https://doi.org/10.15388/TMP.2024.7

NAVIGATING THE LEGAL LANDSCAPE OF CYBERSECURITY REGULATION IN LITHUANIA

Ugnė Juknevičiūtė

Vilnius University Faculty of Law
2nd year student
Saulėtekio av. 9, I block, 10222 Vilnius
E-mail: ugne.jukneviciute@tf.stud.vu.lt

Vladyslav Murachov

Vilnius University Faculty of Law
3rd year student
Saulėtekio av. 9, I block, 10222 Vilnius
E-mail: vladyslav.murachov@tf.stud.vu.lt

Academic supervisor of the paper Dr. Neringa Gaubienė
Email address: neringa.gaubiene@tf.vu.lt

Annotation. *This article focuses on the analysis of Lithuanian cybersecurity legislation and possible problems that exist or will exist against the background of current threats and developments in European Union law.*

Keywords*: Cybersecurity, Cybersecurity Regulation, Cybersecurity policy, Cybercrime, Data Protection, Lithuania.*

Anotacija. *Šiame straipsnyje daugiausiai dėmesio skiriama Lietuvos kibernetinio saugumo teisės aktų analizei ir galimoms problemoms, kurios egzistuoja ar egzistuos, atsižvelgiant į dabartines grėsmes ir Europos Sąjungos teisės pokyčius.*

Raktiniai žodžiai: *Kibernetinis saugumas, Kibernetinio saugumo reglamentavimas, Kibernetinio saugumo politika, Duomenų apsauga.*

Introduction

In 2021, during President von der Leyen's State of the Union address, cybersecurity is one of the main priorities of the European Union because of all threats that exist. To become a leader in this field, the EU started to adopt several directives and regulations, the reformation and creation of a new body, the European Union Agency for Cybersecurity, etc. Lithuania is also interested in strengthening its cybersecurity,

given the fact of periodic attacks and threats from Russia (especially during Russia's invasion of Ukraine). Therefore, **this topic is extremely relevant** to Lithuanian lawmakers concerning digital security legislation. This article analyses a variety of possible challenges that Lithuania might face, both with the adoption of new legislation and the correction of old mistakes that, unfortunately, still exist.

The purpose of this article is to analyse and summarise all the legislative cybersecurity issues and challenges that the Lithuanian authorities are facing. In order to achieve the purpose of this study are relevant following **tasks:** 1) analysis of Lithuanian cybersecurity situation; 2) overview of Lithuania's current threats and legal problems; 3) analyse current national laws on cybersecurity; 4) analysis of international law concerning Lithuanian legislation; 5) providing recommendations. The **object** of this research is the analysis of European Union (EU) and Lithuanian cybersecurity legislation, executive documents of the National Cyber Security Centre (NCSC) and the Ministry of Defence, and reports of international and national bodies. The paper applies the linguistic **method**, which is used to interpret concepts and analyse their content; the analytical method is used to uncover the problems of legal regulation by examining certain aspects in their essence; the comparative method assesses Lithuanian, European Union and international regulation, as well as assessing practical scenarios to address future technical, economic or social challenges.

1.1. Lithuanian cybersecurity situation and key measures

Lithuania has been recognised in various global indices for its strong position in cybersecurity. For example, the ITU Global Cybersecurity Index 2020 ranked Lithuania sixth in the world, and the Foundation's E-Government Academy Cybersecurity Index 2021 ranked it second, highlighting its progress in this area. According to the NCSI, Lithuania ranks second in global cybersecurity metrics. The NCSI evaluates countries based on several indicators, including legal, technical, organisational, capacity building, and cooperation aspects.

The high level of cybersecurity was even confirmed by the Lithuanian Cyber Security Council. As we understand it, the authorities have a focus on the NIS2 Directive, namely its integration into the Lithuanian national system, and the adoption of recommendations from the audit "Ensuring Cybersecurity" carried out by the National Audit Office of Lithuania.

The National Cyber Security Centre of Lithuania (NCSC) has been actively providing recommendations and guidelines for critical infrastructure operators, focusing on preventive cybersecurity measures. Particular attention was paid to the continuity of operational plans and training programs. In April 2022, exercises were conducted to test the secure state data transmission network and assess the institutional capacity to use it, ensure timely information exchange and response to potential threats between cybersecurity entities.

Lithuania is also focusing on educational initiatives to strengthen its cybersecurity capabilities. Universities such as Mykolas Romeris University, Kaunas University of Technology and Vilnius University offer specialised cybersecurity programs, contributing to the training of qualified professionals in the field. In addition, Lithuania's digital infrastructure is outstanding: the country is recognized for its availability of digital skills, 4G internet coverage, and one of the fastest public Wi-Fi speeds in the world.

