Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference .2025. Volume V, 141-148

Security in Legal Education: Challenges and Solutions in the Modern World

Inga Kudeikina
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
inga.kudeikina@rsu.lv

Sandra Kaija
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
sandra.kaija@rsu.lv

Ivans Jānis Mihailovs
Faculty of Social Sciences
Riga Stradiņš University
Latvian Academy of Culture
Riga, Latvia
ivans.mihailovs@rsu.lv

Lidija Juļa
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
lidija.jula@rsu.lv

Vitālijs Rakstiņš
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
vitalijs.rakstins@rsu.lv

***Abstract*—Legal education is an essential foundation for the sustainability and development of society, ensuring democracy and security by preparing future lawyers, including judges. In an era of rapid digitalization, security issues in legal education are becoming increasingly relevant. Problems such as access to confidential documents, insufficient knowledge of digital security risks, and the lack of protection mechanisms pose significant threats to students, faculty, and lawyers. Addressing these issues is essential to maintain trust in the legal system and ensure the integrity of legal education. The aim of this study is to analyze security aspects in legal education, focusing on the need to improve students' understanding of legal and practical security issues. The study explores how cybersecurity training can be integrated into legal education so that future lawyers acquire the necessary skills to responsibly handle sensitive information in a secure digital environment. The study uses a qualitative research approach that includes a review of the legal framework, academic literature and case studies on cybersecurity challenges in legal education. Comparative analysis is used to examine best practices across jurisdictions regarding security measures in legal studies. In addition, expert opinions from legal professionals and educators are taken into account to assess the effectiveness of current approaches and identify areas for improvement. The results highlight the need to integrate cybersecurity courses into legal education curricula and improve regulatory frameworks to address digital security risks. A more comprehensive approach to legal education that includes practical cybersecurity training would improve students' ability to navigate ethical and professional challenges in the digital age. Implementing these measures would not only reduce cybersecurity risks but would also better prepare law students for their professional responsibilities by ensuring their competence in protecting sensitive legal information.**

Keywords - cybersecurity, data protection, legal education.

I. Introduction

Legal education is an essential foundation for the sustainability and development of society, ensuring democracy, security, and the rule of law, as it prepares future lawyers, including judges, security institution employees, and other legal specialists [1], [2]. According to the explanation given in the National Encyclopedia, legal education is a set of systematized knowledge in legal sciences; the system of acquiring this knowledge in educational institutions, the process of legal education, the theory, practice, and didactics of teaching legal sciences, legal education, as well as continuous professional development [3]. Therefore, in addition to academic challenges, it is important to pay attention to security aspects that affect students, teaching staff, and practicing lawyers (also in accordance with the Latvian Cybersecurity Strategy for 2023–2026 [4]). In today's rapidly changing world, where information and communication play a significant role, security issues in legal education are becoming increasingly relevant. For example, access to confidential documents, insufficient knowledge of digital security risks, and a lack of protection mechanisms create significant problems that can threaten the security of both students and institutions. Higher education institutions should pay increasing attention to these issues by improving studies and integrating relevant study courses into the study process [5], [6]. Also, the use of AI in education offers unique opportunities in legal education. AI

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8472

systems, with their vast databases and analytical capabilities, can present students with complex problems and scenarios that require more than just rote memorization or basic understanding. These systems can challenge students to use higher-order thinking skills, such as analysis, synthesis, and evaluation, to navigate through these problems [7], [8]. To ensure the effective implementation of AI, cybersecurity policies, legal education must include specialized knowledge of cybersecurity laws and their practical application [9]. Another important concern is the readiness of students to work with digital legal resources and their ability to mitigate potential security risks associated with using online databases and other digital tools [5]. This article will analyze certain security aspects in legal education that affect the improvement of the study process, ensuring that future lawyers develop an understanding of the legal and practical aspects of security during their studies and acquire the necessary cybersecurity skills and abilities to work with sensitive information in a secure digital environment.

II. Materials and Methods

The purpose of this work is to analyze cybersecurity problems in legal education and offer effective solutions for the protection of confidentiality and sensitive data to improve students' readiness to work with digital legal resources and prevent possible security risks. To achieve this goal, the study will employ the analysis of legal acts and legal doctrine, including academic research and expert opinions on security issues in the education of future legal professionals.

