.1007/978-3-031-25695-0_15

DEMCHENKO, M.V., GULIEVA, M.E., LARINA, T.V., & SIMAEVA, E.P. (2021). Digital transformation of legal education: Problems, risks and prospects. *European Journal of Contemporary Education*, *10*(2), 297-307. doi: https://doi.org/10.13187/ejced.2021.2.297

Directive (EU) 2016/1148 of the European Parliament and of the Council of concerning measures for a high common level of security of network and information systems across the Union. (2016). Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Directive (EU) 2018/1972 of the European Parliament and of the Council of establishing the European Electronic Communications Code. (2018). Retrieved from: https://eur-lex.europa.eu/eli/dir/2018/1972/oj

DISTERER, G., & KLEINER, C. (2013). BYOD bring your own device. *Procedia Technology*, *9*, 43-53. doi: https://doi.org/10.1016/j.protcy.2013.12.005

DLA Piper ransomware hack: What can we learn from it? (2024). Retrieved from: https://www.titanfile.com/blog/dla-piper-ransomware-hack-can-learn/

FORRADELLAS, R.F.R., & GALLASTEGUI, L.M.G. (2021). Digital transformation and artificial intelligence applied to business: Legal regulations, economic impact and perspective. *Laws, 10*(3), 70. doi: https://doi.org/10.3390/laws10030070

FREUND, J., & JONES, J. (2015). *Measuring and managing information risk: A FAIR approach*. Portsmouth: Butterworth-Heinemann. doi: https://doi.org/10.1016/C2013-0-09966-5

GAFNI, R., AVIV, I., & HAIM, D. (2024). Multi-Party Secured Collaboration Architecture from Cloud to Edge. *Journal of Computer Information Systems, 64*(5), 698-709. doi: https://doi.org/10.1080/08874417.2023.2248921

GAIE, C., & KARPIUK, M. (2024). The provision of e-services by public administration bodies and their cybersecurity. In: C. Gaie, M. Mehta (Eds.), *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations* (pp. 175-188). Cham: Springer. doi: https://doi.org/10.1007/978-3-031-55575-6_7

GAO, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the western model. *International Spectator*, *57*(3), 15-30. doi: https://doi.org/10.1080/03932729.2022.2074710

GASHI, S., IMARALIEVA, T., ABDYKADYROV, S., LAILIEVA, E., & BABAYEV, F. (2024). Research on the impact of artificial intelligence on financial security in the context of modern technological challenges. *Revista Interdisciplinar de Ciencia Aplicada, 8*(13). doi: https://doi.org/10.18226/25253824.v8.n13.08

GJIKA, J. (2023). Harmonizing Albanian electronic communications law: A comprehensive analysis of European electronic communications code impact. *Balkan Social Science Review*, *22*(22), 189-221. doi: https://doi.org/10.46763/BSSR232222189g

GLASZE, G., CATTARUZZA, A., DOUZET, F., DAMMANN, F., BERTRAN, M.G., BÔMONT, C., & ZANIN, C. (2022). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919-958. doi: https://doi.org/10.1080/14650045.2022.2050070

GOLDSTEIN, M. (2016). Cravath law firm discloses a data attack. Retrieved from: https://www.nytimes.com/2016/03/31/business/dealbook/cravath-law-firm-discloses-a-data-attack.html

HABERMAS, J. (2022). Reflections and hypotheses on a further structural transformation of the political public sphere. *Theory, Culture & Society*, *39*(4), 145-171. doi: https://doi.org/10.1177/02632764221112341

HAMDAMOVA, F. (2020). Strategy "Digital Uzbekistan-2030": Prerequisites for adoption, main provisions, mechanisms and prospects of realization. *Society and Innovations*, *2*(1/S), 131-143. doi: https://doi.org/10.47689/2181-1415-vol2-iss1/s-pp131-143

ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements. (2013). Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC 27043:2015: Information technology – Security techniques – Incident investigation principles and processes. (2015). Retrieved from: https://www.iso.org/standard/44407.html

