Recent Developments of Cyber-Offences in Slovenia

Andreja Primec, Bojan Tičar

Abstract

Digitalisation of the economy has exceeded its original boundaries and expanded to all areas of social life. In addition to all the benefits of digitalisation, it also creates risks of malicious use of the electronic information potential. Cyber security should play its part to prevent electronic information network and system intrusions, misuse of information, and to ensure smooth and secure information flow.

Research design of this paper is the set of three research methods used in collecting legal information about cyber security regulation and analysing findings. First approach is descriptive analysis of legal regulation. Second method is desktop analysis of recently adopted legal acts. Third research method is observational study. Synthesis is presented in the conclusions.

Legal regulation of cyber security refers to protecting the data and information systems against unauthorised access, use, disclosure, disruption, alteration, or destruction. Cyber security is concerned with the confidentiality, integrity, and availability of data regardless of the form the data may take electronic, print or any other.

The Law of Minor Offences will apply to minor offences in the field of cyber security about "general" issues: liability of the perpetrator, imposition of sanctions, minor offence proceedings, etc., whereas the provisions of special legislation,

ILIRIA International Review – Vol 11, No 1 (2021)

more specifically, the provisions of the Cyber Security Law and the Electronic Communications Law, will apply to the identification of an act as a minor offence.

However, in accordance with the *lex specialis derogat legi* generali principle, the general provisions of the Law of Minor Offences will apply only if such issues are not regulated otherwise by the Cyber Security Law and the Electronic Communications Law.

Keywords: *cyber security, cyber offences, minor offences, administrative violations, cyber systems, information networks*

1. Introduction

Cyber-attacks are becoming more sophisticated, targeted, widespread, and undetected (ENISA, 2020). Therefore, it is not surprising that the new and fundamentally different type of crime, cybercrime, requires elaborating new criminological theories. A new academic discipline, cyber criminology, which focuses on the reasons for the emergence of crime in cyberspace and its impact on the physical environment, has arisen (Meško, 2018).

Information security issues were generally studied in a technological context but growing security needs have extended researchers' attention to exploring the management role. From this point of view, information security is defined as the activity to protect information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities (Hagen, Albrechtsen and Hovden, 2008). Consequently, the most researched issues are the importance of security policy and the impact of awareness, training, and compliance on information security effectiveness. Chang and Lin, (2007) found out that effective security policy and practice is vital for information security as only technical measures are not sufficient for this purpose. Information security awareness is more effective than other estimates ((Hagen, Albrechtsen and Hovden, 2008). One of the most appropriate tools to reach effective information security is information security training (Ma, Schmidt and Pearson, 2009). Awareness of the importance of information security with training and education positively impacts employee attitude and behaviour towards information security policy (Parsons et al., 2014). (See more: Soomoro, Shah & Ahmed, 2016).

Over the past decade, Slovenian theory has been intensively dealing with information security and related issues. It raises questions related to the Slovenian perception of cybercrime awareness and fear (the Slovenian perspective on the perception of cybercrime in terms of awareness and fear (Meško and Bernik, 2011); about the understanding of information technology users (Lobnikar et al, 2021); on the use of mobile devices among young people (Markelj and Bernik, 2011) and in Slovenian organisations (Markelj and Završnik, 2016), on modern aspects of information security (Bernik et al. 2013), like information security issues regarding smart cars (Markelj et al. 2018) and ethical hacking (Tomše and Markelj, 2020).

2. Cyber offences as legally regulated minor offences

It should be pointed out first that in the Republic of Slovenia in general minor offences are regulated in the Law of Minor Offences (2011). A minor offence is any act that represents a violation of an act, a decree adopted by the Government, or an ordinance adopted by a self-governing local community that has been determined to be a minor offence and for which a sanction for minor offences has been prescribed (Article 6 of this law).

The Law of Minor Offences governs the so-called general law on minor offences, whilst the specific part of the minor offence law is governed in numerous legislative and regulatory provisions containing descriptions of specific offences. The Law of Minor Offences as a general law (i.e., *lex generalis*) operates in accordance with the principle of subsidiarity. It is used where specific laws do not regulate statutory matters differently (i.e., *lex specialis derogat legi generali*), (Tičar and Primec, 2018). The Law of Minor Offences as a systemic law lays down the conditions applying to liability for minor offences, the imposition of sanctions for minor offences and their enforcement, minor offence proceedings, and the authorities and courts that have jurisdiction to decide on minor offences (Selinšek, 2003).