III. Results and Discussion

A. The Importance of Legal Education in Public Safety and Sustainable Development

Legal education is one of the cornerstones of sustainable development and security of society, ensuring that members of society understand their rights and obligations, promoting the rule of law, and strengthening state power. When evaluating the importance of legal education in the context of state power functions, in Latvia, the Ministry of Justice, namely the executive branch, is responsible for the state unified lawyer exam, which is presumed to be one of the guarantees of legal education quality. In carrying out its duty, the executive branch also ensures the functioning of the judiciary. Although the existence of legal education provides opportunities to work in various professions and offers broad career opportunities, the requirement to obtain higher education and professional qualification as a lawyer is mandatory for persons in the judicial system – judges, prosecutors, sworn advocates, sworn notaries, and sworn bailiffs. In the judicial system, where justice is administered and important decisions are made that affect people's lives, there are strict requirements regarding professional training, ensuring both competence and responsibility in performing assigned duties. This requirement not only guarantees that the judicial system will function effectively but also strengthens public trust in the rule of law and its institutions, since only qualified persons can ensure objective and fair judicial work. This is especially important in the context of the separation of powers, as only qualified and independent lawyers can ensure that judicial decisions are made objectively, in compliance with all legal principles, and are effectively executed, which, in turn, promotes public trust in the rule of law. In connection with these important aspects, especially regarding judges as guarantors of the right to a fair trial, it has been rightly stated in the scientific literature that public trust in the judicial system as the basis of public welfare depends on judges [10].

Legal education is an essential basis for obtaining a position in the judicial system, as it provides the necessary knowledge, skills and competences that are important for fulfilling a responsible position in the judicial system. The work of these persons is related to the interpretation and application of laws in specific cases, as well as to observing justice and the rule of law, which requires both theoretical knowledge and practical skills. However, legal education is an important, but not the only prerequisite for obtaining, for example, the position of a judge. It is the first step towards professional activity in the judicial system. The state imposes a number of requirements on applicants for the position of a judge, namely, it determines not only the education requirement, but also, for example, the citizenship, age, professional experience requirement.

Historically, judges could be “just a decent person” (without any educational qualifications). Historical sources indicate that the situation in Europe changed in the 18th century, when professionals, educated lawyers, became judges, one of the reasons being that legal norms were codified [11]. In addition, previously, work in the relevant field had to start from office and then, while already working, one had to study the relevant norms. However, today, the legislator has provided for the possibility of immediately becoming a judge of a regional court or the Supreme Court with education and professional experience, theoretically without working a single day in the judicial system. Currently, the educational qualification plays a significant role in the work of a judge. First of all, so that a person, upon becoming a judge, can immediately begin to perform the duties of a judge, and also to judge qualitatively. You, so that a judge can constantly improve his or her qualifications. Here it is necessary to recall what was mentioned at the beginning of the chapter, that legal education is also the improvement of qualifications / professional competence. Continuous improvement of qualifications is an essential component of any profession. It is also essential in the selection of candidates for the position of judge. Because not only the formal criteria – the presence/absence of higher education and professional qualifications as a lawyer, as well as the existence of a master's or doctoral degree – are important, but also the ability and competence to improve one's qualifications.

Here it can be argued: if ensuring the training of appropriately qualified lawyers is the task of the executive branch, then the task of the judicial system itself is to create a supportive, development-oriented environment in which each judge could improve their skills and qualifications.

The quality of legal education directly affects the competence not only of judges, but also of lawyers, prosecutors and other judicial system employees, which in turn

determines how effectively rights and justice are ensured in society.

Despite acquiring theoretical knowledge, legal education graduates face difficulties in applying practical skills. Legal study programs often do not sufficiently emphasize the development of critical thinking problem-solving and practical skills, which are essential for effective legal practice and ensuring public safety.

Critical thinking plays a vital role in legal education. The scientific literature indicates that applied to law, critical thinking is the ability: 1) to evaluate a legally relevant object from a specific legal-doctrinal, legal-empirical or legal-theoretical normative framework, using relevant (legal and other) sources of information; 2) A legally relevant object can be: a) the existing law (legislation, court decisions, treaties and so on), b) the legal and political system (including, for instance, the legislature, the administration and the judiciary), c) current legal opinions or theories about the law and the legal and political system (such as legal positivism or ELS) or d) actions from legal and political authorities (such as the police) or citizens; 3) to express one's own opinion about it which deviates from the mainstream understanding; 4) and to substantiate this opinion with good arguments based on standards derived from this specific framework [12].