JOHNSON, C.S., BADGER, M.L., WALTERMIRE, D.A., SNYDER, J., & SKORUPKA, C. (2016). Guide to cyber threat information sharing. doi: http://dx.doi.org/10.6028/NIST.SP.800-150

KAROVSKA-ANDONOVSKA, B., & TANESKI, N. (2020). Legal aspects of security in cyberspace. *Security Dialogues*, *11*(1), 99-100. doi: http://dx.doi.org/10.47054/SD2010099ka

KHARCHENKO, V., PONOCHOVNYI, Y., QAHTAN, A.-S.M., & BOYARCHUK, A. (2017). Security and availability models for smart building automation systems. *International Journal of Computing, 16*(4), 194-202. doi: http://dx.doi.org/10.47839/ijc.16.4.907

KIRSIENE, J., & AMILEVIČIUS, D. (2022). Digital transformation of legal services and access to justice: Challenges and possibilities. *Baltic Journal of Law & Politics, 15*(1), 141-172. doi: http://dx.doi.org/10.2478/bjlp-2022-0007

KOÇI, A. (2022). Cyber security and legal challenges on managing online data. In: D. Dašić (Ed.), *Security Challenges of Modern Society – Dilemmas and Implications*. (pp. 187-201). Belgrade: Faculty of Law, Security and Management "Constantine the Great".

KOLBAYEV, N., TUYENBAYEVA, K., SEITIMBETOVA, D., & APAKHAYEV, N. (2024). Methods of Modelling Electronic Academic Libraries: Technological Concept of Electronic Libraries. *Preservation, Digital Technology and Culture, 53*(2), 81-90. doi: https://doi.org/10.1515/pdtc-2024-0001

LEESE, M. (2023). Staying in control of technology: Predictive policing, democracy, and digital sovereignty. *Democratization*, *31*(5), 963-978. doi: https://doi.org/10.1080/13510347.2023.2197217

MANKO, D., ZGHAMA, A., ATAMANOVA, N., ARABADZHY, N., & USTINOV, D. (2023). Legal regulation of the digital environment: Digitization of the state-legal and law enforcement sphere. *Amazonia Investiga*, *12*(70), 125-133. doi: https://doi.org/10.34069/AI/2023.70.10.11

MOHAMED, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2), 2272358. doi: https://doi.org/10.1080/23311916.2023.2272358

MONITORING OF NATIONAL CYBERSECURITY STRATEGY 2020-2025. (2023). https://aksk.gov.al/wp-content/uploads/2024/01/Monitoring-of-the-National-Cyber-Security-Strategy-2022.pdf

NARAYANAN, P.S., ANI, R., & KING, A.T.L. (2020). TorBot: Open-source intelligence tool for dark web. In: G. Ranganathan, J. Chen, Á. Rocha (Eds.), *Proceedings of ICICCT 2019 "Inventive Communication and Computational Technologies"* (pp. 193-207). Singapore: Springer. doi: https://doi.org/10.1007/978-981-15-0146-3_19

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. *Cybersecurity Framework*. doi: https://doi.org/10.6028/NIST.CSWP.04162018

NGUYEN, M.T., & TRAN, M.Q. (2023). Balancing security and privacy in the digital age: An in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), 1-12.

NURBATYROVA, R., JAPAROV, B., APAKHAYEV, N., ABDULAZIZ, B., & KHUSHKELDIYEVA, S. (2024). Digital Transformation of Archives in the Context of the Introduction of an Electronic Document Management System in Kazakhstan. *Preservation, Digital Technology and Culture, 53*(3), 147-155. doi: https://doi.org/10.1515/pdtc-2024-0017

OPFER, C. (2021). Jones Day hit by data breach as vendor Accellion hack widens. Retrieved from: https://news.bloomberglaw.com/business-and-practice/jones-day-hit-by-data-breach-as-vendor-accellion-hacks-widen

PALKO, D., BABENKO, T., BIGDAN, A., KIKTEV, N., HUTSOL, T., KUBOŃ, M., HNATIIENKO, H., TABOR, S., GORBOVY, O., & BORUSIEWICZ, A. (2023). Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences (Switzerland), 13*(4), 2393. doi: https://doi.org/10.3390/app13042393