In addition, employees of the state and critical information infrastructure were encouraged to responsibly assess increased cybersecurity risks. More than 1,200 state and municipal employees completed a comprehensive three-day cybersecurity training, and another 2,400 civil servants attended shorter NCRC training on basic cybersecurity knowledge. A special course was also organised for Lithuanian organisations supporting Ukraine.

But, as you will see later, the paper deliberately minimises its reliance on broad doctrinal analysis (especially Lithuanian) to focus on real-world applications and challenges in the cybersecurity domain of Lithuania and the European Union. There is no doctrine on cybersecurity in general yet. Therefore, it focuses on current EU legislation and global cyber threats, providing a direct, applied assessment of the issues at hand rather than theoretical discourse. Given that EU and Lithuanian cybersecurity legislation is still in its infancy, largely based on research by EU agencies and organisations, this focus allows for a better understanding of new areas such as anti-hacking policies and the protection of critical actors in the changing global cybersecurity environment.

Despite these precautions and innovations, cybercrime is happening, and before we look at the legal framework of these incidents, we must consider what kind of crimes are happening. By doing so, we will determine which crimes require the most attention in terms of legal response.

1.2. Brief overview of Lithuania's current threats

Lithuania, like many other countries, is a regular victim of cyberattacks, with both individuals and public bodies losing hundreds or even millions of euros and large amounts of data. It is particularly noteworthy that the same year 2022 was marked by Russia's invasion of Ukraine, which had a significant impact on the cyber landscape both in Ukraine and abroad. Of course, one of the features of cybercrime is its "untraceability", but Russia is dealing a serious blow to the cybersecurity of Lithuania, Ukraine and the European Union.

For example, an attack on the KA-SAT satellite network on 24 February 2022 led to disruptions in internet services in several European countries. For the first time, the EU publicly accused Russia of this attack.

As for Lithuania, while the total number of cyber incidents recorded by the NCSC remained the same as in 2021, the number of distributed denial-of-service (DDoS) attacks increased, especially in June 2022, targeting Lithuanian public and private sector websites. These attacks, claimed by groups supporting the policies of the Russian Federation, attempted to influence more than 130 publicly accessible websites. It is noteworthy that Lithuania not only withstood these attacks without damage to the websites, but also became stronger by devoting more attention and resources to cybersecurity. But at the same time, for example, phishing campaigns are still happening, especially because of the war.

In 2022, cybercrime in the digital space doubled (by 52%) compared to the previous year, with financial gain being the main motive. In Lithuania alone, cybercriminals have successfully lured almost €12 million from citizens and businesses. NCSC reported 4,080 cyber incidents in 2022, similar to 2021, with a marked increase in the number of DDoS attacks. Most incidents were related to the spread of malware, phishing attacks aimed at extracting confidential information, and attempted intrusions. Similarly, ransomware attacks were among the most common types of cyber incidents in Europe (report of NCSC 2022).

But we should not forget about possible risks, for example, in the 2024 Lithuanian presidential election or the European Parliament elections. Although there were no cybercrimes against elections in the last elections. There were cyber incidents in Poland and Slovakia last year, which, of course, did not affect the elections, but undermined the situation. We should also add the fact of the spread of AI technologies and Russia's war against Ukraine, whose aggressor has repeatedly tried to interfere with the cybersecurity of other countries.

Given the fact that the largest number of cyber incidents were against government organisations or organisations that own critical infrastructure, we will focus on such bodies. Moreover, they are more regulated and more controlled by the authorities, but they also have certain problems, which we will discuss further.

2. Existing Legal Framework in Lithuania

2.1. Analysis of current national laws related to cybersecurity

Lithuania, like other European Union member states, aligns its cybersecurity regulations with European Union directives and regulations. Therefore, national legislation needs to be analysed first, before focusing on EU legislation and comparing Lithuanian and EU legislation.

The main aim of Republic of Lithuania law on Cyber Security is to ensure the prevention, suppression and investigation of cybercrime. The law sets out the principles on which cybersecurity is based: non-discrimination in cyberspace, the essence that

same laws and values must apply in cyberspace as in physical space; proportionality of cybersecurity, means that legal, technical measures must not restrict the activities of cybersecurity entities in cyberspace more than is necessary; the primacy of the public interest – foremost ensure the protection of the public interest, but also can not substantially violate the rights of consumers. All these principles must be mutually compatible, without allowing one principle to take precedence over the other.

