Problems and Prospects of Digitalisation in the Field of Jurisprudence to Ensure Cyber Protection of Information

Submitted: 25 November 2024
Reviewed: 25 January 2025
Revised: 13 February 2025
Accepted: 18 February 2025

Henris Balliu[*]
https://orcid.org/0009-0008-5994-0271
Erisa Xhixho[**]
https://orcid.org/0009-0009-2869-5629
Nazira Abdukarimova[***]
https://orcid.org/0000-0002-6353-2528
Nazgul Adylova[****]
https://orcid.org/0009-0000-4852-1321
Nail Abbasov[*****]
https://orcid.org/0000-0002-2713-8697

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.56248

Abstract

[Purpose] The purpose of the study is to examine the impact of digitalisation on the field of jurisprudence with a special focus on ensuring cyber protection of information.

[Methodology/approach/design] The study methodology includes the analysis of cyber threats for law firms, such as phishing and distributed denial of service (DDoS) attacks, an assessment of international cybersecurity standards (Budapest Convention, ISO/IEC 27001), and the use of modern security technologies (encryption, multi-factor authentication).

[Findings] Employee training programmes and the possibilities of using artificial intelligence and machine learning to automate data protection were examined. Electronic platforms simplify the exchange of documents and increase the transparency of interactions due to the session recording function. The legal field is facing acute cybersecurity problems

[*]Lecturer at the Department of Public Law, University of Tirana, 1010, 4 Mother Teresa Str., Tirana, Albania. E-mail: balliuhenris@gmail.com.
[**]Full Doctor, Researcher at the Department of Public Law, University of Tirana, 1010, 4 Mother Teresa Str., Tirana, Albania. E-mail: erisaxhixho@outlook.com.
[***]Full Doctor, Professor at the Faculty of Law, Jusup Balasagyn Kyrgyz National University, 720033, 547 Frunze Str., Bishkek, Kyrgyz Republic. E-mail: abdukarim_na@hotmail.com.
[****]PhD, Associate Professor at the Faculty of Law, Jusup Balasagyn Kyrgyz National University, 720033, 547 Frunze Str., Bishkek, Kyrgyz Republic. E-mail: n.adylova@outlook.com.
[*****]PhD, Researcher at the Department of Humanitarian Sciences, Baku Business University, AZ1122, 88A H. Zardabi Str., Baku, Azerbaijan. E-mail: nail-abbasov@hotmail.com.

due to the processing of confidential information. The main types of cyber-attacks faced by law firms include phishing, ransomware, and DDoS attacks. Each of these attacks can have serious consequences for data security, the reputation of companies, and their ability to provide legal services.
[Practical implications] The research underscores the critical need for law firms to implement robust cybersecurity measures, including compliance with international standards and regular employee training, to protect sensitive information and maintain client trust. This shift not only enhances operational efficiency and compliance but also positions firms competitively in a digitally-driven market, ultimately impacting client access to legal services and the overall landscape of legal practice.
[Originality/value] The development of specialised software for the legal field has opened up new opportunities to improve the efficiency and protection of information, ensuring compliance with legislation and integration with external systems.

Keywords: Virtual Consultations. DDoS Attacks. Quantum Encryption. Cybersecurity. Control Systems. Automation.

INTRODUCTION

Digitalisation has substantially transformed the legal field, which is associated with a sharp increase in the volume of electronic data and the active use of digital tools for creating, storing, and processing documents. The transition to electronic documents simplifies the search, access, and exchange of information, which speeds up processes and increases the efficiency of law firms. In addition, the use of cloud technologies allows providing access to data from anywhere in the world and facilitates the work of remote employees. Collaboration on documents becomes easier due to the possibility of simultaneous editing and a simplified approval process.

Nevertheless, the transition to electronic document management is not without risks. Electronic documents are subject to cybersecurity threats, requiring substantial investments in data protection (Nurbatyrova et al., 2024). Dependence on technology can also become a problem, as technical failures or loss of Internet access can temporarily paralyse the company's work. In addition, not all jurisdictions recognise electronic documents equally with paper ones, which complicates the work with international cases. The transition to electronic document management also requires training of employees in new technologies, which can be difficult for those who are accustomed to traditional working methods (Kerimkhulle et al., 2023). Digitalisation in law creates many critical challenges, among which the issues of cybersecurity and technological sustainability are highlighted (Amelin et al., 2021). Switching to electronic documents and virtual consultations substantially increases the vulnerability of law firms to cyber-attacks, which can lead to the leakage of confidential

information and serious financial losses (Ginters et al., 2014). Additionally, dependence on technology and insufficient technical training of employees can disrupt the company's work in the event of failures or loss of Internet access. Differences in the legal systems of different jurisdictions also complicate the recognition of electronic documents, which necessitates additional efforts to comply with regulatory requirements in international affairs. The use of outdated technologies increases information security risks, making it difficult to meet modern data protection standards (Gafni et al., 2024). In addition, insufficient employee awareness of cyber threats and new technologies weakens protection and hinders the development of effective response strategies. These problems underline the need for an integrated approach to ensuring cybersecurity in the context of the rapid development of digitalisation in the legal field.