According to the first paragraph of Article 3 of the Minor Offences Act in force in the Republic of Slovenia (ZP-1, 2011), minor offences may be defined by law, a government decree, or an ordinance of a self-governing local community. This provision implies *sui generis* application of the *lex certa* principle, i.e., the principle that minor offences must be prescribed by law. Four rules must be followed when defining minor offences (Selinšek, 2003):

- *lex scripta* – minor offences may only be prescribed by law, a

government decree, or an ordinance of a self-governing local community.

- *Lex stricta* – the descriptions of minor offences must be clear and unambiguous.
- *Lex certa* – minor offences must be defined in a manner such that a challenged minor offence decision may be reviewed based on a regulation (i.e., a law, a government decree, or an ordinance of a self-governing local community); and
- *lex praevia* – regulations should always prescribe minor offences in advance; retroactivity is prohibited.

The *lex certa* principle can be defined, *mutatis mutandis*, following the European Court of Human Rights criteria in the judgment in *Sunday Times v. the United Kingdom* (Application No. 6538/74, dated 26 April 1979). In that case, the Court believed two requirements must be fulfilled to deem something "prescribed by law". For minor offences, these requirements are the following (Škrubej, 2001):

- The regulation in which a minor offence is prescribed must be adequately accessible; citizens must have access to the legal rules applicable to a given case that is adequate in the circumstances.
- A legal norm must be formulated with sufficient precision to enable citizens to regulate their conduct: they must be able – if need be, with appropriate advice – to foresee, to the degree that is reasonable in the circumstances, the possible consequences of a given action.

In accordance with the above, the Law of Minor Offences will also apply to minor offences in the field of cyber security about "general" issues: liability of the perpetrator, imposition of sanctions, minor offence proceedings, etc., whereas the provisions of special legislation, more specifically, the provisions of the Cyber Security Law and the Electronic Communications Law, will apply to the identification of an act as a minor offence. However, in accordance with the *lex specialis derogat legi* generali principle, the general provisions of the Law of Minor Offences will apply only if such issues are not regulated otherwise by the Cyber Security Law and the Electronic Communications Law.

Cyber offences are regulated by the Cyber Security Law in Chapter XI Criminal Provisions (Articles 36 to 39). Under the Cyber Security Law cyber offences are decided on within expedited proceedings and that a fine exceeding the minimum amount of a fine prescribed by this law may be imposed for them.

Two main types of proceedings for adults committing offences include offence proceedings by an offence authority (*expedited proceedings*) and ordinary court proceedings (Čas and Orel, 2016). Therefore, cyber offence proceedings for violations of the Cyber Security Law will be held before a minor offence authority and not before a court.

An offence authority is a body that supervises the implementation of a specific provision in accordance with the act defining minor offences (Čas and Orel, 2018). The Cyber Security Law stipulates that reviewing the operation of its provisions as well as the provisions of regulations adopted on the basis thereof, and the implementation of administrative decisions issued by the national competent authority shall be carried out by cyber security inspectors of the national competent authority (The Cyber Security Law, 2018, Articles 21, 22 and 31).

In accordance with the above quoted legal provision a special unit, i.e., the Cyber Society Inspectorate has been set up at the Cyber Security Administration of the Republic of Slovenia. Inspectors are persons with special powers and responsibilities. During the performance of supervision, they are obliged to observe the provisions of the Inspection Law (2007) and the provisions of sectoral regulations. Therefore, when imposing measures in the field of cyber security they are also allowed to impose measures provided for by the Cyber Security Law. The work of inspectors as minor offence authorities will begin in practice by carrying out their supervisory function if a potential minor offence is established, defined as such by the Cyber Security Law. If cyber security inspectors identify in their work a personal data breach or a suspected personal data breach, they shall notify thereof the Information commissioner for personal data protection (Cyber Security Law, 2018, Article 31). The rules on minor offence proceedings will not be dealt with in more detail, as that would be beyond the scope of our paper.

The basic rule relating to the imposition of a fine within expedited proceedings is that a minor offence authority can impose a fine within expedited proceedings irrespective of the type of decision (a minor offence decision or a penalty notice) in the amount in which it is prescribed, or the minimum prescribed fine if a scale of fines is used, unless otherwise provided for by the Act.