For example, on 7 November 2019, the Constitutional Court adopted a judgment in case No. 2018-25-01, which assessed the compliance of Article 50.4 of the Latvian Penal Code with Article 91 of the Constitution. This article established different regimes for serving sentences for men and women serving sentences of deprivation of liberty in a closed prison. The Constitutional Court concluded that such a difference was not objectively and reasonably justified, thus violating the principle of equality enshrined in Article 91 of the Constitution. Consequently, the Constitutional Court found this legal regulation to be inconsistent with Article 91 of the Constitution. [13].

When analyzing this judgment, the following methodology can be used: 1) The judgment is assessed considering Article 91 of the Constitution, which establishes the principle of equality – "all persons are equal before the law". This principle is essential to ensure that discriminatory differences are not created in the application and results of national legal acts based on unnecessary criteria, such as gender. The judgment of the Court also analyzes the Latvian Penal Code, which establishes different sentencing regimes for men and women. The Court recognizes that such regulation, which establishes discrimination based on gender, is contrary to Article 91 of the Constitution, because gender differences are not objectively and reasonably justified. Thus, within the framework of the legal analysis, it is recognized that it is not justified by the principle of non-discrimination and balanced legal values. 2) The object of the judgment is the existing law – the Latvian Penal Code – which regulates sentencing regimes. The task of the court was to assess the compliance of this regulatory act with Article 91 of the Constitution, considering that the right to equality is one of the pillars of fundamental rights. The court's conclusion on the need to prevent gender discrimination in the service of punishment is based on the interpretation of this norm. 3) In this case, the court takes a critical attitude towards the norms of the law that considered gender differences to be justified, indicating that the regulatory framework must be changed. The court indicates that gender differences cannot be justified by the need to create different conditions in prisons, and considers them to be unfounded and unnecessary, since it directly violates the individual's right to equality. 4) The court rightly indicates that gender discrimination in the regime of execution of punishment is contrary to the principles of the Constitution. The argumentation is based on the fundamental principles of the legal system, namely, the principles of equality, justice and respect for human rights. The court implemented a critical thinking approach to social justice and the prevention of discrimination, which allowed it to identify an unnecessary gender difference in the regulation.

This judgment is an example of how a court is able to express an independent and critical opinion, assessing the inequality of existing norms and proposing changes that have a beneficial effect on human rights and the rule of law in the state.

The aim of legal education is not only to provide theoretical knowledge of legal norms, but also to develop the ability to critically analyze and understand laws and the practice of their application. Critical thinking skills are an essential element in legal education, as they allow students not only to understand and master the laws, but also to analyze, evaluate and challenge the existing legal framework and make legal decisions that are objective and justified. A lawyer with high critical thinking skills is able to ask important questions about the existing legal system and its effectiveness.

Critical thinking encourages the search for alternative approaches to specific problems and issues. It is not limited to the application of existing laws, but also allows students to seek new, innovative methods of solving legal problems or interpreting laws, which is necessary, for example, in legal research or case law.

We must not forget about artificial intelligence either. The use of AI in education offers unique opportunities to cultivate critical thinking. AI systems, with their vast databases and analytical capabilities, can present students with complex problems and scenarios that require more than just rote memorization or basic understanding. These systems can challenge students to use higher-order thinking skills, such as analysis, synthesis, and evaluation, to navigate through these problems [8].

In addition, critical thinking helps to create a responsible attitude towards the use and application of law, promotes the development of legal culture, which undoubtedly strengthens public safety.

Critical thinking skills are also vital in cybersecurity to evaluate technologies, address security challenges, and make informed and long-term decisions about organizational security. It helps to measure risks, predict potential

threats, and respond effectively to cybersecurity incidents, while adhering to legal and ethical standards. Thus, critical thinking in cybersecurity becomes an important tool to ensure effective and sustainable protection against cyber threats.

The legal system is changing, and only those lawyers who are able to think critically can actively participate in its improvement, ensuring justice and efficiency. Thus, universities today must strive to provide students with the intellectual studies, critical thinking skills necessary for high-level leaders in a complex future society.

B. The role of legal education in strengthening cybersecurity and sustainable societal development

In today's digital age, legal education plays a crucial role not only in promoting public safety and sustainable development but also in strengthening cybersecurity. An effective legal education ensures that future and current lawyers, judges, and other legal professionals are well-versed in existing regulatory frameworks and policy planning documents while also being equipped to address new challenges posed by rapid technological advancements.