The problem identified in the field under study is that digitalisation in the field of law, although it opens up new opportunities for optimising processes and increasing efficiency, also creates substantial challenges for ensuring cyber protection of information. A study by Khomyshyn et al. (2022) has identified the main system engineering problems associated with the use of computer and digital technologies in legal activities, especially in the context of data security. Adonis (2020) examined gaps in existing international legal instruments, especially in the context of digital sovereignty, where public and private actors face problems regulating cross-border data movement and the need to ensure their security within different jurisdictions. Gaps requiring further study include the lack of uniform international standards for regulating the use of cloud services, blockchain technologies, and artificial intelligence (AI) in legal practice. The main problem is that, despite the rapid growth of digitalisation in the legal field, existing systems and processes do not have time to adapt to new challenges in the field of cybersecurity. This is especially relevant in the context of protecting human rights and ensuring the confidentiality of information.

Pyrohovska et al. (2024) in her research emphasises that the development of information technology creates both new opportunities for the protection of human rights and new threats. Abdalla Abdelkarim (2024) considered emerging issues at the intersection of cyberspace and law, defining cyber jurisprudence as a new area of legal science. The development of standards guaranteeing the protection of human rights in the digital environment, including the right to privacy and data security, requires further investigation. Another urgent problem is the gap between rapidly developing digital technologies and outdated legal norms, which makes it difficult to implement effective cyber defence. Ofori and Akoto (2020) analysed problems related to law enforcement and the admissibility of digital evidence in court proceedings. A study by Bakhramova et al. (2023) covers aspects of the digital transformation of legal services, pointing to the need

to increase fairness and efficiency in the context of digitalisation. The necessary areas for further analysis are the optimisation of the integration of modern technologies into legal practice and the development of new cyber defence standards to improve the effectiveness of data protection and information security. Another problem requiring additional research is that digitalisation in the field of jurisprudence requires a review of the priorities of legal regulation. Sidorenko and von Arx (2020) examined the transformation of law in the context of digitalisation, highlighting the need to determine the right priorities in the legal field. Manko et al. (2023) investigated the legal regulation of the digital environment and identified gaps in the regulation of the state legal and law enforcement sphere. It is necessary to improve the regulation of the digital environment to ensure proper cyber protection.

The purpose of the study was to analyse the impact of digitalisation on the legal sphere with a special focus on the issues of information protection from cyber threats. Within the framework of this goal, the following tasks were set:

1.Investigate the impact of the transition to electronic documents and virtual consultations on cybersecurity in legal practice.

2.Assess the risks and challenges associated with the use of outdated technologies and insufficient knowledge of cyber threats among legal professionals.

3.Analyse modern technologies and methods of data protection, such as cryptography, multi-factor authentication, and biometric systems, in the context of their application in the legal field.

4.Develop a methodology that includes a comprehensive study and analysis of the problems and opportunities of digitalisation in the field of law, with a focus on ensuring the cybersecurity of data.

MATERIALS AND METHODS

The study employs a mixed-methods approach to analyse the impact of digitalisation on the legal field, particularly focusing on cybersecurity threats and protective measures. A comprehensive analysis of cyber threats to law firms, including phishing, ransomware, and distributed denial-of-service (DDoS) attacks, was conducted. Additionally, an assessment of international cybersecurity standards, such as the Budapest Convention on Cybercrime and ISO/IEC 27001, was undertaken to evaluate their applicability in legal practice. The study also considers the effectiveness of modern security technologies, including encryption, multi-factor authentication (MFA), and biometric systems, in ensuring data protection. The study examined employee cybersecurity training programmes such as KnowBe4, Cofense PhishMe, and CyberSafe, as well as anti-phishing methods, including the use of spam filters and employee training. The

features of ransomware programmes that encrypt data on infected systems and demand a ransom for their recovery are also analysed.

The research methodology integrates a combination of qualitative and quantitative methods. The qualitative aspect involved an in-depth review of academic literature, legal frameworks, and case studies related to cybersecurity in legal practice. Key sources include peer-reviewed journal articles, industry reports, and regulatory documents that provide insights into the evolving cyber threats and countermeasures within the legal sector. The quantitative component involved a statistical analysis of cyber-attack incidents targeting law firms, drawing upon publicly available cybersecurity reports and datasets.

The primary data collection involved semi-structured interviews with cybersecurity experts and legal professionals. These interviews aimed to understand the challenges faced by law firms in implementing cybersecurity measures and to explore best practices for mitigating cyber threats. The participants included IT security specialists, legal practitioners, and compliance officers from law firms of various sizes. Thematic analysis was applied to categorise responses and identify recurring themes regarding cybersecurity challenges and solutions in legal practice. Furthermore, a case study approach was employed to examine notable cybersecurity breaches in the legal sector. This included the analysis of cyber-attacks on law firms in Albania, Kyrgyzstan, and Azerbaijan, highlighting the consequences of inadequate cybersecurity measures. These case studies provided empirical evidence of the risks associated with digitalisation and underscored the importance of robust cybersecurity policies.

To assess the impact of modern security technologies on mitigating cyber threats, a comparative analysis was conducted. The effectiveness of encryption technologies, including asymmetric and quantum encryption, was examined in the context of legal document protection. Additionally, the role of MFA and biometric authentication in preventing unauthorised access to legal databases was analysed. A risk assessment model was developed to compare cybersecurity vulnerabilities before and after the implementation of these technologies, using data compiled from cybersecurity reports and law firm security audits. International regulatory frameworks were reviewed to assess the compliance requirements for law firms operating in multiple jurisdictions. The study examined the implications of GDPR and other data protection regulations on legal practice, particularly in relation to client confidentiality and cross-border data transfers. The role of international agreements, such as the Budapest Convention, in fostering global cooperation on cybercrime prevention was also considered.