This law defines cybersecurity principles, institutions which develop and implement cybersecurity policy, powers of these institutions, determines duties of cybersecurity entities and the inter-institutional cooperation (Article 1(1) of Republic of Lithuania law on Cyber Security). The law states that the strategic objectives and priorities of the cybersecurity policy and the measures necessary to achieve them are determined by the Government of the Republic of Lithuania, which affirms the National Cyber Security Strategy, the institutional structure of Cybersecurity council, the organisational and technical requirements for cybersecurity, the National cyber incident response plan and cybersecurity risk management (). In addition, without Government, two ministries have powers in this field. The first is the Ministry of National Defence of the Republic of Lithuania, which formulates the cybersecurity policy, organises control and coordinates its implementation, develops and submits organisational and technical cybersecurity requirements and other functions established by the legislation of the Republic of Lithuania (ibis, article 6). The second one is the Ministry of the Interior, which develops and provides the methodology for the identification of information infrastructure and the information infrastructure and other (ibis, article 7). These different but at the same time similar responsibilities assigned to two ministers often reveal one of the biggest problems in lithuanian legislation. In practice, when it comes to the adoption of new legislation, disagreements arise as to who has to adopt it and whose duty it is.

In addition to the above mentioned law, the Criminal Code of the Republic of Lithuania is directly related to cybersecurity. The chapter "Crimes against security of electronic data and information systems", articles 196 to 198 of Code provide criminal responsibility for physical and legal persons who have caused significant damage. For example, regulated cases include those who destroyed, damaged or replaced computer information; those who destroyed, damaged or replaced a program on a computer, or installed a program on a computer that disrupted or modified the operation of a computer's network, data bank or information system. Also, who has misappropriated, publicly disseminated, distributed or otherwise used computer information preserved by law.

In Lithuania, and other legislation sets out requirements and measures related to cybersecurity. It includes the law on electronic communications which regulates this sector and provides for measures on the security of information and communication networks and services, the law on legal protection of personal data which regulates

the processing of personal data, legislation on information systems of the state and its administration, and financial institutions obliged to comply with additional requirements set out in specific legislation. These mentioned legal acts are interrelated in specific areas of activity and these provisions have direct and indirect effects on cybersecurity issues. In summary, cybersecurity entities must consider all relevant legislation to ensure that their cybersecurity activities are fully compliant with legal requirements.

2.2. Analysis of The National Cyber Security Strategy

The National Cyber Security Strategy (hereinafter Strategy) sets out the main guidelines for the country's cybersecurity efforts, both in the public and private sectors. It has been prepared considering the findings of the studies carried out and proposals of the representatives of the public and private sectors and is in line with the Programme of the Government of the Republic of Lithuania, the National Security Strategy, the Law of the Republic of Lithuania on Cyber Security, and the provisions of the European Union Strategy. The implementation of the Strategy has five purposes: to strengthen cybersecurity and the development of cyber defence capabilities; to ensure the prevention and investigation of criminal offences; to induce a culture of cybersecurity and the development of innovations; to strengthen close public-private and international cooperation; and to ensure the fulfilment of the international obligations in cyber security.

The first objective of the Strategy is to strengthen the country's cybersecurity and develop defence capabilities. Lithuania, like other countries with developed broadband infrastructure is becoming attractive not only to individuals, groups or organised groups, but also to the State Security Department of the Republic of Lithuania (DSS) and the Second Operational Services Department under the Ministry of National Defence of the Republic of Lithuania (AOTD) in the annual Threats to National Security Report states that Lithuania is constantly confronted with various types of cyber incidents aimed at compromising the country's information resources, critical information infrastructure and information infrastructure of national security significance.

The second objective of the Strategy is to ensure the prevention and investigation of cybercrime. Cybercrime harms the global economy, causing billions of euros of damage per year (European Cybercrime Centre (EC3), 2017 Internet Organised Crime Threat Assessment (IOCTA)). Criminals are not only interested in financial misappropriation but in data misappropriation in general. To prevent cybercrime, which is constantly evolving and taking new forms, it is important to develop cross-border cooperation and information exchange, and law enforcement personnel must be well prepared to assess, identify and investigate threats. Furthermore, countries must

comply with international obligations, international standards in cybersecurity, not only at the legal level but also at the practical level.

The third objective of the Strategy is to foster a culture of cybersecurity and innovation. In order to raise the cybersecurity culture of the Lithuanian population, continuous dissemination of information must be ensured, including up-to-date information on incidents.

The fourth objective of the Strategy is to strengthen close cooperation between the public and private sectors. The private sector, with its capital, is in a better position to invest in cybersecurity threat assessment, qualified employees and security systems. However, the private sector is often unable to manage cyber incidents on its own, often beyond the boundaries of its organisation. Public-private cooperation and mutual trust are therefore a prerequisite for comprehensive cybersecurity. The Cybersecurity Information Network (further on Network) is used to implement public-private cooperation. One of the objectives of the Network is to share information on potential and actual cyber incidents, as well as recommendations, guidance, technical solutions and other tools to ensure cybersecurity and cooperation between Network members in the field of cybersecurity. The benefits of ICT[1] are undeniable, but this raises the question of how to respond effectively to security gaps that are detected. As security vulnerabilities are sought by individuals with different objectives, it is important to enable the person who has found a security vulnerability and wishes to remedy it to cooperate with the cybersecurity actors whose ICT security vulnerability has been exposed. Therefore it is important to develop responsible public-private disclosure of ICT security vulnerabilities, which will be achieved by promoting a culture of self-protection and responsible behaviour in cyberspace, improving the performance of law enforcement authorities' functions in the fight against cybercrime and ensuring operational international cooperation in the investigation of cybercrime, and developing effective cooperation between law enforcement authorities and research and academic institutions, the public-private community and the general public.

The fifth objective of the Strategy is to strengthen international cooperation and ensure compliance with international obligations in the field of cybersecurity. Considering the borderless nature of cyber threats and risks, Lithuania will strive to strengthen national cybersecurity actively cooperating with partners, by concluding an international agreement on the legal regulation of cyberspace and targeting international forums for addressing cybersecurity and global internet governance issues. Lithuania has set itself the objective of focusing on cooperation with NATO, the EU and other countries to avoid duplication of functions and activities. Not only at the national level but also in the European Union, the benefits of cooperation are being highlighted and identified not only in theory but also in practice. The EU Strategy (2022) describes how

[1] Information and communication technology

the EU can harness and strengthen the tools and resources to become technologically sovereign. All four cyber communities - internal market, law enforcement, diplomacy, defence - need to work more closely together to achieve common threat awareness, respond jointly to cyber attacks, and set out plans to cooperate with partners around the world to ensure international security and stability in cyberspace.

2.3. Analysis of international law concerning Lithuanian legislation

One of the first and main laws is EU Regulation 2019/881, commonly known as the Cybersecurity Act. This is important for two main reasons. Firstly, it established ENISA (The European Union Agency for Cybersecurity), whose task is to contribute to the overall improvement of cybersecurity in the EU, support policy development and implementation, and assist Member States in preparing for and responding to cyber threats. Secondly, it created a cybersecurity certification system. The regulation introduces a certification system for information and communication technology (ICT) products, services and processes from a cybersecurity perspective. This pan-European cybersecurity certification scheme aims to ensure a high and consistent level of cybersecurity of digital products and services across all EU Member States.

After that, one of the most recent but significant directives, Directive (EU) 2022/2555, also known as NIS 2, is a significant step forward in the European Union's approach to cybersecurity legislation. It replaces the previous Network and Information Security (NIS) Directive (The NIS Directive 2016/1148) and aims to respond to the changing threat landscape by establishing a higher overall level of cybersecurity in the EU.

For example, The NIS 2 broadens the range of sectors and entities under its purview, specifically targeting essential and important entities in sectors such as energy, transport, finance, and digital services. Directive also grants national authorities enhanced powers for the supervision and enforcement of its provisions, including conducting on-site inspections and security audits. In addition, Member States have until October 17, 2024 to adopt the necessary measures to comply with Directive NIS 2 (EU) 2022/2555. The Directive will enter into force on October 18, 2024. Therefore, Lithuania does not have a lot of time and already needs to propose a new draft version of the cybersecurity legislation (we will discuss this in the next sections).

But, in our opinion, and the opinion of many experts, the peculiarity of this directive is the possibility of the main management responsible for cybersecurity being brought to justice for its violation. It is envisaged that private organisations may face a minimum penalty of 2 percent of their annual turnover or up to EUR 10 million. This is nothing new, as it is already in place, for example, in the GDPR. But at the same time, the Directive is not limited and allows for not only administrative but also criminal liability.

An equally important regulation is the Digital Operational Resilience Act (DORA). This is a specialised directive that fills a significant gap in EU financial regulation. It focuses on cyber risk management and establishes rules relating to ICT risk management, incident reporting, operational resilience testing, and monitoring of third-party ICT risks. This law recognizes that ICT incidents and lack of operational resilience can pose a threat to the stability of the entire financial system, even if there is "sufficient" capital allocated to traditional risk categories. The DORA is a legal act of direct effect in EU member states, so it does not require adoption by the Seimas of Lithuania.

The importance of DORA lies in the fact that it is similar to NIS2, but regulates only financial institutions, regardless of the number of employees and capital. NIS 2 states that if sectoral laws, such as the DORA in the field of finance, establish cybersecurity measures equivalent to the NIS 2 Directive for key entities, then the NIS 2 rules do not apply and the sectoral laws prevail. If sectoral legislation does not cover all entities, the NIS 2 rules still apply (Article 4(1) of the NIS 2 Directive). Directive also considers sectoral cybersecurity measures to be equivalent if they are consistent with the measures referred to the NIS 2 Directive (ibis, articles 21(1) and (2), article 4(2)(a)).

In addition, there is a Critical Entities Resilience, a security-focused legislation applicable across the EU. It replaces Directive 2008/114/EC. Unlike NIS2, which concentrates on cybersecurity, CER's goal is to establish a comprehensive framework addressing the resilience of critical entities against various hazards, including both natural and human-made, accidental or deliberate.

There are also many other directives that focus on specific areas of cybersecurity that are important for this paperwork. These include:

- The European Electronic Communications Code (EECC) - is aimed at the regulatory framework of the telecommunications sector; ibis, articles 21(1) and (2), article 4(2)(a)
- Regulation (EC) No 460/2004 - declare the establishment of the European Network and Information Security Agency (ENISA) - EU Agency in order to prevent, address, and respond to network and information security problems of EU-members and of organisation in general;
- The General Data Protection Regulation - about user's data and main points about duties of data protection officers (to protect and/or notify about all possible breaches).

In conclusion, the European Union has many cybersecurity regulations in general: most of the Directives and Regulations are new and have not even entered into force yet. Therefore, Lithuanian lawmakers are now facing new challenges that no other member state has ever experienced, which we will analyse further.

3. Main legal risks and problems in Lithuanian legislation

The adoption of the recent legislative framework in the European Union, as well as the corresponding changes in Lithuanian cybersecurity, is a commendable step towards addressing the existing problems. These legislative efforts are expected to address a significant number of prevalent problems. On the other hand, it should be recognised that such regulatory changes do not fully cover all the challenges specific to the Lithuanian context and, paradoxically, may create additional challenges for the country's legislature.

3.1. Problems with ARSIS

Entities managing and (or) processing state information resources must ensure the organisational and technical cybersecurity requirements set out in the Republic of Lithuania law on Cyber Security and other legal acts. They have to organise and carry out a risk assessment of communications and information systems at least once a year or after major organisational or systemic changes and submit it for the elimination of disruptions to ARSIS (Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema), the system for monitoring compliance of state information resources with the requirements for the security of electronic information.

The purpose of ARSIS is to collect and evaluate information, identify existing breaches, analyse information security risks, and develop risk management. The information obtained during the national cybersecurity risk assessment needs to be used to make strategic decisions that will affect the organisation's operations and business continuity and ensure compliance with the requirements of the legislation of the Republic of Lithuania. To achieve its strategic objectives, each organisation must monitor and evaluate the effectiveness of its activities and the risks it faces, and this requires continuous and organised monitoring because in that way it shows the change in progress over a given period and identifies the strategic problems that need to be solved.

The report of National Audit Office (Valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas", 2022 m. spalio 27d. Nr. VAE-10) stated that 38% (81 out of 212) of the surveyed cybersecurity entities had not carried out a cybersecurity risk assessment during the 3 years (2019-2021) also a significant proportion of the surveyed entities had not conducted a cybersecurity risk assessment at all (56% or 74 out of 131) and did not provide information on identified cybersecurity risks to the NCSC. This analysis shows that the failure to carry out an assessment has led to a failure to assess security management systems and, where necessary, to address the issues that have arisen. According to cybersecurity entities, ARSIS is ineffective, the func-

tionality of the system is not sufficiently utilised, and it does not provide feedback to facilitate the implementation of requirements by cybersecurity entities. According to the managers and administrators of state information resources, the reason why security compliance assessments are not carried out is the lack of human resources, competence and funding. The process of cybersecurity risk evaluation requires specific knowledge in this field and the specialists performing the risk assessment of the institutions are not able to qualitatively assess the cybersecurity risks, which is why it is appropriate to have risk assessment guidelines. However, the problem is that there is no national guidance on the specific risk assessment methodology to be used by cybersecurity entities, which does not allow for digitised security compliance. The framework is important in terms of the information gathered, but it does not contain aggregation, assessment indicators, insights. Entities indicated that ARSIS is only an archive of paper documents, whereas the system should be a tool to see the big picture and compare it with others. The recommendations for improvements were to be implemented by 1 June 2019, but problems have not been resolved, as the current software code does not allow for the extension of ARSIS functionality. In addition, another problem is that there is no consolidated legal framework for cybersecurity and electronic information security. The legislation requires all cybersecurity entities to carry out a risk assessment of their communication and information systems but does not require the results of the risk assessment to be made available to the responsible public authorities. However, The Lithuanian Ministry of National Defence with other institutions is working on the draft amendments to the law on cybersecurity, which will be released in March and it should solve this problem.

To solve problems of the ARSIS system, good practice recommends concluding sectoral risk profiles that provide a quantitative threat analysis and periodic updates, the establishment of an information governance framework that addresses security principles, formal and ongoing information security management methods and ensures that established policies, principles, standards, procedures, methodologies are in line with all applicable international requirements. In addition, to improve cybersecurity risk management, implement a national governance process, develop a common methodology for evaluation compliance in cybersecurity and information resources security and adopt measures to ensure better communication of cyber incidents. Such risk management would allow the relevant authorities to have up-to-date information on the risks identified by cybersecurity entities and to coordinate at the national level a process for their management, ensuring the deployment of the necessary protection, prevention and response measures.

In summary, ARSIS, as a tool for evaluation and monitoring security compliance, is an important element in ensuring the sustainability of the cybersecurity system, and problems that cannot be solved have a negative impact and create conditions

for vulnerabilities to develop. According to research by ISACA[2] and the CMMI[3] Institute, organisations with a strong cybersecurity culture have a better awareness of potential threats, a lower number of cyber incidents, and a higher resilience to potential threats. Currently, institutions are not well prepared for emerging cybersecurity challenges. Cybersecurity exercises and training focused on the latest cybersecurity trends and organised regularly to increase staff attentiveness and cybersecurity culture.

3.2. Risk of creating double legislation

We have already mentioned the difference between DORA, CER and NIS 2, so, for example, clearly financial institutions need the same or additional (different) regulation than other important entities. Lithuania should not apply the provisions of the NIS 2 Directive on cybersecurity risk management and reporting obligations, as well as supervision and enforcement to financial institutions covered by the DORA. However, there may be a problem that financial and other institutions will be lumped together in the new bill without separating them. This could lead to duplication or, on the other hand, uncertainty in the legal framework arising from the inclusion of financial institutions in other entities, making it difficult for institutions to accurately interpret and comply with the law. This was before in Lithuanian legislation, in relation to cybersecurity requirements and electronic information security requirements, where the legislation is still not consolidated. Legislation should not allow for an administrative burden (article 3.1(1) of Republic of Lithuania Law on the Reduction of Administrative burden).

Another example of double or conflicting legislation is the confusion of terms between European acts. For example, Recital 19 in both mandates be clarified, as it introduces disparities between the definition of 'incidents' (and 'vulnerabilities') used in NIS2 and those to be applied in the context of the CRA. They have different thresholds or criteria for what constitutes an 'incident', entities may struggle to determine when and how to report. For example, CRA might require reporting minor incidents with limited impact, while the other focuses on significant incidents only. There are also problems in the articles themselves, where the Act requires notification of ENISA, while the Directive demands to notify local authorities. This difference can lead to confusion about compliance obligations.

---

[2] Information Systems Audit and Control Association, an international association focused on information technology governance.

[3] Capability Maturity Model Integration, it is an improvement training and appraisal program. CMMI can be used to guide process improvement across a project, division or entire organisation.

3.3. Status of small and micro enterprises

The NIS2 suggests that small businesses should be left out of the scope so as not to limit their growth. Therefore, it also proposes incentives in the form of funding or education for SMEs to encourage them to implement cybersecurity measures. On the other hand, this proposal allows Member States to determine which SMEs are critical or important to the economy or society of each particular Member State.

This approach may lead to fragmentation and legal uncertainty for SMEs operating in several Member States, as they may be subject to regulation in one Member State but not in another. In addition, SMEs may incur additional costs associated with complying with varying regulatory requirements in different Member States.

There are two ways, in our opinion, to reduce the negative impact of this. First, there is some kind of "additional" harmonisation between the member states with which we have the largest economic ties. This will minimise the difference with other countries where enterprises that are also located in Lithuania could potentially be located. But this method can only be applied after all the amendments have been adopted in the main member states, which will also take a long time. In this case, it may be easier to continue harmonisation at the NIS3 level (or even reclassify it from a Directive to a Regulation).

The second way is to completely minimise the number of types of small businesses that fall under NIS 2. This will allow companies to develop more easily not only in Lithuania, but also for those operating in several countries. This method may sound very liberal, because This method may sound very liberal, because there are many small businesses that have significant capital or are important.

There is a third, middle way: to minimise this number, but at the same time, the selection of additional entities will be based on a unified approach and will be consistent throughout the EU. Given all these facts, the Lithuanian authorities should find a balance between the ability of small businesses to grow and the cybersecurity of important data.

Thus, allowing Member States to define critical SMEs could lead to regulatory fragmentation and uncertainty for businesses operating in multiple countries. The Lithuanian legislator needs to be very careful about the balance so as not to burden entities

3.4. Personal liability for cybersecurity negligence

As we mentioned earlier, the NIS2 Directive provides for penalties. Including, it allows criminal sanctions, for example, for special negligence on the part of directors of entities. Therefore, we will consider world examples, whether Lithuania needs it and what problems there may be with it.

One example we will look at is the legislation of the United States of America. There, criminal penalties for cybersecurity negligence, including actions that could harm the security, confidentiality, integrity or availability of IT systems, are applied under federal laws. For example, the Computer Fraud and Abuse Act (CFAA) is a key piece of legislation that targets a range of cybercrime activities. Violations under the CFAA may result in a fine or even imprisonment, the length of which depends on the nature of the violation and the existence of aggravating circumstances.

One more example is the Caremark case in Delaware. The court decided that liability for failure to monitor risk can only be imputed to individual board members where: (a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.

Does Lithuania need it? Yes and no. On the one hand, the number of obligations is increasing, and therefore gross violations by directors can compromise the cybersecurity of not only entities, but the entire security of Lithuania. For example, even recently there was a serious data breach, where 260,000 user data were stolen. We cannot say who is to blame and how this leak occurred, but it is an example of the fact that such situations do happen and, for example, failure to update cyber systems or ignoring any training programs will increase the risks in general. On the other hand, this may partially discourage private companies from operating in Lithuania due to a certain fear that directors may be punished for a mistake. But if, for example, a criminal penalty in the form of a fine is introduced, then, logically, this is the same as punishing the entire company for the violation, which is already included in the NIS2 Directive.

Thus, this practice exists. The argument in favour of criminal liability is the ultimate responsibility of the manager for the security of the organisation and the potential public harm that can be caused by breaches. However, challenges include the difficulty of determining the exact cause of a breach, the rapidly changing threat landscape and the reality of operating in a complex environment.

Therefore, even if no criminal penalties are envisaged, some form of personal liability should be considered for certain individuals who are completely negligent in their cybersecurity of important institutions.

4. Conclusion

1. There are few key points that should be considered in the new legislation. First of all, fixing the ARSIS and implementing a national governance process. ARSIS does not provide feedback to facilitate the implementation of requirements. Therefore, it should be concluding sectoral risk profiles that provide a quantitative threat

analysis and periodic updates. As a result, it would ensure better communication about cyber incidents and would improve risk management.

2. Create national guidelines on the risk assessment methodology. It should develop a common methodology for evaluation compliance in cybersecurity and information resources security. Establishment of an information governance framework that addresses security principles, information security management and ensures that established standards, procedures, methodologies comply with all applicable international requirements.
3. Consolidation of legislation: the new European legislation should contribute to a more consolidated legislation. If earlier it concerned issues between cybersecurity and electronic data protection requirements, now it is about the correct harmonisation of the new Directives so that the requirements do not repeat (or at least do not conflict) with each other and other regulations.
4. Refraining from imposing harsh obligations: new and consolidated requirements are needed, but too high cybersecurity requirements (above NIS2 requirements) will reduce the development of companies (especially small and micro entities), or even the outflow of such organisations from Lithuania to Member States with lesser limitations and obligations.
5. Promoting and detailing the legislation about the use of certification: The NIS2 Directive entails an increase in ICT-related costs. One way to reduce these costs at the national level is to establish a certification system. Such well-designed certification systems can serve as a model for the development of certification in the EU. The authorities will ensure that the certification is in the country and guarantee the recognition of international certification for non-critical devices/applications.

List of sources

Legislative acts

1. Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. direktyva (ES) 2022/2555 dėl aukšto bendro kibernetinio saugumo lygio Sąjungoje užtikrinimo priemonių, iš dalies keičianti Reglamentą (ES) Nr. 910/2014 ir Direktyvą (ES) 2018/1972 bei panaikinanti Direktyvą (ES) 2016/1148 (NIS 2 Direktyva) (Tekstas svarbus EEE). OL L 333, p. 80. Available at the link: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
2. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl tokių duomenų laisvo judėjimo bei panaikinant Direktyvą 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, p. 1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
3. „Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. reglamentas (ES) 2022/2554 dėl skaitmeninio veikimo atsparumo finansų sektoriuje ir iš dalies keičiantis reglamentus

(EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011." OL L 333, 2022-12-27, p. 1–79. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554.
4. Europos Parlamento ir Tarybos 2022 m. gruodžio 14 d. direktyva (ES) 2022/2557 dėl kritinių subjektų atsparumo stiprinimo ir panaikinant Tarybos direktyvą 2008/114/EB." OL L 333, 2022-12-27, p. 164–198. Available at: Directive 2022/2557.
5. Europos Parlamento ir Tarybos 2018 m. gruodžio 11 d. direktyva (ES) 2018/1972, nustatanti Europos elektroninių ryšių kodeksą (persvarstyta)." OL L 321, 2018-12-17, p. 36–214. Available at: Directive (EU) 2018/1972.
6. Europos Parlamento ir Tarybos 2004 m. kovo 10 d. reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos saugumo agentūrą." OL L 077, 2004-03-13, p. 1–11. Available at the link: Regulation (EC) No 460/2004.
7. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl tokių duomenų laisvo judėjimo bei panaikinant Direktyvą 95/46/EB (Bendrasis duomenų apsaugos reglamentas)." OL L 119, 2016-05-04, p. 1–88. Regulation (EU) 2016/679.
8. Lietuvos baudžiamasis kodeksas, 2000 m. rugsėjo 26 d. Nr. VIII-1968. TAR, 1968.
9. Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014 m. gruodžio 11 d. Nr. XII-1428. TAR, 0553.
10. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, 2018m. gruodžio 11d., Nr. V-1183. TAR, 0526.
11. Nacionalinė kibernetinio saugumo strategija, 2018m. rugpjūčio 13 d., Nr. 818. TAR, 3252.
12. Nacionalinė saugumo strategija, 2002m. gegužės 28d., Nr. IX-907.
13. Kibernetinio saugumo informacinio tinklo nuostatai, 2019m. lapkričio 27d., Nr. V-998.
14. Valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas", 2022 m. spalio 27d. Nr. VAE-10.
15. Aštuonioliktosios Lietuvos Respublikos Vyriausybės programa, 2020m. gruodžio 11d., Nr. XIV-72.
16. Procesų vertinimo modelis, naudojant COBIT®5, APO12 proceso „Valdyti riziką" BP3 bazinės praktikos „Valdyti rizikos profilį" aprašymas, 61–62 psl.

Other sources

17. Key trends and statistics of the National Cyber Security Status of Lithuania, 2022 Ministry of National Defence of the Republic of Lithuania.
18. Valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas". 2022 m. spalio 27 d. Nr. VAE-10.
19. Zoey Stambolliu, Alberto Di Felice, "Building a strong foundation for the Cyber Resilience Act: key considerations for trilogues." (2023, September 25). Available at:https://www.digitaleurope.org/resources/building-a-strong-foundation-for-the-cyber-resilience-act-key-considerations-for-trilogues/.

20. "The Board of Directors' Duty of Oversight and Cybersecurity." The CLS Blue Sky Blog, Columbia Law School, October 28, 2021. Available at: https://clsbluesky.law.columbia.edu/2021/10/28/the-board-of-directors-duty-of-oversight-and-cybersecurity/#_ftn5.
21. Speech by President von der Leyen at the State of the European Union Address" [Online] (2021, September 15). Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.
22. Lithuania Records Over 4,000 Cyber Attacks in 2022. [Online] (2023). Available at: https://www.lrt.lt/en/news-in-english/19/2002523/lithuania-records-over-4-000-cyber-attacks-in-2022.
23. Lithuania-Russia Cyberattacks. [Online] (2022). Available at: https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html.
24. Cyber Security Council Overviewed National Cybersecurity Situation and Major Undertakings. [Online] (June 26, 2022). Available at the link: https://kam.lt/en/cyber-security-council-overviewed-national-cybersecurity-situation-and-major-undertakings/.
25. "Ukrainu bēgļi Lietuvā saņem viltus e-pasta vēstules; uzbrukums saistīts ar Krieviju" [Online] (2023, January 23). Available at: https://www.tvnet.lv/7696931/ukrainu-begli-lietuva-sanem-viltus-e-pasta-vestules-uzbrukums-saistits-ar-krieviju.
26. European Election at Risk from AI, Says EU's Cyber Agency. [Online] (2023, October 19). Available at the link: https://www.politico.eu/article/european-union-election-risk-artificial-intelligence-interference-cybersecurity-agency-enisa/.
27. The European Parliament has an Election Security Problem. [Online] (2023, December 10). Available at: https://www.politico.eu/article/european-parliament-election-cybersecurity-problem/.
28. "Informuoja apie dar vieną didelio masto programišių ataką Lietuvoje: nutekinti 260 tūkst. vartotojų duomenys." [Online]. Available at: https://www.delfi.lt/login/progresas/kibernetinis-saugumas/informuoja-apie-dar-viena-didelio-masto-programisiu-ataka-lietuvoje-nutekinti-260-tukst-vartotoju-duomenys-95593475.
29. International Telecommunication Union. "Guide to Developing a National Cybersecurity Strategy - Strategic Engagement in Cybersecurity." 2018. Available at: https://www.itu.int/hub/publication/d-str-cyb_guide-01-2018/.
30. European Union Agency for Law Enforcement Cooperation (Europol). "European Cybercrime Centre (EC3), Internet Organised Crime Threat Assessment (IOCTA), 2017.

SUMMARY

This article provides a detailed assessment of legislative cybersecurity issues and challenges that Lithuanian authorities are facing and might face in the future. To achieve this purpose, Lithuanian cybersecurity legislation is evaluated and compared with European Union law. This study draws attention to and assesses the problematic aspects related to cybersecurity regulation.

After analysing all sources, it can be concluded that Lithuania needs to improve its legal instruments to ensure that they are robust, adaptable and in line with new cybersecurity threats and technological advances because cybercrime remains a persistent issue. The balance between security and privacy, flexibility and capabilities of entities and individuals must be maintained. The Republic of Lithuania law on Cyber Security and The National Cyber Security Strategy sets out the main guidelines to ensure the prevention and investigation of cybercrime. Even though from a theoretical point of view, it seems that the law adjusted the aims of risk management, the organisational and technical requirements for cybersecurity and Cyber Security Strategy sets out the main objectives for the country's cybersecurity efforts, both in the public and private sectors. But on the practical part, the picture is completely different.