One of the key issues is how legal education can prepare specialists to effectively prevent cyber threats and respond to cybersecurity incidents. How can we ensure that lawyers are not only familiar with legal regulations but also capable of applying this knowledge in practice by developing and implementing effective security measures? [9]. Another critical concern is the readiness of students to work with digital legal resources and their ability to mitigate potential security risks associated with using online databases and other digital tools [5].

Cybersecurity legislation and policy documents establish the legal framework necessary to protect critical infrastructure, personal data, and other sensitive information. The European Union's Directive on security of network and information systems (NIS Directive) [14] and the General Data Protection Regulation (GDPR) are prime examples of the growing importance of cybersecurity legislation.

To ensure the effective implementation of cybersecurity policies, legal education must include specialized knowledge of cybersecurity laws and their practical application. Lawyers specializing in cybersecurity can make a significant impact in both the public and private sectors, helping to create a secure and well-regulated digital environment [15].

C. Cybersecurity in education: challenges and solutions

Cybersecurity has become one of the most critical areas affecting all aspects of life, including education. Higher education institutions increasingly rely on e-learning platforms, which, while offering flexibility and accessibility, also introduce new risks related to the security of sensitive data and academic content. The main threats include unauthorized access to study materials, personal data leaks, and ransomware attacks, all of which can disrupt academic processes and have serious consequences for both students and faculty.

Recognizing these challenges, Regulation 2021/887 of the European Parliament and of the Council, adopted on 21 May 2021, established the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC). The primary objective of the ECCC is to promote research, innovation, and implementation in the field of cybersecurity by supporting the European Union (EU) Cybersecurity Competence Community. This community consists of public authorities and private sector participants working together under the framework defined by the Regulation. In Latvia, the National Cybersecurity Center has been actively addressing cybersecurity risks in the education sector, particularly concerning the use of e-learning platforms and university study resources [15].

The academic environment has become an attractive target for cyber attackers. Various digital platforms used in the study process store both academic and personal data, making secure data management crucial to prevent breaches and unauthorized access. Data leaks can have severe consequences for students and educational institutions alike. For example, at the end of 2024, a significant data breach occurred in Latvia's Unified Local Government Information System, affecting residents of 42 municipalities (excluding Riga). The leaked data included names, surnames, personal identification numbers, declared addresses, and even metadata from municipal employee documents. This incident is considered the largest known data breach in Latvia [16].

Such security breaches pose significant risks, as the exposed information can be exploited for fraudulent activities, including phishing scams and identity theft. The scientific literature highlights that “academic institutions are particularly vulnerable to cyber threats due to their valuable intellectual property, sensitive personal data, and research data.” Cyberattacks targeting universities range from phishing schemes and ransomware attacks to sophisticated attempts to steal research data, ultimately threatening the integrity of research and financial stability [6].

Latvian universities are increasingly facing cyberattacks that involve both data leaks and damage to information systems. These incidents not only disrupt the learning process but also create dissatisfaction among students and faculty, undermining trust in digital education. The CERT.LV activity report for the third quarter of 2024 revealed a 267% increase in cyber threats, highlighting a surge in attacks on virtual environments. Analysis indicates that many of these attacks are politically and commercially motivated, with support from Russia and China, though the majority have been successfully neutralized [17]. This alarming trend underscores the urgent need for enhanced cybersecurity measures and effective cooperation between academic institutions and security experts to ensure a safe and stable learning environment.

The rapid advancement of artificial intelligence (AI) technologies presents new challenges in education. AI can be exploited to conduct automated phishing campaigns, generate fake academic resources, and simulate cyber threats, misleading students and faculty and endangering academic integrity. Additionally, deep fake technology

enables the creation of falsified video and audio materials, which could compromise the reputation of educational institutions or spread disinformation. Disinformation campaigns aim to destabilize academic institutions and erode public trust in the education system [6]. These emerging threats highlight the necessity of a comprehensive cybersecurity approach in education, combining technological solutions with the development of critical thinking skills.

Cybersecurity has gained increasing importance at the national level as security threats continue to evolve. To strengthen national cybersecurity, the Cabinet of Ministers approved the Latvian Cybersecurity Strategy for 2023–2026 on 14 March 2023. This strategy outlines key policy directions and identifies future threats, focusing not only on strengthening technological protection but also on fostering international cooperation and enhancing public awareness of cybersecurity issues. The education sector plays a crucial role in implementing cybersecurity policies and developing protection systems [4].