The limitations of the study include its reliance on publicly available cybersecurity reports, which may not capture all incidents due to underreporting. Additionally, while case studies provide valuable insights, their findings may not

be universally applicable to all legal firms. Future research could explore emerging cybersecurity technologies and their long-term implications for legal practice. The study's findings contribute to understanding how digitalisation affects the security of legal information and provide recommendations for strengthening cybersecurity measures in the legal profession.

RESULTS

Digitalisation has substantially changed the legal field, leading to an increase in the volume of electronic data and the use of digital tools for creating, storing, and processing documents. Electronic documents simplify the search, access and transfer of information, which speeds up processes and increases the efficiency of law firms. It also reduces the cost of paper, printing, and storage, which can lead to substantial savings in the long run. In addition, electronic documents can be stored in cloud services, providing convenient access from anywhere in the world and simplifying the work of remote employees. Collaboration on documents also becomes easier due to the possibility of simultaneous editing and simplification of the approval process.

However, the transition to electronic documents involves certain risks. Electronic documents are subject to cybersecurity threats, requiring substantial investments in data protection. Dependence on technology can also become a problem, as technical failures or loss of Internet access can temporarily paralyse the company’s work. In addition, not all jurisdictions recognise electronic documents equally with paper ones, which can complicate the work with international cases. The transition to electronic document management also requires staff training in new technologies, which can be difficult for employees accustomed to traditional working methods. Virtual legal consultations conducted through video conferences, online chats, and specialised platforms provide a convenient way to receive legal assistance. They allow clients to receive consultations from the comfort of home, which is especially important in conditions of remote work or the impossibility of face-to-face meetings. This saves time and resources, allowing lawyers to manage their schedules more flexibly, and clients to receive consultations faster without having to visit the office. Electronic platforms also simplify the exchange of documents and increase the transparency of interaction through session recording functions.

However, virtual consultations are associated with certain challenges. Ensuring data privacy and security is becoming critically important, as virtual consultations can be vulnerable to cyber-attacks. The need to adapt to new technologies can also create difficulties for some clients and lawyers. In addition, the lack of personal contact can make it difficult to establish trusting relationships, which is especially important in cases requiring a delicate approach. In the legal

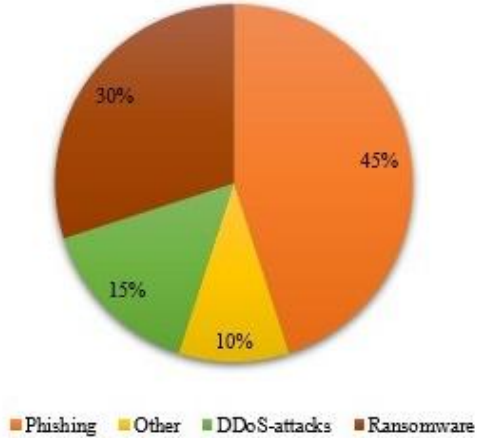
field, cybersecurity issues are becoming particularly acute, since law firms process a huge amount of confidential and sensitive information related to client cases, commercial contracts, intellectual property, and other important data (Karovska Andonovska & Taneski, 2020). The main types of cyber-attacks faced by law firms include phishing, ransomware, and DDoS attacks. Each of these attacks has serious implications for data security, the reputation of companies, and their ability to provide legal services. Phishing is one of the most common and dangerous threats to law firms (Gupta et al., 2020). Attackers send emails or messages disguised as trusted sources, such as partners or clients of the company, to deceive employees and gain access to their credentials or other confidential data. If an employee, unaware of the trick, opens such an email and clicks on a link or downloads an attachment, malicious software can take control of their computer or the company's network. The consequences of such attacks can be devastating, including the leakage of confidential information, disruption of the company and substantial financial losses.

Law firms can use various methods, including the use of spam filters and employee training to protect against phishing. An important part of the training is to inform employees about the methods of recognising phishing attacks and the correct actions if they are detected. Examples of programmes that help train employees include KnowBe4, which provides interactive phishing courses and simulations to increase security awareness; Cofense PhishMe, which offers practical scenarios and management of phishing attack reports; and CyberSafe, which focuses on cyber threat training through video tutorials and quizzes. These programmes help employees develop cybersecurity skills, which reduces the risk of successful phishing attacks and improves the overall protection of information in a law firm (Veasey, 2019). Ransomware poses another serious threat to law firms. Such programmes encrypt company data, blocking access to it until a ransom is paid. In the legal field, where access to documents and information is crucial for the performance of daily duties, an attack using a ransomware programme can paralyse the work of a firm for a long time. Even if the ransom is paid, there is no guarantee that the data will be restored, and the loss of reputation can lead to a loss of customer trust and a reduction in the customer base.

DDoS attacks are aimed at overloading the servers or networks of a law firm, making them inaccessible to employees and clients (Widespread cyberattack blocks..., 2022). Although such attacks do not lead to data leaks, they can disrupt online services, slow down the processing of cases and cause customer dissatisfaction. In legal practice, where timing and efficiency play an important role, even short-term failures can lead to serious consequences, including violation of agreements and legal liability to clients. All of these types of attacks have a substantial impact on law firms. In addition to direct financial losses due

to extortion, downtime, and loss of customers, firms may face additional costs for data recovery, security upgrades, and legal liability for data leaks. In addition, affected firms may lose their reputation, which will negatively affect their business in the long run. In this regard, law firms need to pay special attention to cybersecurity measures, including employee training, the introduction of modern security technologies and regular security audits. Figure 1 shows the distribution of different types of cyber-attacks in law firms and helps to understand which types of attacks are the most common, which is important for prioritising cybersecurity measures.