In addition to the general rule, the Law of Minor Offences (2011) enforced an exception relating to the imposition of a fine within expedited proceedings under which it is possible to specify by another (sectoral) law

that within expedited proceedings a fine may also be imposed whose amount exceeds the minimum prescribed fine if a scale of fines is used (Časm and Orel, 2016). The Cyber Security Law made use of that option by providing for in Article 36 that in accordance with this Act a fine for a minor offence may be imposed whose amount is higher than the lowest prescribed fine set out in this Act. As a result, the minor offence authority which is to decide on a minor offence will be given specific powers to determine the sanction (Čas and Orel, 2018), more specifically, authorisation to determine a sanction within the prescribed scale of fines (Filipič, 2018).

3. New regulation of cyber security in Slovenia

Slovenian Cyber Security Law (2018) is relatively new. It was adopted as the first systemic law related to cyber security, as until that time the area had not been regulated in Slovenia. The Government's Cyber Security Strategy (GovRS a, 2016), whose main aim was to establish an effective cyber security assurance system, which will both prevent and eliminate the consequences of security incidents in Slovenia until 2020 provided a basis for the adoption of this law. Other national and European documents also presented a commitment to adopting this law, including EU Network and Cyber Security Directive (hereinafter NIS Directive, 2016/), measures for a high common level of security of network and cyber systems across the Union which has been implemented through the Cyber Security Law (2018).

The purpose of NIS Directive (2016) was to ensure a high common level of network and cyber security by improving the security of the internet and the private networks and information systems underpinning the functioning of our societies and economies (EC, 2013, p. 2). The determination of the penalties (which must be effective, proportionate, and dissuasive) applicable to infringements of national provisions adopted pursuant to this directive falls under Member States' competence (NIS Directive, 2016, Article 21).

The Cyber Security Administration (i.e., *Uprava za informacijsko varnost*) is the highest state authority at the strategic level in the field of cyber security, which acts as a body within the Ministry of Public Administration. The Administration functions as a central coordination body at the strategic

level of the national cyber security assurance system and is a single point of contact of the state in international cooperation in this area (CWofSA, 2021).

At operational level, SI-CERT acts as the national response centre for cyber security at the Academic and Research Network of Slovenia (i.e., *ARNES*), also responsible for notification of incidents of operators of essential services, while SIGOV-CERT acts as the response centre for incidents in information systems of state administration authorities.

Furthermore, the Administration for Civil Protection and Disaster Relief of the Republic of Slovenia (i.e. *URSZR* is a special state authority as a body within the Ministry of Defence of the Republic of Slovenia) through its system for protection from natural and other disasters, the Slovene Intelligence and Security Agency (i.e., *SOVA*) in the field of counter-intelligence operations (Office of the Government of the Republic of Slovenia under the direct authority of the Prime Minister), the Police (as a body within the Ministry of the Interior) or its IT and Telecommunications Office, Criminal Police Directorate – in particular the Computer Investigation Centre with its capabilities for fighting cybercrime (GofRS b, 2016, p. 1) also play an important role.

As regards the legislation in this field, the Cyber Security Law (2018) is the most important source based on which three implementing regulations were adopted:

- Decree determining essential services and the detailed methodology for determining essential service operators (OGRS 32/2019),
- Rules on security documentation and security measures of operators of essential services (OGRS 32/2019), and
- Rules on security documentation and security measures of state administration authorities (OGRS 68/2019).

The State Administration Law (2012) provides, inter alia, that management of IT and communication systems, provision of electronic public administration services, operation of the eGovernment (i.e., *eUprava*) portal, secure boxes, etc. fall within the competence of the Ministry of Public Administration (see Article 34a of this law for more details) and introduces the duty of cooperation of all ministries and other state authorities with the Ministry of Public Administration in putting in place the information and communication systems The Decree on cyber security in the state administration (OGRS 29/2018) was adopted on the basis of this law.

Legal entities or natural persons providing public communication networks or publicly available electronic communication services (operators) are subject to specific obligations regarding security and integrity of networks and services, laid down by the Electronic Communications Law (2005) in Chapter VII (Security of Networks and Services, and Operation under Exceptional Circumstances).

The provisions of Directive 2016/1148/EC do not apply to the operators. The same logic was also followed by the Cyber Security Law by excluding the operators' obligations from its provisions. They remained regulated by the Electronic Communications Law (Government of the Republic of Slovenia, b, 2016, p. 2).

The provisions on penalties laid down by the Cyber Security Law and the Electronic Communications Law for those who violate cyber security assurance provisions are outlined below.

In the determination of a sanction, it will have to take into consideration the general rules from Article 26 of the Law of Minor Offences (2011) and the circumstances of a minor offence: gravity of the minor offence, perpetrator's negligence, or intent, mitigating and aggravating circumstances, etc. However, it will not ease the sanction and impose a fine below the prescribed amount, which would be beyond the scope of its powers from Article 36 of the Cyber Security Law (2018).