Latvia has been actively developing cybersecurity policies in the education sector, involving various organizations. The Ministry of Defence, in collaboration with CERT.LV, the University of Latvia, and the National Guard Cyber Defence Unit, annually organizes a cybersecurity challenge for young people to develop their knowledge and skills in this field [18]. Additionally, Riga Technical University (RTU) has launched a two-year cybersecurity education project aimed at preparing students and professionals for careers in cybersecurity [19]. Similarly, the professional master's study programme "Cybersecurity Engineering" at Vidzeme University of Applied Sciences provides in-depth knowledge and essential skills for security testers and other specialists in this field [20].

D. Cybersecurity risks in legal education

Modern legal education increasingly relies on digital technologies and information systems, particularly in distance learning and online assessments. However, this growing dependence on digital tools also exposes legal education to various cybersecurity risks, which can be categorized as follows:

1) Disruptions to the Study and Research Process Cyberattacks targeting the websites and databases of educational institutions, as well as online study and examination tools, can severely disrupt legal education. Unauthorized access or remote manipulation of information systems may lead to the complete suspension of distance learning, compromise the objectivity of assessments, or interfere with automated grading algorithms. Additionally, the uncontrolled advancement of disruptive technologies, particularly artificial intelligence solutions, heightens the risk of their malicious use [21].

2) Threats to Data Availability and Integrity Cyberattacks can compromise data availability—for instance, by encrypting critical data, rendering cloud-hosted information inaccessible, or even deleting data entirely [10]. Moreover, attackers can alter original files without authorization, undermining data integrity. Such risks pose significant challenges to the continuity of legal education.

3) Reputational and Confidentiality Risks Data breaches that expose sensitive information to unauthorized third parties can damage the reputation of educational institutions. These risks may involve data leaks, industrial cyber espionage, and intellectual property theft, all of which can have long-term consequences for both students and faculty.

4) Cybercrime Risks Security vulnerabilities in the digital environment also make legal education institutions potential targets for cyber fraud and other cybercrime activities [22].

While cybersecurity risks cannot be entirely eliminated, legal education institutions can implement a range of measures to ensure minimum cybersecurity standards, mitigate system vulnerabilities, and develop business continuity plans. However, there are currently no external regulations that require legal education institutions to adopt mandatory cybersecurity protection measures. It is also important to note that most cybersecurity measures do not require significant financial investments [23].

E. Regulatory acts and policy planning documents for strengthening cybersecurity in legal education

Technological developments and new risks, as well as several current geopolitical events, have contributed to the relatively rapid development of cybersecurity regulation, especially in the last five years. Political scientists Evija Djatkoviča and Māris Andžāns have published an overview of significant regulatory enactments and policy planning documents in this area until 2021 [24]. Therefore, this part of the article focuses on the most recent documents, as well as those aspects that affect legal education.

On 1 September 2024, the National Cybersecurity Law entered into force, defining cybersecurity in Article 1 as "activities that meet the definition set out in Article 2(1) of Regulation 2019/881" [25], i.e. "'cybersecurity' means activities that must be carried out to protect network and information systems, their users and other persons affected by cyber threats" [26].

The Latvian Cybersecurity Strategy for 2023-2026 envisages identifying the current training opportunities for cybersecurity specialists and identifying the needs of future cybersecurity specialist education programs, accordingly developing a plan for the training of cybersecurity specialists, starting from secondary vocational education to second-level higher education. The document also recognizes that "the introduction of professional standards, which need to be developed in accordance with existing international standards, is also essential", as well as promoting the rule of law in cyberspace and reducing cybercrime [4].

This directly resonates with the goal set out in the Digital Transformation Guidelines for 2021–2027: "A high level of digital security and trust in Latvia's digital space is ensured by the implementation of a modern cybersecurity policy, intensive use of reliable electronic identification

and other trust services, as well as effective protection of personal data and other rights in the digital environment," which actually requires every citizen to master various digital technologies and develop digital skills, because "the individual's opportunities to get educated, compete in the labor market, and fully participate in social processes depend on them" [27].

The provisions of these documents create the need to implement significant changes in education, including legal education, by improving studies and integrating relevant study courses into the study process in order to reduce the threat to both students themselves and various institutions, as well as develop the competence to identify and assess specific cyber problem cases.