Figure 1 – Distribution of types of cyber-attacks in law firms



Leaks of confidential information in the legal field can have disastrous consequences for both clients and the law firm itself. For example, in 2019, Albania experienced a substantial leak of confidential information related to a cyberattack on government and financial institutions (Sultanbayeva et al., 2023). The attack exposed the personal data of thousands of citizens, including passport numbers, addresses, and financial information. This incident has led to concern among the public and has caused a need for improved data protection. In response to the leak, the Albanian authorities began reviewing cybersecurity laws and measures and implementing new protocols to protect personal information (Haciyeva, 2021). The attack also led to legal consequences for the affected institutions, which faced the need to pay compensation and increase security to meet the new standards.

In Kyrgyzstan, in 2020, a data leak was recorded from the database of one of the largest banking structures in the country (Pandey et al., 2020). As a result of the attack, the perpetrators gained access to the personal information of the

bank's customers, including account numbers, transaction data, and personal data. This incident caused a resonance in the country and led to the need for an audit of the security of banking systems. The affected bank has faced legal consequences such as lawsuits from customers, claims for damages and fines from regulators for violating data security standards. In response to the leak, the bank has taken several measures to improve cyber security. A comprehensive audit of security systems was conducted to identify vulnerabilities, after which modern security technologies such as multi-level authentication and data encryption were implemented to prevent access by intruders. Information campaigns were launched to raise customer awareness, which included recommendations on creating strong passwords and recognising phishing attacks. Cybersecurity trainings were also conducted for the bank's employees to increase their knowledge of possible threats and protection methods. The Bank began to actively cooperate with government regulators to comply with and improve data security standards, which also included the introduction of new rules and procedures.

In Azerbaijan, in 2021, there was a data leak from the state register, which affected a large number of citizens and organisations (Talesh & Cunningham, 2021). As a result of the attack on systems containing important information, data on taxpayers, businesses, and individuals were disclosed. This incident has led to serious consequences for data privacy and disrupted the work of government agencies. The Azerbaijani authorities were forced to conduct a comprehensive investigation and implement new security measures to prevent similar incidents in the future. The legal consequences included the need to comply with new data protection standards and possible penalties for violating personal information protection laws.

The lack of cybersecurity qualifications among legal professionals is a substantial problem that can affect the level of cyber protection in law firms. Legal professionals who do not have sufficient knowledge of modern threats may not realise the scale and nature of the risks, which leads to an incorrect assessment of threats and insufficient data protection. This increases the likelihood of successful cyber-attacks. The lack of incident response strategies can also be a problem, as insufficient qualifications make it difficult to develop and implement effective action plans. This delays the response time to attacks, exacerbating the consequences and complicating data recovery. In addition, a lack of knowledge about regulatory requirements can lead to non-compliance with legislation, which is fraught with fines and legal problems. Lack of qualifications also makes it difficult to choose the right security technologies, which reduces the level of cybersecurity. Problems with employee training can worsen the situation, as a lack of awareness among them contributes to successful phishing attacks and other types of cyber-attacks.

The use of outdated systems and technologies poses a substantial risk to law firms, hampering their ability to effectively protect confidential information and ensure reliable operation. The main risks associated with the use of old software and hardware include security vulnerabilities, compatibility, and integration, lack of support, increased operating costs, legal and compliance issues, performance issues, and an increased risk of data leakage. Older software often does not receive updates and patches that fix known vulnerabilities. This makes systems more susceptible to cyber-attacks such as viruses, trojans, and ransomware. Hackers actively use known vulnerabilities in old software to access protected data, which can lead to leaks of confidential information and disruption of the company's work. Outdated software may also have compatibility issues with modern systems and technologies, which makes it difficult to integrate with new applications and tools. This can lead to reduced work efficiency, problems with data exchange, and increased time to complete tasks. In the legal field, where accuracy and promptness are critical, this can cause delays and errors. In addition, software and hardware manufacturers often stop supporting older versions, which means there is a lack of technical assistance and updates. Without support, firms may encounter problems in maintenance and error correction, which may affect the stability of systems and increase the risk of data loss. Older hardware and software require more time and resources for maintenance and support, which can lead to increased operating costs. Frequent breakdowns and failures of old equipment can lead to additional repair and replacement costs.

The use of outdated technologies may also lead to non-compliance with legal requirements and safety standards. In legal practice, compliance with data protection norms and standards is mandatory, and non-compliance can lead to fines and legal sanctions. For example, non-compliance with the General Data Protection Regulation (GDPR) or other data protection laws can have serious legal and financial consequences for the company. Older software and hardware may have poor performance, which slows down workflows. In law firms that require processing large amounts of data and complex documents, this can reduce overall work efficiency and lead to delays in providing services to clients, which negatively affects the reputation of the firm. In addition, outdated software may not have modern data protection features, which increases the risk of leaks and hacks. Without modern encryption and security methods, information can become vulnerable to malicious attacks.

The integration of AI and machine learning into cybersecurity represents a promising direction for substantially improving threat protection and cyber risk management. AI and ML offer new approaches to threat detection, process automation and analysis of large amounts of data, which substantially increases the efficiency and speed of response to cyber threats. AI and ML are able to

substantially improve threat detection by using algorithms that can analyse and interpret large amounts of data in real-time. Modern security systems equipped with AI can detect anomalies and suspicious activities that may indicate potential cyber-attacks. Such systems use behaviour analysis techniques to build profiles of normal activity and detect abnormalities that may indicate intrusions. AI-based solutions can identify new types of threats and attacks that were not previously known, thereby providing proactive protection. Process automation is another important area of AI and ML application in cybersecurity (Teichmann & Boticiu, 2024). Many traditional processes, such as network monitoring, incident response, and threat management, require substantial human resources and time. AI and ML allow automating these processes, which reduces the likelihood of human error and increases the speed of response to incidents. For example, automated systems can independently block suspicious activity, isolate affected systems, and run recovery scenarios without requiring human intervention.

Analysing large amounts of data is a key task in cybersecurity, as modern networks generate a huge amount of information. AI and ML can efficiently process and analyse these data, identifying patterns and trends that may not be visible in traditional analysis. This allows organisations to identify potential threats faster, assess their risk level, and make informed decisions about protection measures. In addition, AI and ML help in incident management and threat response by improving post-attack investigation and analysis processes. Machine learning can analyse previous incidents and identify common features and techniques used by attackers, which helps in creating more effective protection strategies (Teichmann & Wittmann, 2023). However, the integration of AI and ML into cybersecurity also poses certain challenges. The need to train models on high-quality data, managing false positives, and ensuring data confidentiality are key aspects that require attention. In addition, attackers can also use AI to develop more sophisticated attacks, which requires constant updating and adaptation of defence mechanisms.

With the development of encryption technologies, law firms are gaining new opportunities to protect confidential information. Modern encryption methods such as asymmetric encryption and quantum encryption offer a high level of security for data that is transmitted or stored digitally. Asymmetric encryption uses two keys – one for encryption, the other for decryption – which makes it more resistant to hacking compared to traditional symmetric methods. This is especially important for legal organisations that process sensitive information such as customer personal data, commercial contracts, and legal documents. Quantum encryption, which is at the forefront of technology, promises an even higher level of security based on the principles of quantum mechanics, which virtually eliminates the possibility of unauthorised access to data. With the

development of digital technologies, the legal field is undergoing substantial changes, which has led to a sharp increase in the volume of electronic data. Law firms are now actively using digital tools to create, store, and process documents. These data include confidential customer information, legal documents, evidence, business correspondence, contracts, and other important files. In most cases, they have a high degree of sensitivity and may include financial information, personal data, intellectual property, and strategic business plans. The loss or compromise of such data can lead to serious legal consequences, including loss of customer trust and lawsuits.

Law firms are increasingly implementing modern security technologies such as encryption, MFA, and biometric systems to effectively protect these data. Each of these technologies has its own advantages in improving safety and reducing risks. Table 1 shows a comparison of the risk level before and after the introduction of these technologies, their application in legal practice:

Technology	**Risk level before implementation**	**Risk level after implementation**	**An example of a real threat**	**Effects**	**Illegal use of accounts**
Asymmetric encryption	High	Low	Interception of data during transmission	Leakage of confidential information	Encryption of e-mail and documents
Quantum encryption	Medium	Very low	Hacking using powerful computers	Loss of key data	A promising direction for mission-critical data
MFA	High	Low	Password theft	Unauthorised access to systems	Access to client data management systems
Biometric systems	Medium	Low	Forgery or theft of biometric data	Illegal use of accounts	Employee authentication for access to confidential information

Table 1 – The impact of modern security technologies on the level of cyber risks in law firms

Source: compiled by the authors.

These technologies allow law firms to substantially increase the level of security of their data. Asymmetric encryption, for example, substantially reduces the risk of data leaks, and multi-factor authentication makes it difficult for unauthorised access to systems. Biometric systems, in turn, provide an additional level of protection by restricting access to confidential information only to authorised employees.

Law firms are increasingly faced with the need to use specialised software that can not only optimise their work but also provide a high level of data security. The development of such software focused on the legal field opens up new opportunities to improve the efficiency and protection of information, which is especially important in conditions of strict legal requirements. Specialised software for the legal field may include the functions of case management, electronic document management, automation of document creation and processing, and ensuring secure communication with clients and partners. One of the key tasks of such software is to ensure compliance with data protection legislation, such as GDPR in Europe or HIPAA in the USA. This is achieved by integrating advanced encryption technologies, multi-factor authentication, and other cybersecurity techniques.

In addition, software development for law firms should consider the specific requirements related to the storage and processing of confidential information. For example, document management systems should ensure reliable storage and encryption of data, and the ability to quickly access them if necessary. It is also important to provide functions for automatic auditing and tracking of user actions to ensure transparency and control over the use of data. Another important feature is integration with other systems and services, such as judicial databases, state registries, and electronic reporting systems. This will allow lawyers to work effectively with external sources of information and get access to the necessary data faster. Specialised software can also include tools for analysing big data, which will allow lawyers to more effectively identify patterns, predict case outcomes, and develop more informed legal strategies. In the context of globalisation and the development of digital technologies, cyber threats are becoming increasingly international. For the legal field, which deals with the protection of confidential information and compliance with legislation, international cooperation and standardisation play a critical role in ensuring reliable cyber protection. International standards such as ISO/IEC 27001 (international standard to manage information security) and GDPR set uniform data protection requirements that are applied in different countries. Compliance with these standards allows law firms not only to comply with the requirements of local legislation but also to ensure a high level of security when working with international clients and partners. The standards also help to unify approaches to data protection, which simplifies interaction between law firms in different countries.

International agreements, such as the Budapest Convention on Cybercrime (Council of Europe, 2024), also play an important role in strengthening cyber defence. These agreements facilitate the exchange of information on cyber threats and crimes between countries, which allows responding more quickly to incidents

and preventing their recurrence. Law firms operating internationally can use such mechanisms to protect their interests and those of their clients and participate in global initiatives to counter cybercrime. In addition, international cooperation contributes to the development of new technologies and methods of protection. Joint research conducted within the framework of international consortia allows developing more effective solutions to combat cyber threats. This is especially important for the legal field, where data protection is a priority.

DISCUSSION

Digitalisation has had a substantial impact on the legal field, transforming data management, and document management processes. Electronic documents have improved access to information, accelerated workflows, reduced paper and storage costs, and simplified collaboration and remote interaction. However, as the analysis showed, the transition to electronic document management is associated with risks such as vulnerability to cyber-attacks, the need for investments in data protection and dependence on technology. An important aspect also remains the recognition of electronic documents at the same level with paper documents in various jurisdictions, which creates obstacles in international affairs. Virtual consultations certainly provide many benefits for both lawyers and clients. They can substantially reduce time and financial costs, facilitate access to legal services and provide more flexible interaction, regardless of the geographical location of the participants. This is especially true in the context of globalisation and the spread of remote work when the ability to provide legal services via the Internet becomes an integral part of business.

Susskind (2023) emphasises that technological changes are transforming the legal profession, especially in terms of cost optimisation and increasing the availability of legal aid. These aspects coincide with the results of this study, according to which virtual consultations can substantially reduce costs and provide an opportunity for a wider range of clients to access legal services, which is especially important in conditions of financial or geographical constraints. However, despite these positive results, serious cyber threats related to virtual consultations have been identified. Confidential data such as trade secrets or personal information are often discussed during consultations, which makes law firms and their clients vulnerable to cyber-attacks. The risks of data leakage or unauthorised access to information remain high, which, in turn, may entail legal and financial consequences. The results demonstrate that cyber threats related to virtual consultations require serious data protection measures, such as encryption of communications and the introduction of multi-factor authentication. These conclusions echo the study of Rossner and Tait (2023), who considered the advantages of virtual courts and consultations. He concluded that such formats

make justice more accessible by allowing participants in trials to participate regardless of their location. Indeed, virtual consultations allow participants to interact without the need for physical presence, which is especially important in international affairs. However, it was stressed that along with the increase in accessibility, the likelihood of cyber threats is also increasing.

The study focuses on the critical need to protect the confidential information of clients in the legal field. The main challenges are cyber-attacks such as phishing, ransomware, and DDoS attacks that threaten the integrity of data and the normal functioning of law firms (Spytska, 2024). For example, attacks on government agencies in Albania, and data leaks in Kyrgyzstan and Azerbaijan illustrate the vulnerability of data when protection is insufficient. This highlights the need to develop cyber defence strategies and enhanced data security controls. Phishing is a deceptive attempt to gain access to personal information through fake emails or websites (Tkachenko et al., 2024). If employees are not aware of the protection methods, this can lead to data leakage, disruption of the company's work and financial losses (Bocheliuk et al., 2019). The solution to the problem involves regular employee training and the use of multi-level authentication. Ransomware encrypts data and demands a ransom for decrypting it. An attack of this type can paralyse the company's work, depriving it of access to important documents. This leads to financial losses and deprivation of customer trust. Regular data backups and a recovery plan after an attack are important to protect against ransomware (Iklassova et al., 2024). DDoS attacks overload the company's network resources, causing disruptions to websites and online services. This may interrupt the provision of legal services, which will negatively affect the reputation of the company. Protection against such attacks includes the use of specialised services and software to prevent overloading of systems. Law firms need to integrate comprehensive cybersecurity measures, including employee training and modern security technologies to effectively protect data (Nechyporenko et al., 2019). This will help prevent data leaks and preserve the company's reputation.

The results of the study confirm the conclusions made by Rajabova (2024), on the need for strict data protection measures, especially in the context of real estate transactions. This coincides with the main findings of the current study, which highlights the importance of encryption and multi-factor authentication to prevent information leaks. In particular, the introduction of such technologies can substantially reduce the risks associated with the leakage of confidential data. Sohal and Gupta (2020) raise an important question about the advantages of cloud platforms for data management but also points to increased risks of cyber threats. This is reflected in the results of the study, which indicate the need for a balanced approach to the use of cloud technologies, considering potential vulnerabilities.

Law firms using cloud solutions should be aware of the risks and take appropriate protective measures. The study determined that modern encryption technologies, such as asymmetric and quantum encryption, play a vital role in ensuring the security of data transmitted and stored in digital format. Asymmetric encryption using a key pair (public and private) provides a high level of protection, enabling the encryption of data and its transfer without the risk of interception (Vilks et al., 2024). This method is especially effective for protecting the confidential information of legal documents and the personal data of clients. The conclusions are supported by data demonstrating a substantial reduction in information leaks in law firms where modern encryption technologies are implemented.

The data of the results correspond to the study by Corne (2020), who emphasises the importance of using encryption to protect confidential information, pointing out that encryption is one of the central elements for ensuring data security. These conclusions coincide with the results of the study, confirming the need to introduce these technologies into legal practice. However, it is noted that the use of asymmetric encryption can be difficult for small and medium-sized enterprises due to the high cost of implementation and the need for regular updating of the technical infrastructure. This conclusion is consistent with the study by Gonzalez (2017), who examines existing legal approaches to encryption and identifies shortcomings in current laws and regulations that prevent the adaptation of encryption technologies for small law firms. It was also noted that legal support for the implementation of these technologies is insufficient, which leads to incompatibility between modern security standards and the actual possibilities of their implementation. This aspect was also identified in the course of this study, especially when analysing the problems faced by small law firms in the process of compliance with regulatory requirements and safety standards. The study established that international cooperation and the implementation of standards such as ISO/IEC 27001 and the GDPR are key factors for increasing the level of cybersecurity of law firms. The application of ISO/IEC 27001 contributes to the improvement of the information security management system and helps legal organisations establish clear data protection processes and policies, ensuring compliance with international requirements and best practices.

The results of the study by Ramadhan and Rose (2022) stress the difficulties of adapting the ISO/IEC 27001 standard for small and medium-sized legal entities. This coincides with the findings of the current study, which also showed that small firms often face a lack of resources to effectively implement this standard. Limited financial and human resources can hinder the implementation of comprehensive cyber defence measures, which makes them vulnerable to cyber-attacks. An analysis by Lopes et al. (2019) confirms that ISO

27001 standards can facilitate compliance with GDPR requirements. The current study also determined that law firms that have implemented ISO 27001 do a better job of meeting GDPR requirements, which reduces the risks of non-compliance and potential legal consequences. Nevertheless, differences have been identified that require additional attention. While Lopes et al. focuses on the relationship between ISO 27001 and GDPR standards, the study shows that law firms outside the EU face challenges adapting these standards to diverse jurisdictions. This highlights the need for further global harmonisation of cybersecurity standards. Thus, the findings of the current study confirm the importance of international standards for improving cybersecurity but also indicate the need for a more flexible approach to their implementation in various legal contexts.

CONCLUSIONS

The study established that the transition to electronic documents and digital tools has substantially increased the efficiency of law firms. Electronic documents simplify access, search, and exchange of information, reducing the cost of paper, printing, and storage. Despite the advantages, the transition to electronic documents is fraught with risks, such as the threat of cyber-attacks, dependence on technology, and legal difficulties in various jurisdictions. Cyber threats require substantial investments in data protection, and dependence on technology can lead to temporary paralysis of operations in the event of technical failures. It is also necessary to train employees in new technologies, which can be problematic for those who are used to traditional working methods.

The study highlighted those virtual legal consultations provide a convenient way to get help, reducing time and resources. However, they are also subject to risks such as the threat of data leakage and problems adapting to new technologies. The lack of personal contact can make it difficult to establish trusting relationships, which is important in sensitive cases. Law firms face serious cyber threats such as phishing, ransomware, and DDoS attacks. These attacks can cause confidential information leaks, disruptions, and loss of reputation. Examples of incidents in different countries confirm the need for effective cyber defence measures and rapid response to threats.

International standards such as ISO/IEC 27001 and GDPR help to harmonise approaches to data protection and simplify work with international clients and partners. International agreements, such as the Convention on Cybercrime, facilitate the exchange of information about cyber threats and accelerate the response to incidents. The integration of AI and ML into cybersecurity offers new approaches to threat detection, process automation, and big data analysis. However, this requires high-quality model training, false alarm management, and data protection.

The study is limited in the fact that it focuses on existing data protection methods and technologies in the legal field, which may not consider new threats and technologies, and also does not cover all legal systems and practices in different countries, which reduces the universality of its conclusions and recommendations. Further research in this area may include the study of new cyber threats and data protection technologies and the development of adaptive incident response methods.

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

Abdalla Abdelkarim, Y. (2024). Introduction to cyber jurisprudence. *SSRN, 8*. https://dx.doi.org/10.2139/ssrn.4929165

Adonis, A. A. (2020). International law on cyber security in the age of digital sovereignty. *E-International Relations, 5*, 1-5.

Amelin, O. Yu., Kyrychenko, T. M., Leonov, B. D., Shablystyi, V. V., & Chenshova, N. V. (2021). Cyberbullying as a way of causing suicide in the digital age. *Journal of the National Academy of Legal Sciences of Ukraine, 28*(3), 277-289. https://doi.org/10.37635/jnalsu.28(3).2021.277-289

Bakhramova, M., Ekaterina, K., Khazratkulov, O., & Rustam, R. (2023). Legal services 4.0: Digital transformation for increased fairness and efficiency. *International Journal of Cyber Law, 1*(4), 111-116. https://doi.org/10.59022/ijcl.48

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/

Corne, T. C. (2020). Legal protection of privacy data through encryption technology. *Lampung Journal of International Law*, *1*(2), 63-70. https://doi.org/10.25041/lajil.v1i2.2027

Council of Europe. (2024). Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention

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. https://doi.org/10.1080/08874417.2023.2248921

General Data Protection Regulation. (2024). https://gdpr-info.eu/

Ginters, E., Aizstrauts, A., & Chinea, R. M. A. (2014). Sociotechnical aspects of policy simulation. In: *Handbook of Research on Advanced ICT Integration for Governance and Policy Modeling* (pp. 113-128). Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-6236-0.ch007

Gonzalez, O. (2017). Cracks in the armor: Legal approaches to encryption. *Journal Of Law, Technology & Policy, 2019*(1), 1-48.

Gupta, B. B., Dahiya, A., Upneja, C., Garg, A., & Choudhary, R. (2020). A comprehensive survey on DDoS attacks and recent defense mechanisms. In: B. B. Gupta, S. Srinivasagopalan (Eds.), *Handbook of Research on Intrusion Detection Systems* (pp. 186-218). Hershey: IGI Global. https://doi.org/10.4018/978-1-7998-2242-4.ch010

Haciyeva, A. (2021). Personal data, their protection and legislation of the republic of Azerbaijan and the European union in this area. *Law of Ukraine*, 12, 251-262.

Iklassova, K., Aitymova, A., Kopnova, O., Shaporeva, A., Abildinova, G., Nurbekova, Z., Almagambetova, L., Gorokhov, A., & Aitymov, Z. (2024). Ontology modeling for automation of questionnaire data processing. *Eastern-European Journal of Enterprise Technologies, 5*(2-131), 36-52. https://doi.org/10.15587/1729-4061.2024.314129

Islam, M. T., & Huda, N. (2019). Material flow analysis (MFA) as a strategic tool in E-waste management: Applications, trends and future directions. *Journal of Environmental Management*, *244*, 344-361. https://doi.org/10.1016/j.jenvman.2019.05.062

Karovska Andonovska, B., & Taneski, N. (2020). Legal aspects of security in cyberspace. *Security Dialogues, 11*(1), 99-110.

Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry, 15*(10), 1958. https://doi.org/10.3390/sym15101958

Khomyshyn, I., Ortynska, N., Skochylias-Pavliv, O., Andrusiak, I., & Rym, O. (2022). The main systemic engineering problems of using computer and digital technologies in legal activities in the context of ensuring security.

International Journal of Safety and Security Engineering, 12(5), 597-602. https://doi.org/10.18280/ijsse.120507

Larry, C. (2021). Massive data leaks in Albania highlight national cybersecurity shortcomings. https://theowp.org/massive-data-leaks-in-albania-highlight-national-cybersecurity-shortcomings/

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering & Management, 4*(2), em0089. https://doi.org/10.29333/jisem/5888

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. https://doi.org/10.34069/AI/2023.70.10.11

Nechyporenko, V. V., Bocheliuk, V. I., Pozdniakova-Kyrbiatieva, E. G., Pozdniakova, O. L., & Panov, N. S. (2019). Value foundation of the behavior of managers of different administrative levels: Comparative analysis. *Espacios*, *40*(34), 17. https://www.revistaespacios.com/a19v40n34/19403417.html

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. https://doi.org/10.1515/pdtc-2024-0017

Ofori, A. Y., & Akoto, D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*, 045. https://doi.org/10.24966/flis-733x/100045

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128. https://doi.org/10.1108/JGOSS-05-2019-0042

Pyrohovska, V., Rezvorovych, K., Pavlichenko, I., Sushytska, Y., & Ostashova, V. (2024). Human rights protection in the context of information technology development: Problems and future prospects. *Futurity Economics & Law*, *4*(1), 38-51. https://doi.org/10.57125/FEL.2024.03.25.03

Rajabova, A. (2024). Navigating legal data privacy risks in real estate transactions: Safeguarding client data through robust data protection measures. *Web of Semantics: Journal of Interdisciplinary Science*, *2*(7), 154-162.

Ramadhan, N., & Rose, U. (2022). *Adapting ISO/IEC 27001 information security management standard to SMEs.* Luleå: Luleå University of Technology.

Rossner, M., & Tait, D. (2023). Presence and participation in a virtual court. *Criminology & Criminal Justice, 23*(1), 135-157. https://doi.org/10.1177/17488958211017372

Sidorenko, E. L., & von Arx, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. *Digital Law Journal*, *1*(1), 24-28. https://doi.org/10.38044/DLJ-2020-1-1-24-38

Sinha, A. R., Singla, K., & Victor, T. M. M. (2023). Artificial intelligence and machine learning for cybersecurity applications and challenges. In: R. Kumar, P. K. Pattnaik (Eds.), *Risk Detection and Cyber Security for the Success of Contemporary Computing* (pp. 109-146). Hershey: IGI Global. https://doi.org/10.4018/978-1-6684-9317-5.ch007

Sohal, K. S., & Gupta, A. (2020). Cloud computing technology and its adoption in law firms. *Amity Journal of Energy & Environment Studies, 6*(1), 14-19.

Spytska, L. (2024). Practice-based methods of bringing to legal liability for anonymous defamation on the Internet and in the media. *Social and Legal Studios, 7*(1), 202-209. https://doi.org/10.32518/sals1.2024.202

Sultanbayeva, G. S., Turdubaeva, E. O., Lozhnikova, O. P., & Tastemirova, G. A. (2023). Developing a platform for cross-border investigative journalism in Central Asia. *Herald of Journalism, 68*(2), 72-81. https://doi.org/10.26577/HJ.2023.v68.i2.07

Susskind, R. (2023). *Tomorrow's lawyers: An introduction to your future.* Oxford: Oxford University Press.

Talesh, S. A., & Cunningham, B. (2021). The technologization of insurance: An empirical analysis of big data an artificial intelligence's impact on cybersecurity and privacy. *Utah Law Review, 2021*(5)*,* 967-1027. https://doi.org/10.26054/0d-9y6k-1t55

Teichmann, F. M., & Boticiu, S. R. (2024). Phishing attacks: Risks and challenges for law firms. *International Cybersecurity Law Review, 5*, 615–622. https://doi.org/10.1365/s43439-024-00110-8

Teichmann, F. M., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime, 30*(6), 1491-1498. https://doi.org/10.1108/JFC-04-2022-0093

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. https://doi.org/10.1002/cav.70003

Veasey, E. N. (2019). Protection of client confidential information from cyberattacks is a compelling business and ethical priority for inside and outside corporate counsel. *Business Lawyer, 75*(1), 1495-1518.

Vilks, A., Kipane, A., & Krivins, A. (2024). Preventing international threats in the context of improving the legal framework for national and regional security. *Social and Legal Studios, 7*(1), 97-105. https://doi.org/10.32518/sals1.2024.97

Widespread cyberattack blocks government and public websites in Albania. (2022). https://www.euronews.com/2022/07/18/widespread-cyberattack-blocks-government-and-public-websites-in-albania

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