In Articles from 37 to 39, minor offences are regulated separately for different potential parties guilty of a breach of the obligations or addressees by the Cyber Security Law (paragraph one of Article 5), namely: Article 37 specifies minor offences for operators of essential services, Article 38 minor offences for digital service providers and Article 39 minor offences of state administration bodies.

4. Minor offences committed by operators of essential services.

Operators of essential services are defined in paragraph two of Article 5 of the Cyber Security Law as entities operating in the following areas: Energy, Digital infrastructure, Drinking water supply and distribution, Health care, Transport, Banking, Financial market infrastructure, Food supply and Environmental protection.

Essential services are services provided in the areas referred to above and are vital to maintaining key social and economic activities (point 1 of Article 4 of the Cyber Security Law, 2018). Moreover, the Republic of

Slovenia identified sub-areas by way of the Decree determining essential services and the detailed methodology for determining essential service operators in the areas of energy and transport. For example, in energy, the sub-areas include power, oil, and gas, and in transport, however, air, rail, water, and road transport (Article 4 of the Decree, OGRS 32/2019). The Government compiled a list of essential services in the areas mentioned above and sub-areas annexed to the Decree (OGRS, 32/2019).

Therefore, operators of essential services are entities providing (essential) services identified by the Government Decree.

Offences that they may commit, as set out in paragraph one of Article 37 of the Cyber Security Law (2018), include:

1. Failure to fulfil obligations from paragraphs one or five of Article 10 of this law (appointment of a contact person for cyber security and a substitute as well as provision of their contact details to the national competent authority; provision of changes to contact details to the national competent authority).
2. Failure to fulfil obligations from Article 11 of this law (failure to meet security requirements, e.g., identification of key, steering and monitoring information systems and parts of the network to ensure the provision of essential services, evaluation of risks and implementation of measures to control risks relating to security of networks and information systems (see Article 11 of the Cyber Security Law for more details).
3. Failure to fulfil obligations from paragraphs one, two or five of Article 12 of this law (obligation to set up and maintain security documentation; elaboration and implementation of security measures (organisation, logical-technical and technical measures); putting in place and maintaining log files on operation of own key, controlling or monitoring information systems or parts of the network for the period of six months on the territory of the Republic of Slovenia, except for the areas of digital infrastructure, banking and financial market infrastructure, for which they can be provided on the territory of the EU);
4. Failure to fulfil obligations from paragraphs one or two of Article 13 of this law (reporting incidents to SI-CERT, which may have a significant impact on continuity of essential services they provide, protection of log files or audit trails, where they exist at the time of incident reporting).

5. Failure to fulfil obligations from paragraph six of Article 14 of this law (reporting a significant impact to SI-CERT on continuity of essential services of the operator relying on a third-party digital service provider, resulting from an incident impacting the operation of the digital service provider).
6. Failure to fulfil obligations from the decision issued based on paragraph four of Article 21 of this Law (non-compliance with measures imposed on an addressee of the law by a decision of the national competent authority to prevent the continuation of a major or critical incident or in the case of a cyberattack or to eliminate its consequences).
7. Failure to fulfil obligations from the decision issued based on paragraph four of Article 22 of this law (non-compliance with measures imposed on an operator of essential services under increased threat by a decision of the national competent authority to prevent the realisation of an incident and to limit the expected consequences of a threat thereof).

A legal entity shall face a fine ranging from EUR 500 to EUR 10,000 for the offences. If a minor offence has been committed by a legal entity meeting the criteria under the Companies Law (2009) for a medium-sized or large company, the fine ranges between EUR 10,000 and EUR 50,000, while a sole trader or an individual who performs independent activities shall be fined EUR 500 to EUR 10,000.

The responsible person of a legal entity, of a sole trader or of an individual who performs independent activities shall face a fine ranging from EUR 200 to EUR 2,000. It should be noted that an essential service may also be provided by a state authority or a self-governing local community body (or another body governed by public law – paragraph three of Article 37) not held liable for a minor offence as a legal entity, which is in compliance with Article 13a of the ZP-1 excluding the liability of the Republic of Slovenia and self-governing local communities as legal persons; however, it solely permits the liability of responsible persons of state authorities and self-governing local communities, where the law so provides but not the implementing regulation (a government or a municipal decree). A fine in the same amount as that imposed on responsible persons of other types of entities, i.e., from EUR 200 to EUR 2,000 shall be imposed on responsible persons of operators of essential

services, which are state authorities or self-governing local community bodies.