It should be noted that critical thinking, safety and cybersecurity issues are already an essential part of the curriculum developed in the competency-based approach at the primary and secondary levels of education, as a cross-cutting skill in developing digital literacy - the learner effectively uses digital technologies for various purposes, analyzes the benefits and risks of digital communication, critically analyzes the reliability of information in the media; when creating their own content, they observe privacy, ethical and legal conditions; evaluate, adapt to their needs and follow healthy and safe technology usage habits [28].

In primary education, the learner must be able to analyze and assess the impact of technology on mental and physical health, society and the environment. To observe healthy and safe habits of using technology, justify their necessity. To construct, control and manage their digital identity [29]. In secondary education, in order to implement diverse plans, the learner must be able to purposefully choose or adapt and effectively use appropriate digital technologies, analyze the benefits and risks of digital communication, behave responsibly and communicate in the digital environment in accordance with their own and others' interests [28], [30].

The latest national professional higher education standard also states that the strategic goals of the first and second cycle professional higher education study programs are to ensure that graduates are able to responsibly and safely choose and use information technologies for the performance of work duties, research and lifelong learning, as well as for the acquisition, creation and sharing of digital content [30].

These goals also directly correspond to the challenges posed by the use of artificial intelligence, stipulating that "a data analytics course should be integrated into most programs in higher education" [7]. In turn, the information report "Strategic Roadmap for the Digital Decade for Latvia by 2030" states: "In the 2023 Digital Decade Report on Latvia, the European Commission has recommended accelerating efforts in the field of digital skills. Namely, Latvia is encouraged to continue implementing measures to integrate digital solutions into the education system throughout the entire education cycle, integrating them into all subjects" [31].

Combining the importance of legal education in public safety and sustainable development with regulatory enactments and policy planning documents to strengthen cybersecurity, it can be concluded that legal education is indispensable in modern society. Its main challenge is to ensure that lawyers are prepared to identify and prevent cyber threats, promoting a safe and sustainable digital environment.

IV. Conclusion

In legal science study programs, student training usually focuses on the analysis and interpretation of legal acts, developing practical skills for working with various legal sources, but cybersecurity issues, including those set forth in the legal profession standard, may currently often not be sufficiently addressed during the study program.

In the legal education process, cybersecurity and the protection of sensitive data are of fundamental importance, as students regularly work with confidential information, law enforcement and court practice materials, and legal databases during both academic studies and professional practice. However, there are several significant challenges in the current system:

Firstly, a lack of education on cybersecurity among students could pose a significant risk of data breaches. To mitigate this risk, it is imperative that law students have access to supplementary learning materials and training in secure computing and the protection of digital information. This will serve to reduce the likelihood of accidental or unintentional data leakage.
Second, digital resources used in legal databases and distance learning may not be adequately protected against potential cyber-attacks. Access to electronic court systems could be vulnerable if secure authentication mechanisms are not used, but this depends on the specific safeguards in place.
Thirdly, breaches of confidentiality may occur during student placements, particularly where there are no clear guidelines for the secure storage and transmission of sensitive documents. Personal email accounts, insecure cloud storage and poorly chosen passwords are sometimes used, which can increase the risk.
Fourthly, security vulnerabilities in students' personal devices could pose a risk to the protection of sensitive data. This can happen if students use poorly secured devices that may not have the necessary encryption tools and cybersecurity solutions.

Fifth, the specificity of legal education is associated with good skills in using information and communication technologies, as, for example, the national unified professional qualification exam for lawyers is taken in an electronic environment, as well as with several challenges of using various technologies and artificial intelligence in legal studies and research (which simultaneously raises several issues related to academic integrity).

Furthermore, although universities already offer various security solutions, current cybersecurity policies are often not sufficiently strict or effective to prevent potential threats.

To ensure confidentiality and the protection of sensitive legal data in legal education, specific measures are needed in two main areas: practical measures and the inclusion of requirements in legislation.

Although cybersecurity issues in legal education are not yet sufficiently developed, it is clear that they are becoming increasingly relevant as digitalization continues to affect the study process. To ensure that law students are prepared to work with sensitive data and understand security risks, universities need to take targeted measures to improve cybersecurity.

By introducing specialized training, improving e-study security mechanisms, and developing stricter confidentiality and quality guidelines, it is possible to achieve that the legal education environment becomes safer and more responsive to today's digital and security challenges.

Students who learn to use secure digital tools and understand the principles of data protection will be better prepared to work in courts, law firms, law enforcement agencies, etc. in the future, promoting trust and security in general.

Proposals for practical measures: 1) Integrating cybersecurity training into the study process – include cybersecurity and data protection courses as mandatory study content in law study programs; organize practical seminars and training on secure processing of sensitive data using real cases from legal practice; provide students with information resources on cybersecurity, including guidelines on secure password use, encryption technologies and secure data storage. 2) Strengthen the protection of sensitive data during student internships – set clear guidelines for students' handling of confidential data, for example, prohibiting storing it on personal smart devices/computers or transferring it using insecure emails; ensure that documents used during student internships are encrypted and accessible only to authorized persons; universities should work more closely with internship sites (courts, law firms, etc.) to ensure compliance with confidentiality policies and necessary training for students and internship sites; develop guidelines for secure device use, emphasizing the need for strong passwords, secure cloud storage, and regular system updates; promote student awareness of secure online communication using encrypted emails and file transfer tools.

Proposals for improving the regulatory framework: 1) Internal regulations of higher education institutions on data security – develop and implement a unified cybersecurity policy that regulates student access, document storage and information protection; clarify liability for violations of sensitive data processing and provide for liability for confidentiality violations in the study process. 2) Amendments to legal acts to strengthen cybersecurity in legal education – develop guidelines for universities on minimum data protection standards based on GDPR requirements; review the regulation of access to legal databases, ensuring that only registered users with appropriate rights can access sensitive legal materials; regulate the security of digital exams and distance learning, stipulating that secure authentication and monitoring mechanisms are used during exams; improve the standard of the legal profession by supplementing the acquisition of content related to (cyber)security and data protection during legal studies. 3) Cooperation between the judicial system and universities on cybersecurity issues – promote cooperation between universities and judicial institutions in the development of cybersecurity policy to provide students with practical knowledge of data protection in the judicial system; cooperate with IT security specialists to adapt study processes to the latest technological requirements; prepare recommendations for the Ministry of Justice for the implementation of digital security measures in legal education.

Overall, ensuring the security of sensitive data in legal education requires both a practical approach to student education and improving the use of technology, as well as the development of legislation that sets stricter security and data protection standards in higher education. The implementation of these measures would not only help reduce cybersecurity risks in legal education, but would also prepare students for professional activities in the digital age, where mitigating and protecting against cybersecurity risks is a key issue of professional ethics and responsibility.

REFERENCES

[1] I. Kudeikina and S. Kaija, "Problems relating to judicial selection in the context of sustainable development of society," European Journal of Sustainable Development, vol. 11, no. 4, 2022.

[2] J. Smith, Legal Education and Societal Security: Building a Sustainable Future. Cambridge University Press, 2021.

[3] D. Apse, "Juridiskā izglītība." Available: https://enciklopedija.lv/skirklis/2570-juridisk%C4%81-izgl%C4%ABt%C4%ABba. [Accessed: Feb. 10, 2025].

[4] "Latvijas kiberdrošības stratēģija 2023.–2026. gadam." Available: https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABbas%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf. [Accessed: Feb. 15, 2025].

[5] T. Brown, "Cybersecurity measures in higher education," Journal of IT Security, vol. 12, no. 3, pp. 45-58, 2020.

[6] Handbook for Academic and Scientific Institutions Improve Risk Management and Institutional Resilience in the Face of Security Threats. Rīga, RSU, 2024.

[7] "Informatīvais ziņojums 'Par mākslīgā intelekta risinājumu attīstību.'" Available: https://likumi.lv/ta/id/342405-par-maksliga-intelekta-risinajumu-attistibu. [Accessed: Feb. 15, 2025].

[8] Y. Walter, "Embracing the future of artificial intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education," International Journal of Educational Technology in Higher Education, vol. 21, no. 15, 2024.

[9] L. Johnson and K. Miller, Cybersecurity Law and Policy: An Essential Guide. Routledge, 2020.

[10] J. Doe, "WannaCry ransomware impact on institutions," Cybersecurity Journal, vol. 5, no. 2, pp. 33-40, 2018. [Accessed: Feb. 10, 2025].

[11] S. Osipova, "Tiesneša ētika. Komunikācijas ētikas dimensija: nodotās informācijas skaidrība." Available: https://www.satv.tiesa.gov.lv/runas-un-raksti/tiesnesa-etika-komunikacijas-etikas-dimensija-nodotas-informacijas-skaidriba/#_ftn2. [Accessed: Feb. 10, 2025].

[12] B. van Klink, "Critical thinking in academic legal education," LaM, Aug. 2023.

[13] Satversmes tiesas spriedums par Latvijas Sodu izpildes kodeksa 50.4 panta atbilstību Latvijas Republikas Satversmes 91.

pantam. Available: https://www.satv.tiesa.gov.lv/cases/. [Accessed: Feb. 15, 2025].

[14] European Commission, "Directive on security of network and information systems (NIS Directive)." Available: https://ec.europa.eu. [Accessed: Feb. 10, 2025].

[15] Aizsardzības ministrija. Available: https://www.mod.gov.lv/lv/zinas/uzsakts-darbs-pie-kiberdrosibas-izglitibas-cela-kartes-izstrades. [Accessed: Feb. 15, 2025].

[16] K. Kairis, "Tehniska brāķa dēļ noplūst pašvaldību darbinieku un iedzīvotāju dati." Available: https://www.lsm.lv/raksts/zinas/latvija/13.11.2024-tehniska-braka-del-noplust-pasvaldibu-darbinieku-un-iedzivotajudati.a576336/. [Accessed: Feb. 15, 2025].

[17] CERT.LV, "Darbības pārskats, 3. ceturksnis, 2024." Available: https://cert.lv/lv/2024/11/cert-lv-darbibas-parskats-par-2024-gada-3-ceturksni. [Accessed: Feb. 15, 2025].

[18] "Aicinām piedalīties Latvijas kiberdrošības izaicinājumā 2025." Available: https://www.visc.gov.lv/lv/jaunums/aicinam-piedalities-latvijas-kiberdrosibas-izaicinajuma-2025. [Accessed: Feb. 15, 2025].

[19] RTU, "RTU ar partneriem kiberdrošībā izglītos studentus." Available: https://lvportals.lv/dienaskartiba/370581. [Accessed: Feb. 15, 2025].

[20] "Kiberdrošības inženierija." Available: https://va.lv/studijas/magistrs/kiberdrosibas-inzenierija. [Accessed: Feb. 12, 2025].

[21] A. Smith and B. Jones, "Artificial intelligence and data security risks," AI & Law Review, vol. 9, no. 4, pp. 22-35, 2020.

[22] L. Johnson and K. Lee, "Phishing attacks in digital education," International Journal of Cybersecurity, vol. 14, no. 1, pp. 67-79, 2022.

[23] A. Brown, Digital Legal Resources and Cybersecurity Challenges in Education. Oxford University Press, 2022.

[24] E. Djatkoviča and M. Andžāns, "Latvia: Entangled system-in-progress amidst terrorism, Russia and cyberthreats," in M. Andžāns, A. Sprūds, and U. Sverdrup, Eds., Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication. Latvian Institute of International Affairs, 2021.

[25] ["Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA ... (Kiberdrošības akts)." Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj/?locale=LV. [Accessed: Feb. 15, 2025].

[26] Nacionālās kiberdrošības likums. Available: https://likumi.lv/ta/id/353390. [Accessed: Feb. 15, 2025].

[27] "Digitālās transformācijas pamatnostādnes 2021.-2027. gadam." Available: https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf. [Accessed: Feb. 15, 2025].

[28] Ministru kabineta 2019. gada 3. septembra noteikumi Nr.416. “Noteikumi par valsts vispārējās vidējās izglītības standartu un vispārējās vidējās izglītības programmu paraugiem”. Available: https://likumi.lv/ta/id/309597. [Accessed: Feb. 15, 2025].

[29] Ministru kabineta 2018. gada 27. novembra noteikumi Nr. 747. “Noteikumi par valsts pamatizglītības standartu un pamatizglītības programmu paraugiem”. Available: https://likumi.lv/ta/id/303768. [Accessed: Feb. 15, 2025].

[30] Ministru kabineta 2023. gada 13. jūnija noteikumi Nr. 305. “Noteikumi par valsts profesionālās augstākās izglītības standartu”. Available: https://likumi.lv/ta/id/342818-noteikumi-par-valsts-profesionalas-augstakas-izglitibas-standartu. [Accessed: Feb. 15, 2025].

[31] "Informatīvais ziņojums 'Digitālās desmitgades stratēģiskais ceļvedis Latvijai līdz 2030. gadam.'" Available: https://tapportals.mk.gov.lv/legal_acts/82b52f77-febe-4480-ac95-c11eff9c283a. [Accessed: Feb. 15, 2025].