Regulation (EU) 2016/679 of the European Parliament and of the Council On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

(2016). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Regulation (EU) 2022/1925 of the European Parliament and of the Council On contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828. (2022). Retrieved from: http://data.europa.eu/eli/reg/2022/1925/oj

Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC. (2022). Retrieved from: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Resolution on Issues of Development of Inclusive Education in the Kyrgyz Republic. 2019. Retrieved from: http://cbd.minjust.gov.kg/act/view/ru-ru/14590

SAKHIPOV, A., YERMAGANBETOVA, M., LATYPOV, R., & UALIYEV, N. (2022). Application of blockchain technology in higher education institutions. *Journal of Theoretical and Applied Information Technology, 100*(4), 1138-1147. doi: http://dx.doi.org/10.1109/ICISCT50599.2020.9351424

SHABALIN, A., SHTEFAN, O., ANDRUSHCHENKO, L., & OLEFIR, V. (2024). Use of digital technologies in judicial proceedings in some countries of Europe and the USA. *Measuring Environmental Impacts and Judiciary Environments, the Critical Analysis*, *9*(1), 1-16. doi: https://doi.org/10.22373/petita.v9i1.218

SIDORENKO, E.L., & VON ARX, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. *Digital Law Journal*, *1*(1), 24-38. doi: https://doi.org/10.38044/dlj-2020-1-1-24-38

SULE, M.J., ZENNARO, M., & THOMAS, G. (2021). Cybersecurity through the lens of digital identity and data protection: Issues and trends. *Technology in Society*, *67*, 101734. doi: https://doi.org/10.1016/j.techsoc.2021.101734

ŚWITAL, P., & SKOCZYLAS, D. (2024). The information sphere in the age of cyberthreats. Disinformation and cybersecurity. *Teka Commission of Legal Sciences*, *17*(1), 257-271. doi: http://dx.doi.org/10.32084/tkp.5812

SYARIEF, E. (2022). Security concerns in digital transformation of electronic land registration: Legal protection in cybersecurity laws in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 32-46.

TACHE, C.E.P., & SĂRARU, C.S. (2024). Evaluating today's multi-dependencies in digital transformation, corporate governance and public international law triad. *Cogent Social Sciences*, *10*(1), 2370945. doi: https://doi.org/10.1080/23311886.2024.2370945

TIKHOMIROV, Y., KICHIGIN, N., TSOMARTOVA, F., & BALKHAYEVA, S. (2021). Law and digital transformation. *Law Journal of the Higher School of Economics*, *2*, 4-23.

TKACHENKO, O., GONCHAROV, V., & JATKIEWICZ, P. (2024). Enhancing Front-End Security: Protecting User Data and Privacy in Web Applications. *Computer Animation and Virtual Worlds, 35*(6), e70003. doi: https://doi.org/10.1002/cav.70003

TSINDELIANI, I.A., PROSHUNIN, M.M., SADOVSKAYA, T.D., POPKOVA, Z.G., DAVYDOVA, M.A., & BABAYAN, O.A. (2022). Digital transformation of the banking system in the context of sustainable development. *Journal of Money Laundering Control*, *25*(1), 165-180. doi: https://doi.org/10.1108/JMLC-02-2021-0011

WITTING, C. (2005). Duty of care: An analytical approach. *Oxford Journal of Legal Studies*, 25(1), 33-63. doi: https://doi.org/10.1093/ojls/gqi003

ZENIN, S., KORNEV, A., LIPEN, S., SHEPELEV, D., & TANIMOV, O. (2023). Transformation of law and legal activity in the context of the development of digital technologies. *Lex Humana*, *15*(1), 277-290.

ZYHRII, O., TRUFANOVA, Y., PARASHCHUK, L., SAMPARA, N., & TSVIGUN, I. (2023). Law and technology: The impact of innovations on the legal system and its regulation. *Social & Legal Studios*, *6*(4), 267-275. doi: https://doi.org/10.32518/sals4.2023.267

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET