Digital transformation in the legal sector: Challenges and opportunities for cybersecurity and data protection

Submitted: 19 November 2024
Reviewed: 7 January 2025
Revised: 21 January 2025
Accepted: 25 January 2025

Erisa Xhixho[*]
https://orcid.org/0009-0009-2869-5629
Niiazbek Pazylov[**]
https://orcid.org/0000-0002-6180-9634
Viktor Savchenko[***]
https://orcid.org/0000-0001-7104-3559
Nurkhanbek Patiev[****]
https://orcid.org/0009-0000-3797-4464
Munarym Pazylova[*****]
https://orcid.org/0000-0002-7515-5635

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i1.56176

Abstract

[Purpose] The purpose of this study was to examine the principal issues of cybersecurity and data protection in the context of digital transformation in the legal system of the Kyrgyz Republic.

[Methodology/approach/design] The study conducted legal and comparative analysis of the regulatory framework and its application in modern conditions. Additionally, the content of reports from governmental and international organisations was examined to assess current trends in data protection and digital services. The study analysed key documents such as the National Development Strategy of the Kyrgyz Republic for 2018-2040 and the Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028, the Civil and Criminal Codes of the Kyrgyz Republic, as well as laws of the Kyrgyz Republic regulating access to information, data protection, and cybersecurity, namely, "On the Right of Access to Information", "On Protection of State Secrets of the Kyrgyz Republic", "On the National Archive Fund of the Kyrgyz Republic", "On the Electrical Connection". Special attention was paid to the Tunduk system as an essential element of digital public administration and interaction between public authorities.

[*]Department of Public Law, University of Tirana, 1010, 4 Mother Teresa Sq., Tirana, Albania. E-mail: erisaxhixho18@gmail.com.
[**]Department of Civil Law and Procedure, Osh State University, 723500, 331 Lenin Str., Osh, Kyrgyz Republic. E-mail: n_pazylov@outlook.com.
[***]Faculty of Business, Kauno Kolegija Higher Education Institution, 50468, 20 Pramones Ave., Kaunas, Lithuania. E-mail: viktor_savchenko@hotmail.com.
[****]Department of Theories, History of State and Law, Osh State University, 723500, 331 Lenin Str., Osh, Kyrgyz Republic. E-mail: nurk-patiev@outlook.com.
[*****]Department of Civil Law and Procedure, Osh State University, 723500, 331 Lenin Str., Osh, Kyrgyz Republic. E-mail: mu_pazylova@hotmail.com.

[Findings] The key findings showed that despite great strides in digitalisation, the existing legislative framework of the Kyrgyz Republic needs considerable adaptation to ensure data protection and cybersecurity in a rapidly evolving digital environment.
[Practical implications] The study offered recommendations, including the creation of a national cybersecurity centre, the introduction of international data protection standards, and the development of human resources in the field of information security.
[Originality/value] The findings confirm the need to modernise the legal framework to ensure a sustainable and secure digital transformation in the Kyrgyz Republic, which is critical for protecting citizens' data and increasing trust in public services.

Keywords: Legal mechanisms. Electronic infrastructure. Electronic document management. Software. Socio-economic development.

INTRODUCTION

Digital transformation in the modern world has become an integral part of all spheres of life, including the legal sphere, which requires special attention to cybersecurity and data protection issues. With the rapid development of information technology and the growing number of digital threats, the need for effective protection of data and information systems is of key significance. For Kyrgyzstan, as a developing country, integrating cybersecurity into strategic management is not only an essential element of sustainable development, but also a necessary measure to ensure the security of citizens and state institutions.

The principal challenge facing the country is the lack of adaptation of legislative and organisational measures to the new threats posed by cyberattacks and data breaches. Despite the growing number of regulations aimed at governing information security, many key aspects are still unresolved. Specifically, critical infrastructure protection and cyber hygiene are not sufficiently covered. This poses additional risks to information systems and data in an environment of global digitalisation, where cybercriminals are using increasingly sophisticated methods to hack into information systems. In this regard, the study of cybersecurity and data protection in the legal sphere of Kyrgyzstan becomes particularly relevant, as these issues directly affect the efficiency of the work of state bodies, the protection of confidential information of citizens, and assurance of the stable functioning of the country's economy. With the adoption of the Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028 (Ministry of Digital Development of the Kyrgyz Republic, 2024), Kyrgyzstan continues to develop cybersecurity and data protection. This document is a logical continuation of the Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023 (Ministry of Justice of the Republic of Kazakhstan, 2019), which laid the foundation for national cybersecurity and coordination between government agencies and the private sector.

The new framework emphasises better management of risks associated with cyberattacks, as well as adaptation to international practices to national conditions. A major step is the establishment of a national cybersecurity incident

response system to effectively detect, analyse, and respond to threats. Kyrgyzstan's participation in international cybersecurity exercises, such as the Global Online Exercise in 2020 and the Interregional Exercise for CIS countries in 2019 in Malaysia, has helped strengthen cooperation with the global community and share best practices (International Telecommunication Union, 2021). Despite the successes achieved in implementing the strategy, there are still significant challenges that require attention. One of the primary challenges is the insufficient updating of the regulatory framework. For instance, prominent aspects such as critical infrastructure protection and cyber hygiene are not fully covered. This creates more risks for information systems, as well as limits the effectiveness of the measures implemented. Furthermore, there is insufficient monitoring of the implementation of the strategy's provisions due to inconsistencies in legislation and limited resources allocated to cybersecurity. All this makes it difficult to protect the subjects of legal relations in the digital environment and requires further measures to improve cybersecurity in Kyrgyzstan.

From 2018 to 2023, interest in cybersecurity and legal data protection has increased noticeable, as evidenced by a series of studies analysing the risks of digitalisation of legal processes and developing suitable legal mechanisms. Syarief (2022) focused on cybersecurity challenges in the digitalisation of land registries in Indonesia. In this context, the study emphasised the need to strengthen legislation and its practical application to ensure cybersecurity in the digital transformation of legal systems. Möller (2023) emphasised the relationship between digital transformation and cybersecurity. The researcher argued that digital transformation in the legal sector is not possible without understanding and minimising these risks, highlighting the significance of comprehensive data protection measures at all stages of technology adoption. Mijwil et al. (2023) explored the importance of cybersecurity management in the digital transformation of public services. Researchers considered how effective cybersecurity governance can contribute to successful digital transformation and citizen data protection.

Ahmed et al. (2021) provided a comparative analysis of the legal systems of Iraqi Kurdistan and Estonia, demonstrating how successful digital transformation requires the integration of cybersecurity measures into legislative and administrative processes. Saeed et al. (2023) examined the challenges associated with cybersecurity in the context of digital business transformation. This research is relevant to the legal field, where the protection of confidential information plays a key role. Maglaras et al. (2020) analysed the advancement of cybersecurity in Greece in the context of digital transformation. The significance of state-level coordination and the development of national cybersecurity strategies is relevant to the legal sector, where data protection and the prevention of cyberattacks are critical tasks. Uwadinma and Ikeatu (2024) examine the unique challenges facing the practice of law in Nigeria in digital transformation. Lack of technological infrastructure and resistance to change are formidable barriers to cybersecurity.

Reier Forradellas and Garay Gallastegui (2021) highlighted that digital transformation, including in the legal field, requires a clear legal framework to protect data and minimise the risks associated with the use of latest technologies. Popa Tache and Săraru (2024) emphasise the complex interrelationships between digital transformation, corporate governance, and international law. The successful digital transformation of the legal sphere requires the consideration of cybersecurity as a key element in the development of regulatory rules. Nainggolan (2023) notes that philosophy of law plays a crucial role in formulating fair and effective rules to protect data and the public interest in the era of digital transformation.

The reviewed studies suggest that the digital transformation in the legal field presents many challenges, among which cybersecurity and data protection are key. The introduction of digital technologies such as electronic land certificates and artificial intelligence significantly increases the risks of cyberattacks and fraud. This emphasises the need to develop and strengthen legal mechanisms aimed at protecting data and citizens' rights.

The purpose of this study was to identify the principal factors affecting cybersecurity and data protection in the context of the development of digital technologies in the legal system of Kyrgyzstan. The objectives of the study included an assessment of the implementation of the Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023 (Ministry of Justice of the Republic of Kazakhstan, 2019) considering the objectives of the Decree of the President of the Kyrgyz Republic No. 221 "On the National Development Strategy of the Kyrgyz Republic for 2018–2040" (Ministry of Justice of the Republic of Kazakhstan, 2018) and the Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028 (Ministry of Digital Development of the Kyrgyz Republic, 2024); analysis of the state of the regulatory framework governing cybersecurity in the legal sphere; identification of existing gaps in cybersecurity control and coordination mechanisms; and development of recommendations to improve data protection with a focus on international cooperation and adaptation to digital challenges.

MATERIALS AND METHODS

This study performed a detailed analysis of regulatory documents and strategic programmes related to digital transformation and cybersecurity in the Kyrgyz Republic, as well as international standards and examples of successful practices of leading countries in this area. The focus was on key national documents, such as the Decree of the President of the Kyrgyz Republic No. 221 "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" (Ministry of Justice of the Republic of Kazakhstan, 2018) and the Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028 (Ministry of Digital Development of the Kyrgyz Republic, 2024), which define long-term goals and objectives in the field of digitalisation.

A comprehensive study of the regulatory framework governing access to information, data protection, and cybersecurity in the Kyrgyz Republic was

conducted. The focus was on key documents such as the Criminal Code of the Kyrgyz Republic No. 127 (Ministry of Justice of the Republic of Kazakhstan, 2024b) and the Civil Code of the Kyrgyz Republic No. 15 (Ministry of Justice of the Republic of Kazakhstan, 2024a), as well as Law of the Kyrgyz Republic No. 217 "On the Right of Access to Information" (Ministry of Justice of the Republic of Kazakhstan, 2024c), the Law of the Kyrgyz Republic No. 210 (15) "On Protection of State Secrets of the Kyrgyz Republic" (Ministry of Justice of the Republic of Kazakhstan, 2023a), the Law of the Kyrgyz Republic No. 125 "On the National Archive Fund of the Kyrgyz Republic" (Ministry of Justice of the Republic of Kazakhstan, 2023b), and the Law of the Kyrgyz Republic No. 31 "On the Electrical Connection" (Ministry of Justice of the Republic of Kazakhstan, 2023b). These laws form the legal basis for ensuring information security and regulate citizens' access to government data. A comparative comparison was made between the national legislation of the Kyrgyz Republic and international data protection standards such as the General Data Protection Regulation (GDPR).

The study considered the successful examples of digitalisation in countries such as Estonia, Singapore, and Japan. The focus was on programmes such as e-Estonia, covering e-government, e-citizenship, and cybersecurity; Smart Nation Singapore, integrating digital technologies into public administration, the economy, and everyday life, with a special focus on data security; and Society 5.0 Japan, which combines digital technology and innovation to enhance public administration and provide protection against cyberthreats. The study of these cases assessed how these states have made great strides in improving the transparency and efficiency of public administration through the adoption of digital technologies. Particular attention was paid to how these countries have managed to integrate cybersecurity into their governance system and minimise the risks associated with data breaches and cyberthreats.

The reports of the Ministry of Digital Development of the Kyrgyz Republic (2024), Regional United Nations Group for Europe and Central Asia on Digital Transformation (2021), and World Bank Group (2024) on digitalisation, implementation of electronic systems, and information security were examined. This analysis helped to assess the country's progress in the development of digital technologies, as well as to identify existing barriers to the effective implementation of digital solutions, such as infrastructure and staffing deficiencies in remote regions. Both qualitative and quantitative analyses of statistical data provided by the National Statistical Committee of the Kyrgyz Republic and the Institute of Statistical Research and Professional Development (2020) were conducted. The data included indicators of access to digital services in different regions of the country, as well as incidents of data breaches and cybercrime. This identified weaknesses in the system that need to be focused on to improve cybersecurity. A structural-functional approach was applied to analyse the performance of the Tunduk system, which is the main platform for data exchange between government agencies. Such aspects as automation of processes, reduction of human factor, and improvement of interaction between state structures were analysed.

A dialectical approach was employed to examine changes in the Kyrgyz Republic's legislation related to digital transformation and data protection. This approach helped to identify contradictions and problems in existing regulations and propose possible solutions to them, as well as to consider the prospects for further reforms in this area aimed at improving cybersecurity and legal regulation of digital processes.

RESULTS

The Decree of the President of the Kyrgyz Republic No. 221 "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" (Ministry of Justice of the Republic of Kazakhstan, 2018) focuses on the long-term sustainable development of the country, with special attention paid to the need for digital transformation of various sectors of the economy and public services. The inclusion of digitalisation as one of the priority areas in this document is driven by the need to make public administration more transparent, efficient, and accountable. This was a major step in changing approaches to data processing and protection, as digitalisation reduces the human factor in decision-making and data management processes, which reduces the risks of leaks and misuse of information.

The Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028(Ministry of Digital Development of the Kyrgyz Republic, 2024) was adopted to ensure a systematic approach to the development of digital infrastructure and the integration of latest technologies into government processes. One of the key aspects of this vision is cybersecurity and data protection, which is related to the increasing risks in the context of active adoption of information technology. The adoption of this document made it possible to formulate concrete goals and objectives for the protection of personal data, to develop standards and requirements for the security of information systems, as well as to strengthen legal and organisational measures to prevent cyber incidents. The concept also aims to develop human resources capacity in the field of information technology, which is critical for the achievement of data protection goals.

The adoption of these regulations has fundamentally changed the situation with cybersecurity and data protection in the Kyrgyz Republic. Until 2019, the country's legislative framework was underdeveloped in this area, creating vulnerabilities in information security systems. With the introduction of the above-mentioned Concept and the National Strategy, the process of actively reforming the country's legislation and technical equipment to counter cyberattacks and protect the confidential data of citizens and government agencies commenced (Table 1).

Document	Principal goals and objectives	Impact on data protection and cybersecurity
Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028	Sustainable socio-economic development. Development of electronic infrastructure. Increasing transparency of public administration and implementation of e-government.	Creation of a single platform for data management. Increasing responsibility for data processing, reducing corruption risks. Integration of data protection at the level of electronic public services.
Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023	Digitalisation of all public services. Development of digital skills among the population. Integration of cybersecurity systems into government processes.	Implementation of cybersecurity standards at the level of government agencies. Ensuring the protection of citizens' personal data when they interact with government platforms. Countering cyberattacks and cyber incidents through the implementation of integrated monitoring and response systems.
Tunduk electronic interaction system	Automation and integration of data exchange between government agencies. Minimisation of paperwork. Increased transparency and reduction of corruption schemes.	Data encryption and access control to ensure the security of transmitted information. Human error reduction, which minimises the risks of data breaches. Strengthening of legal protection of data through the integration of international security standards.

Table 1 – Description of the goals and objectives of regulatory documents and development programmes in the field of digital transformation, as well as their impact on various aspects of data protection and cybersecurity in the Kyrgyz Republic

Source: compiled by the authors of this study based on the Concept of Digital Transformation of the Kyrgyz Republic for 2024-2028 (Ministry of Digital Development of the Kyrgyz Republic, 2024) and the Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023 (Ministry of Justice of the Republic of Kazakhstan, 2019).

Each document and programme aimed at digital transformation in the Kyrgyz Republic plays a vital role in strengthening cybersecurity and data protection. Specifically, the Tunduk system of electronic interagency interaction has become one of the key elements of the digital transformation of the Kyrgyz Republic, which directly affects the processes of data protection and cybersecurity. Implementation of the system makes it possible to significantly simplify the exchange of information between different government agencies, minimising the use of paper documents and increasing the speed and accuracy of data processing.

For the Kyrgyz Republic, digitalisation presents both new opportunities and significant challenges. The benefits include improved safety and efficiency of industrial operations, which is particularly relevant in the context of the use of automation and unmanned technologies. However, digitalisation also brings considerable risks, primarily related to the rise of cybercriminals. The key components of the digital economy in the country include e-commerce, development investment, public administration, and export-import activities. The largest contributor to the digital economy is virtual commerce, which, as in other

countries, is actively developing in the segments of household appliances, electronics, clothing, and footwear. The use of digital technologies in legal practice in the Kyrgyz Republic is gradually expanding to include both the public and private sectors. The principal methods and tools focus on automating processes, increasing transparency, accelerating judicial and administrative procedures, and improving access to justice. These include electronic document management, the introduction of e-courts, and the use of digital signatures.

Electronic document management is an essential component of the digitalisation of legal activities, providing a series of significant advantages and allowing for creation, signing, and transmission of documents in electronic form, which substantially saves time and resources associated with their processing and storage. Physical storage of papers incurs costs for office space, maintenance, and archiving, while electronic archives minimise these costs and provide instant access to documents at any time. Moreover, centralised storage systems can avoid problems with document loss, which is a key factor for legal security. From the standpoint of information security, electronic document management has major advantages. The use of modern encryption and multi-level authentication technologies protects documents from unauthorised access and forgery. This is crucial for working with legally relevant documents that require strong data protection. In conventional document management, there is a risk of physical theft or loss, which is avoided in the digital environment. Such systems also offer audit capabilities – every document transaction is recorded, providing transparency and traceability.

The digital signature plays a crucial role in ensuring the legal validity of electronic documents. It is a key element of the process, allowing the authenticity of the document and the identity of the signatory to be confirmed. The use of digital signatures considerably accelerates the conclusion of contracts and submission of applications, and avoids bureaucratic delays associated with the need for personal presence. For instance, in Kyrgyzstan, digital signatures are already actively used in both government agencies and private companies. However, for this tool to become used *en masse*, it is necessary to expand its use and adapt the regulatory framework to meet the modern requirements of the digital economy.

Kyrgyzstan's e-courts are an integrated system where citizens can file lawsuits, exchange procedural documents, and take part in sessions remotely. This format is particularly important for those living in remote regions where access to court facilities may be difficult. Furthermore, e-courts contribute to accelerating court processes and reducing the time taken to process cases. The digitalisation of the judiciary also reduces the probability of corruption by minimising personal interaction between participants in the process and increasing the transparency of procedures. The introduction of such technologies in Kyrgyzstan opens new opportunities to improve access to justice. Another prominent area is the creation of online platforms for providing legal advice. These platforms enable citizens to receive legal aid from the comfort of their homes, which is particularly relevant for those living in regions with limited access to legal services. For example, a person can apply for a consultation via the Internet, get answers to their questions,

and even order the execution of legal documents without having to visit a lawyer's office in person. This not only reduces the cost of legal services, but also makes them more accessible to a wider audience.

In the international arena, there is an active development of automated legal analysis systems using artificial intelligence. These technologies enable efficient processing of large amounts of information, analysis of legal documents, precedents, and predictions on case outcomes. While the use of artificial intelligence in the legal sphere is only beginning to be introduced in Kyrgyzstan, this trend could considerable affect he improvement of lawyers' efficiency in the future. Such systems will be able to automate many routine tasks such as drafting contracts or analysing legal documentation, freeing up specialists to handle more complex issues. However, the introduction of artificial intelligence requires sizeable investment in infrastructure and research, which at this stage of development is in its infancy in Kyrgyzstan. Thus, the digitalisation of the legal sector in Kyrgyzstan has immense potential to increase the efficiency and accessibility of justice, improve data protection and accelerate legal processes. However, for these technologies to reach their full potential, further investment is needed in modernising infrastructure, adapting the regulatory framework, and developing human resources capable of working with new digital tools.

In 2024, the Kyrgyz Republic's legal framework governing cybersecurity and data protection includes a series of key laws that stay in force but require adaptation and updating to meet the modern challenges of the digital world. The Law of the Kyrgyz Republic No. 210 (15) "On Protection of State Secrets of the Kyrgyz Republic" (Ministry of Justice of the Republic of Kazakhstan, 2023a) continues to play a vital role in protecting state data and regulating the protection of information important to the security of the country. It sets out rules about what information can be classified, who is entitled to access it, and how it should be protected. However, with digitalisation and increasing cyberthreats such as data breaches and cyber espionage, the law faces new challenges. Previous mechanisms for protecting state secrets, which focused mainly on physical protection and access control, are no longer sufficient to protect against the rise of cyberattacks and digital threats. In this regard, the law needs to be revised to strengthen provisions on electronic data protection and introduce new measures to prevent cyber espionage and leaks through digital channels.

The Law of the Kyrgyz Republic No. 217 "On the Right of Access to Information" (Ministry of Justice of the Republic of Kazakhstan, 2024c) regulates citizens' access to information held by state bodies and other institutions that are obliged to disclose information of public importance. This regulation is aimed at increasing transparency in the activities of the authorities, improving civil control, and ensuring the accountability of state structures to society. It also regulates the exceptions under which access to information may be restricted – for instance, where the information falls within the categories of state secrets, contains confidential data, or other restrictions established by legislation. However, with the development of digital technologies and the spread of information via the Internet, there is a need to adapt this law to the new conditions. Specifically, clarification and supplementation of the provisions on electronic data disclosure

is required, including issues of data transmission security, protection of personal data, and preservation of confidentiality when accessing information through digital channels.

The Law of the Kyrgyz Republic No. 125 "On the National Archive Fund of the Kyrgyz Republic" (Ministry of Justice of the Republic of Kazakhstan, 2023b) regulates the preservation, management, and access to archival documents and data. Archives contain important documents that are of historical, cultural, and national value, and protecting this data digitally becomes a critical task. With the active digitalisation of archives, there is an increasing risk of cyberattacks that could lead to leaks or corruption of electronic data. Therefore, the law needs to be updated to accommodate the latest methods of preserving electronic archives and the introduction of strict cybersecurity measures. There should also be mechanisms in place to protect data in case of leaks or attacks, as well as ways to recover information. The Law of the Kyrgyz Republic No. 31 "On the Electrical Connection" (Ministry of Justice of the Republic of Kazakhstan, 2023c) covers issues related to the provision of communication through electrical and postal channels, and it stays relevant in modern world, especially considering the digital economy. However, in the context of data transmission through digital channels, the law needs to be modernised to provide stronger measures to protect citizens' data. This includes strengthening cybersecurity for personal data transmitted through digital communication systems and implementing security standards that are in line with international norms. The law should also mandate the protection of data from interception, leaks, and hacking when transmitted via electronic means of communication.

The Civil Code (Ministry of Justice of the Republic of Kazakhstan, 2024a) and the Criminal Code of the Kyrgyz Republic (Ministry of Justice of the Republic of Kazakhstan, 2024b) are fundamental documents regulating liability for offences, including cybercrime. The Civil Code covers civil legal relations related to compensation for damages caused by a data breach or cybersecurity breach. For example, if a citizen's personal information has been stolen or used without authorisation, the victim may be able to sue for damages resulting from these actions. However, it is important that the law prescribe detailed rules on the types of liability and compensation for damages caused by cyber incidents. The Criminal Code regulates penalties for cybercrimes such as hacking into computer systems, data theft, digital fraud, and illegal use of information. However, against the backdrop of the growing threat of new cyberattacks, such as the spread of malicious software attacks on critical infrastructure (e.g., energy systems or transport), digital espionage, and phishing scams, current legislation needs to be better regulated and expanded.

Modern challenges such as ransomware attacks, where attackers block access to sensitive information and demand a ransom to restore it, must be considered. These types of offences may not always be fully covered by existing norms, creating legal gaps. Furthermore, cybercriminals are constantly improving their methods, which requires not only additions to legislation, but also the creation of specialised units to investigate such crimes. To successfully combat new threats, the concept of cybercrime needs to be introduced into legislation at

a deeper level, including the creation of relevant sanctions for such actions and the establishment of more severe penalties for offences related to critical infrastructure and massive data breaches. There should also be stricter liability for offences committed using international communication channels and Internet technologies, which is particularly important in the context of globalisation and the spread of transnational criminal groups.

Thus, the current regulatory framework of the Kyrgyz Republic needs comprehensive adaptation to the modern challenges of the digital world. Gaps in legislation relating to data protection and cybersecurity can lead to increased risks to citizens' rights and state security. It is therefore important not only to update existing regulations, but also to bring them in line with international standards such as the Council of Europe Convention on Cybercrime and GDPR. This will help to better counter cyberthreats and ensure data protection in a rapidly evolving digital environment. Specifically, international experience in cybersecurity, represented by examples from countries such as Estonia, Singapore, and Japan, offers effective strategies that can be adapted for the Kyrgyz Republic to strengthen data protection and prevent cyberattacks.

Estonia is one of the world leaders in cybersecurity, and its experience is of particular interest to countries looking to build a strong digital infrastructure. In 2007, Estonia faced a major cyberattack that paralysed its digital systems. This incident was the starting point for sweeping cybersecurity reforms. As a result, the National Cyber Security Centre was established to coordinate efforts to protect public and private systems from cyberattacks. The Centre plays a key role in developing a cyber defence strategy and cooperates with international organisations such as NATO to strengthen national security (Balagurchik, 2022).

Estonia is also actively developing a culture of cyber hygiene among its citizens. The state has introduced cybersecurity education programmes at all levels of education, from primary school to universities. This helps to create an informed attitude towards security in the digital environment, which reduces the risks of human error, often the cause of data breaches. The e-Estonia initiative to integrate digital technologies into public administration, the economy and the daily lives of citizens covers e-government, e-citizenship, and cybersecurity and could be useful for Kyrgyzstan. Specifically, through the creation of a cybersecurity centre that would not only prevent cyber incidents, but also establish interaction with international partners such as the UN and the Eurasian Economic Union. Furthermore, the introduction of cyber hygiene education programmes will help improve the overall digital literacy of the population, which will reduce the number of cybersecurity incidents (Cybil Portal, 2019).

Singapore is another prime example of a successful cybersecurity strategy. In 2016, the government unveiled a Comprehensive Cybersecurity Strategy that focuses on protecting critical infrastructures such as energy, transport, and banking. The strategy includes not only data protection measures, but also mandatory cybersecurity requirements for companies. All companies handling digital data must adhere to strict standards, which has considerably reduced the risks of data breaches. Singapore is also actively working with the private sector to develop cyber defence measures. The government has created specialised

institutions for training and certifying cybersecurity professionals, which has helped build a strong talent base. This cooperation has not only improved cyber defence, but also fostered the development of an entire industry in cybersecurity. Smart Nation Singapore is an initiative aimed at integrating digital technologies into public administration, the economy, and everyday life, with a special focus on data security Kyrgyzstan can use the experience of Singapore by creating a system of training specialists and introducing certification programmes. This will enable the country to nurture a workforce that can effectively counter cyberthreats. It is also important to work closely with the private sector and develop mandatory data protection standards for companies, which will improve the security of both government and commercial data (Cybil Portal, 2016).

Japan places strong emphasis on cybersecurity research and development. The country is actively investing in creating innovative data protection solutions and collaborating with private companies and academic institutions to develop innovative technologies. Special attention is paid to the protection of critical infrastructure, including energy systems, transport networks, and communications. Japan has established a series of government programmes to support cybersecurity research, making it a leader in the development of data protection solutions. Society 5.0 Japan is a strategy that combines digital technology and innovation to improve government efficiency and provide defence against cyberthreats. For Kyrgyzstan, the Japanese approach to cybersecurity could be a useful example. The country should consider establishing national research centres to develop innovative technologies for data protection. This will enable the development of the scientific base and the introduction of modern defence methods in key sectors of the economy. Protecting critical infrastructure such as power grids and transport networks should also be a priority in Kyrgyzstan's cybersecurity strategy (Cybil Portal, 2023).

Applying the experience of Estonia, Singapore, and Japan could significantly influence the development of cybersecurity in Kyrgyzstan. One of the first steps should be the establishment of a national cybersecurity centre that would not only coordinate efforts to prevent cyberattacks, but also engage in cooperation with international organisations and the private sector. It is also important to develop educational programmes to increase cyber literacy among the public, which will help reduce incidents related to human error. Furthermore, the Kyrgyz Republic should consider establishing certification programmes and training for cybersecurity professionals. Implementing mandatory data protection standards for businesses and government agencies will help improve the protection of personal and sensitive information. Japanese experience in R&D can also be useful. The establishment of national research centres and support for scientific developments will allow Kyrgyzstan to introduce innovative solutions and develop its cybersecurity to international standards.

Thus, Kyrgyzstan can drastically improve its data protection system if it adopts the best practices of countries that have already achieved success in this area. To improve cybersecurity in the Kyrgyz legal sector, it is worth considering a digital transformation model based on international practices and current challenges of digitalisation (Figure 1).

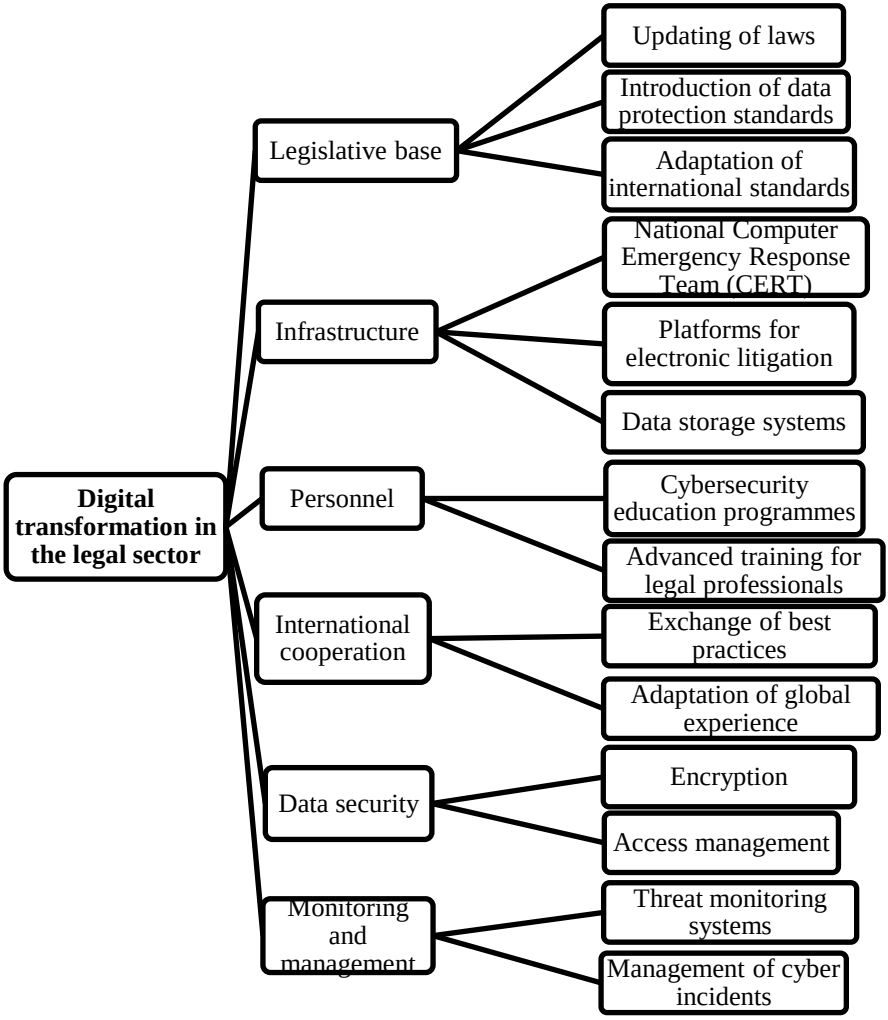

Figure 1 – Model of digital transformation in the legal sector

Note: CERT is the Computer Emergency Response Team.
Source: developed by the authors of this study.

The establishment of a national centre for cybersecurity will be a valuable tool in ensuring the protection of the country's digital assets and the rights of citizens. The centre will not only monitor cyberthreats and respond to incidents involving leaks of sensitive information but will also act as a coordinating body between various government agencies and the private sector. The national centre

can also become a platform for sharing experiences and data on cyberattacks, contributing to the overall level of security (Cybil Portal, 2022).

Data protection law reform is necessary to create an effective regulatory framework that can adapt to rapidly changing cyberthreats. Revising existing laws and implementing mandatory standards for legal actors will create a more robust data protection system. A system of regular audits and certification of legal information organisations could be introduced to ensure comprehensive monitoring of compliance with the newly introduced standards. This will not only provide an opportunity to improve data protection, but also to introduce accountability mechanisms for failure to meet cybersecurity standards. A key area of focus is also the introduction of modern information security technologies such as multi-factor authentication and automated threat detection systems. These technologies will help prevent unauthorised access to systems and protect legal data from cyberattacks. Particular attention should be paid to the protection of electronic evidence, which plays a vital role in court proceedings. The secure storage and transmission of such data should be a priority in the design of cybersecurity infrastructure.

Human resource development in cybersecurity requires the introduction of not only certification programmes, but also continuous professional development for legal staff. It is important that lawyers, judges, and other legal professionals understand the basic principles of cyber hygiene and can effectively liaise with IT departments to ensure a suitable level of information protection. The introduction of cybersecurity courses and trainings into the curricula of law schools can also contribute to the development of a new generation of specialists ready for the challenges of the digital age. Furthermore, data protection in litigation requires platforms that allow for the secure sharing of legal documents and other sensitive information. These platforms must support data encryption and secure electronic signatures to prevent unauthorised access and ensure the legal validity of documents. The introduction of such technologies into judicial practice can accelerate the processing of cases and improve their quality.

Thus, international practices and standards such as the GDPR can help Kyrgyzstan develop a legal framework that meets exacting security requirements, leading to better data protection and increased citizen confidence in the legal system.

DISCUSSION

Based on the findings obtained, digital transformation is a key tool for increasing transparency, efficiency, and sustainability of public administration in the Kyrgyz Republic. The digitalisation of public services and the automation of many processes can substantially reduce the impact of the human factor and minimise corruption risks. However, one of the principal challenges identified by the study is the lack of digital infrastructure, especially in remote and rural areas of the country. This prevents the benefits of the digital economy from being evenly distributed among the population and hinders access to digital public

services. Gómez-Carmona et al. (2023) noted analogous problems, reporting that in countries with less developed infrastructure, such as Kyrgyzstan, significant investments are needed to improve digital infrastructure and ensure equal access to digital services. While O. Gómez-Carmona et al. focus on the development of smart communities and the integration of digital solutions in rural areas, the present study shifts the focus to the digitalisation of public services and the creation of infrastructure to support them. The findings of this study also emphasise that this not only improves the quality of public services, but also ensures greater transparency and accountability of state structures.

An important driver of digital transformation is the development of digital skills, especially among small and medium-sized enterprises (SMEs). Clemente-Almendros et al. (2024) emphasise that without proper training it is impossible to achieve full digital inclusion in SMEs. This supports the findings of the present study, where the need for additional education and certification programmes for employees was identified. However, J.A. Clemente-Almendros et al. do not consider the significance of cybersecurity certification as noted in the current study. The Tunduk e-interaction system has substantially increased the transparency and efficiency of data exchange between government agencies but requires an improved legal framework for data protection. This is consistent with the findings of Begany and Gil-Garcia (2024) who emphasise the need for a regulatory framework to protect open government data. In contrast to the cited study, the current study focused more on technical and organisational data protection measures.

The present study also showed the need for a systematic approach to cybersecurity to protect public and personal data, which is supported by the findings of Al-Daajeh and Alrabaee (2024). Both studies agree that without a strategic approach, data protection will be ineffective. However, the current study proposes the development of safety standards, which was not the focus of the study by Al-Daajeh and Alrabaee. Furthermore, cybersecurity for SMEs, which are still vulnerable to cyberattacks, is a critical aspect. Hoong and Rezania (2024), Racionero-Garcia and Shaikh (2024) also emphasise the need for enhanced data protection for SMEs. However, this study adds that there is a need to create mandatory safety standards for all market players.

With the deployment of 5G technologies, data protection is a key aspect of digital infrastructure development. Akcali Gur (2022) emphasised that new cybersecurity challenges arise with the introduction of 5G in Europe. Both studies point to the need for enhanced legal protection of data, but the current study emphasises the challenges for a developing country. Citizens' awareness of cybersecurity laws is important for their protection. Nguyen (2023) emphasised the significance of media representations of cyber laws in raising public awareness. Both studies emphasise the importance of communication, but the current study focused on improving legal communication between the state and citizens.

Furthermore, it was found that the development of cloud services requires additional data protection measures. This is in line with the findings of Kun (2024) who discusses the need to regulate cloud services in the European Union for data

protection. Unlike the European Union, Kyrgyzstan has yet to develop relevant standards for cloud services. Moreover, the right to cybersecurity should be consolidated legislatively to ensure data protection. Chiara (2024) and Vostoupal et al. (2024) explore this issue in the context of EU legislation, arguing that the right to cybersecurity should be institutionalised. Both studies show that this right needs to be consolidated legislatively, but the present study focused on adapting this right in the context of developing countries.

The study also showed that the use of artificial intelligence can play a key role in cybersecurity, especially in the banking sector. Rodrigues et al. (2022) analysed the specific features of implementing artificial intelligence to improve cybersecurity in the financial sector. Both studies agree that artificial intelligence can improve data security, but the current study focused on the challenges of implementing these technologies in developing countries. In addition, artificial intelligence can be an effective tool to protect critical infrastructures as proved in the study by Sarker et al. (2024). Both studies emphasise that artificial intelligence plays a significant role in cybersecurity, but the present study focused more on the integration of artificial intelligence in government agencies.

Establishing national research centres to address cybersecurity issues can considerably improve data protection. Macas et al. (2022) support this and consider the deep learning technologies a key element to improve monitoring and response to cyberattacks. Both studies emphasise the significance of innovative technologies, but the present study focuses on the establishment of centres for adapting these technologies in Kyrgyzstan. Al-Dosari et al. (2023) emphasised the importance of sustainable development in cybersecurity, especially in the context of transport infrastructure. This is in line with the findings of the present study, which also noted the need for sustainable data protection systems in various sectors of the economy.

Reporting standards need to be developed to ensure cybersecurity reporting and monitoring. Boggini (2024) addresses this issue in the context of the European Union, arguing that cybersecurity monitoring and reporting play a key role in the transparency of government agencies. Both studies support the need for standardisation of reporting, but the present study considered the challenges for developing countries specifically. Thus, the findings of the present study are consistent with the those of other researchers, confirming that digital transformation requires an integrated approach that includes infrastructure development, training, legal protection, and the introduction of innovative technologies.

Digital transformation in Kyrgyzstan faces a series of major challenges, including uneven development of digital infrastructure, lack of qualified personnel, especially in cybersecurity, and the need to modernise the legal framework for data protection. The study found that the greatest challenges to digital inclusion are in remote regions where access to the internet and digital services is still limited. Despite the positive results of the implementation of systems such as Tunduk and the development of digital skills among the population, more attention needs to be paid to cybersecurity and data protection, especially in the evolving digital economy. These findings are consistent with the

findings of Kuzior et al. (2022), Fischer-Hübner et al. (2021), and Aljaradat et al. (2024), who also highlight the need for an integrated approach to digitalisation, including infrastructure development, legal protection, staff training, and the introduction of innovative technologies. However, unlike studies focused on developed countries, the present study focused on the specifics of digitalisation in a developing country context, which makes its findings particularly important for the future development of Kyrgyzstan and other countries with analogous challenges.

CONCLUSIONS

Data protection and information security challenges are becoming increasingly urgent, while conventional defence methods can no longer handle the dynamically evolving cyberthreats. The application of international standards, such as GDPR, can provide a sound basis for developing a national cybersecurity strategy. The implementation of these standards can substantially increase the level of protection of citizens' personal data and create more favourable conditions for the country's integration into the international digital economy.

One crucial step in the proposed strategy is the creation of a national cybersecurity centre that would coordinate the efforts of various public and private organisations to combat cybercrime. The centre could also be a platform for disseminating knowledge about cyber hygiene to the public, which would help raise citizens' awareness of the significance of protecting their data and the correct use of digital technologies. This is crucial in the face of increasing attacks on government information systems and private companies. The study also confirmed the need to develop human resource capacity in the field of information security. The introduction of educational programmes as well as certification courses for legal, IT, and cybersecurity professionals is a mandatory step towards the successful implementation of digital transformation strategies. These measures will not only raise awareness of cyberthreats but will also ensure that effective tools for data protection are implemented at the public and private levels.

Limitations of this study include the lack of long-term data on the results of digital transformation in the Kyrgyz Republic. With many digital initiatives in the country in the early stages of implementation, the long-term effects of these changes are not yet fully visible. This complicates a full understanding of how successful the implemented technologies and legal mechanisms have been. Another limitation is the lack of localised data on cyberattacks and cyberthreats, which complicates the development of detailed national cybersecurity strategies.

In the future, it is important to continue to monitor threats and conduct regular research in this area to update existing data protection strategies promptly and ensure that they adapt to changing conditions. Prospects for further research may also include the development of more comprehensive and nationally adapted data protection mechanisms. It is vital to to examine international practices in the digitalisation of the legal system and cybersecurity in greater depth to identify best practices for implementation in Kyrgyzstan. Specifically, investigating

successful cybersecurity strategies in countries with comparable socioeconomic conditions, such as Georgia, Armenia, and Mongolia, can help create more sustainable and effective solutions to protect data and prevent cyberattacks.

Promising areas of research include monitoring the effectiveness of implemented technologies and their adaptation to national legislation. It is important to investigate how international standards such as GDPR can be integrated into Kyrgyzstan's legal system and to assess the performance of the existing cybersecurity infrastructure. Special attention should be paid to the development of legal and technological mechanisms to minimise the risks associated with new types of cyberthreats, including attacks on critical infrastructure and government systems. Research on the impact of digital transformation on SMEs, especially in cybersecurity, is also promising.

REFERENCES

Ahmed, R.K., Muhammed, K.H., Qadir, A.O., Arif, S.I., Lips, S., Nyman-Metcalf, K., Pappel, I., Draheim, D. (2021). A legal framework for digital transformation: A proposal based on a comparative case study. In: A. Kö, E. Francesconi, G. Kotsis, A.M. Tjoa & I. Khalil (Eds.), *Proceedings of the 10th International Conference "Electronic Government and the Information Systems Perspective"* (pp. 115-128). Cham: Springer. https://doi.org/10.1007/978-3-030-86611-2_9

Akcali Gur, B. (2022). Cybersecurity, European digital sovereignty and the 5G rollout crisis. *Computer Law & Security Review, 46,* 105736. https://doi.org/10.1016/j.clsr.2022.105736

Al-Daajeh, S. & Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security, 141,* 103845. https://doi.org/10.1016/j.cose.2024.103845

AL-Dosari, K., Fetais, N. & Kucukvar, M. (2023). A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector. *International Journal of Sustainable Transportation, 17(12),* 1287-1301. https://doi.org/10.1016/j.susctrans.2023.103056

Aljaradat, A., Sarkar, G. & Shukla, S.K. (2024). Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach. *Journal of Economic Criminology, 5,* 100089. https://doi.org/10.1016/j.jeconc.2024.100089

Balagurchik, D. (2022). "Largest since 2007". Estonia fends off powerful cyberattack after dismantling Soviet monument. Available at: https://nv.ua/amp/estoniya-otrazila-samuyu-masshtabnuyu-kiberataku-s-2007-goda-posle-demontazha-sovetskogo-pamyatnika-50264055.html

Begany, G.M. & Gil-Garcia, J.R. (2024). Open government data initiatives as agents of digital transformation in the public sector: Exploring the extent of use among early adopters. *Government Information Quarterly, 41(3),* 101955. https://doi.org/10.1016/j.giq.2024.101955

Chiara, P.G. (2024). Towards a right to cybersecurity in EU law? The challenges

ahead. *Computer Law & Security Review*, *53*, 105961. https://doi.org/10.1016/j.clsr.2024.105961

Clemente-Almendros, J.A., Nicoara-Popescu, D. & Pastor-Sanz, I. (2024). Digital transformation in SMEs: Understanding its determinants and size heterogeneity. *Technology in Society*, *77*, 102483. https://doi.org/10.1016/j.techsoc.2024.102483

Cybil Portal. (2016). Singapore-United States third country training programme (TCTP) cybersecurity workshops. Available at: https://cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/

Cybil Portal. (2019). EU CyberNet. Available at: https://cybilportal.org/projects/eu-cybernet/

Cybil Portal. (2022). The role of the EU's cyber ecosystem in the global cyber security stability. Available at: https://cybilportal.org/projects/the-role-of-the-eus-cyber-ecosystem-in-the-global-cyber-security-stability/

Cybil Portal. (2023). Project for improvement of cyber resilience. Available at:https://cybilportal.org/projects/project-for-improvement-of-cyber-resilience/

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L. & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916. https://doi.org/10.1016/j.jisa.2021.102916

Gómez-Carmona, O., Buján-Carballal, D., Casado-Mansilla, D., López-de-Ipiña, D., Cano-Benito, J., Cimmino, A., Poveda-Villalón, M., García-Castro, R., Almela-Miralles, J., Apostolidis, D., Drosou, A., Tzovaras, D., Wagner, M., Guadalupe-Rodriguez, M., Salinas, D., Esteller, D., Riera-Rovira, M., González, A., Clavijo-Ágreda, J., Díez-Frias, A., Bocanegra-Yáñez, M. del C., Pedro-Henriques, R., Ferreira-Nunes, E., Lux, M. & Bujalkova, N. (2023). Mind the gap: The AURORAL ecosystem for the digital transformation of smart communities and rural areas. *Technology in Society*, *74*, 102304. https://doi.org/10.1016/j.techsoc.2023.102304

Hoong, Y. & Rezania, D. (2024). Navigating cybersecurity governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers & Security*, *142*, 103852. https://doi.org/10.1016/j.cose.2024.103852

International Telecommunication Union. (2021). Report "ITU-D study on potential development trends in the CIS Region directions for the development of the CIS region in the period 2022-2025. Direction – Digital skills". https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Track%20-%20Digital%20Skills.pdf

Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. *Computer Law & Security Review*, *52*, 105931. https://doi.org/10.1016/j.clsr.2023.105931

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity, 8(4),* 195. https://doi.org/10.3390/joitmc8040195

Macas, M., Wu, C. & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks, 212,* 109032. https://doi.org/10.1016/j.comnet.2022.109032

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C. & Ioannidis, S. (2020). Cybersecurity in the era of digital transformation: The case of Greece. In: *Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (pp.* 1-5). Piscataway: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ITIA50152.2020.9312297

Mijwil, M.M., Filali, Y., Aljanabi, M., Bounabi, M. & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. *Mesopotamian Journal of Cybersecurity, 2023,* 1-6. https://doi.org/10.58496/MJCS/2023/001

Ministry of Digital Development of the Kyrgyz Republic. (2024). Concept Digital Transformation of the Kyrgyz Republic for 2024-2028. Available at: https://digital.gov.kg/en/activities/konczkpcziya-czifrovoj-transformaczii-kyrgyzskoj-respubliki-na-2024-2028-gody/

Ministry of Justice of the Republic of Kazakhstan. (2018). Decree of the President of the Kyrgyz Republic No. 221 "On the National Development Strategy of the Kyrgyz Republic for 2018-2040". Available at: https://cbd.minjust.gov.kg/430002/edition/1095562/ru

Ministry of Justice of the Republic of Kazakhstan. (2019). Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023. Available at: https://cbd.minjust.gov.kg/15479/edition/962966/ru

Ministry of Justice of the Republic of Kazakhstan. (2023a). Law of the Kyrgyz Republic No. 210 (15) "On Protection of State Secrets of the Kyrgyz Republic"**.** Available at: https://cbd.minjust.gov.kg/111719/edition/1229912/ru

Ministry of Justice of the Republic of Kazakhstan. (2023b). Law of the Kyrgyz Republic No. 125 "On the National Archive Fund of the Kyrgyz Republic". Available at: https://cbd.minjust.gov.kg/4-274/edition/1251127/ru

Ministry of Justice of the Republic of Kazakhstan. (2023c). Law of the Kyrgyz Republic No.31 "On the Electrical Connection". Available at: https://cbd.minjust.gov.kg/42/edition/1286788/ru

Ministry of Justice of the Republic of Kazakhstan. (2024a). Civil Code of the Kyrgyz Republic No. 15. Available at: https://cbd.minjust.gov.kg/4/edition/7214/ru

Ministry of Justice of the Republic of Kazakhstan. (2024b). Criminal Code of

the Kyrgyz Republic No. 127. Available at: https://cbd.minjust.gov.kg/112309/edition/2087/ru

Ministry of Justice of the Republic of Kazakhstan. (2024c). Law of the Kyrgyz Republic No. 217 "On the Right of Access to Information". Available at: https://cbd.minjust.gov.kg/4-5355/edition/11754/ru

Möller, D.P.F. (2023). Cybersecurity in digital transformation. In: *Guide to Cybersecurity in Digital Transformation* (pp. 1-70). Cham: Springer. https://doi.org/10.1007/978-3-031-26845-8_1

Nainggolan, B. (2023). Legal dynamics in the digital era: Navigating the Impact of digital transformation on Indonesian society. *Law Development Journal, 5(4),* 714-728. Available at: https://jurnal.unissula.ac.id/index.php/ldj/article/view/36838

National Statistical Committee of the Kyrgyz Republic, Institute of Statistical Research and Professional Development. (2020). Analytical note: Assessment of digital transformation in the Kyrgyz Republic. Available at: https://stat.gov.kg/media/files/2d3ce15c-2581-42cf-b693-8c9dbe33ecdf.pdf

Nguyen, M.Q. (2023). Media presentations of Vietnam's cybersecurity law: A comparative approach with corpus-based critical discourse analysis. *Computer Law & Security Review, 50,* 105835. https://doi.org/10.1016/j.clsr.2023.105835

Popa Tache, C.E. & 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. https://doi.org/10.1080/23311886.2024.2370945

Racionero-Garcia, J. & Shaikh, S.A. (2024). Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives. *Space Policy,* 101648. https://dx.doi.org/10.2139/ssrn.4765696

Regional United Nations Group for Europe and Central Asia on Digital Transformation. (2021). Supporting digital transformation in Europe and Central Asia: Accelerating achievement of sustainable development goals. Available at:https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2021/Cross%20cutting%20session%20on%20digitalization/Stocktaking%20ICTs%20solutions_10_Mar_FINAL%20(1).pdf

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

Rodrigues, A.R.D., Ferreira, F.A.F., Teixeira, F.J.C.S.N. & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance, 60,* 101616. https://doi.org/10.1016/j.ribaf.2022.101616

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., Alabbad, D.A. (2023).

Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors, 23(15)*, 6666. https://doi.org/10.3390/s23156666

Sarker, I.H., Janicke, H., Ferrag, M.A. & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things, 25*, 101110. https://doi.org/10.1016/j.iot.2024.101110

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.

Uwadinma, A.I. & Ikeatu, E.G. (2024). Digital transformation for digital law practice in Nigeria. *Nigerian Journal of Legal Studies, 13*, 100-113. Available at:https://www.nigerianjournalsonline.com/index.php/NJLS/article/view/4699

Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P. & Malinka, K. (2024). The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. *Computer Law & Security Review, 53*, 105988. https://doi.org/10.1016/j.clsr.2024.105988

World Bank Group. (2024). Digital progress and trends report 2023. Available at: https://www.worldbank.org/en/publication/digital-progress-and-trends-report

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