5. Minor offences committed by cyber (digital) service providers.

Only two minor offences for digital service providers are defined in paragraph one of Article 38 of the Cyber Security Law:

1. Failure to fulfil obligations from paragraphs one, two or three of Article 14 of this Act (identification and adoption of appropriate technical and organisational risk management measures for security of networks and information systems in the provision of such services in the EU; adoption of appropriate measures to prevent and minimise the impact of incidents affecting the security of their networks and information systems on the services they provide in the EU and thus ensure the continuity of these services; notification of incidents to SI-CERT having a significant impact on the provision of such services provided in the EU – this obligation applies solely where the provider has access to the information needed to assess the impact of an incident);
2. Failure to fulfil obligations from the decision issued based on paragraph four of Article 21 of this Act (non-compliance with measures imposed on an addressee of the law by a decision of the national competent authority to prevent the continuation of a major or critical incident or in the case of a cyberattack or to eliminate its consequences).

In the case of both minor offences, fines are envisaged for offenders at a level corresponding to the fines set for minor offences committed by operators of essential services: a legal entity shall face a fine ranging from EUR 500 to EUR 10,000, a legal entity meeting the criteria of a medium-sized or large company in accordance with the ZGD-1 a fine from EUR 10,000 to EUR 50,000, a sole trader a fine from EUR 500 to EUR 10,000 and the responsible person of a legal entity or a sole trader a fine from EUR 200 to EUR 2,000.

6. Cyber offences committed by state authorities

Five minor/cyber offences committed by state authorities are defined in paragraph one of Article 39 of the Cyber Security Law (2018):

1. Failure to fulfil obligations from Article 16 of this law (put in place risk management measures on the basis of a risk assessment for security of information systems and parts of the network operated by them; taking the necessary measures to prevent and minimise the impact of incidents affecting the security of networks and information systems of state authorities so as to ensure the continuity of services provided by state authorities; establish the necessary security requirements for specific key parts of a national security system if they draw data from this system);
2. Failure to fulfil obligations from paragraphs one, two or five of Article 17 of this law (establishment and maintenance of a documented system of cyber security management and business continuity management system; elaboration and implementation of the necessary security measures (organisation, logical-technical and technical measures); putting in place and maintaining log files on operation of own information systems or parts of the network for the period of six months on the territory of the Republic of Slovenia);
3. Failure to fulfil obligations from paragraphs one or two of Article 18 of this law (reporting incidents to SI-CERT or to the national competent authority, which may have a significant impact on continuity of services provided by state authorities, where incidents are detected by state authorities having their own capabilities at least at the level of a security operations centre; adequate protection of log files or audit trails at the time of incident reporting).
4. Failure to fulfil obligations from the decision issued based on paragraph four of Article 21 of this law (non-compliance with measures imposed on the addressee of the law by a decision of the national competent authority to prevent the continuation of a major or critical incident or in the case of a cyberattack or to eliminate its consequences).
5. Failure to fulfil obligations from the decision issued based on paragraph four of Article 22 of this law (non-compliance with measures imposed on a state authority managing the information systems under an increased threat by a decision of the national competent authority to prevent the realisation of an incident and to limit the expected consequences of a threat thereof).

As already noted above, responsible persons of a state authority may solely be fined for minor offences committed by state authorities. The

amount of the fine for the responsible person envisaged for the minor offences committed by state authorities ranges from EUR 200 to EUR 2,000, i.e., it is the same as in the case of minor offences committed by responsible persons of operators of essential services and of digital service providers.

7. Communication offences under Slovenian communication legislation

The Agency for Communication Networks and Services of the Republic of Slovenia (hereinafter: Agency) shall monitor the implementation of the provisions of the Electronic Communications Law and regulations and general acts issued pursuant to this law, except in cases within the competence of the Cyber Commissioner in accordance with Articles 155 and 157 of the Electronic Communications Law (2005).

The minor offence authorities competent to decide on offences involving violations of the Electronic Communications Law and regulations issued pursuant thereto include the Agency and the Cyber Commissioner. They decide in accordance with the provisions of the Law of Minor Offences (2011), each in the relevant area of supervision. The minor offence proceedings shall be conducted using an expedited procedure. An offender may face a fine the amount of which exceeds the minimum prescribed fine for a specific minor offence.

The Electronic Communications Law (2005) contains penalty provisions in Articles 232 to 236. Minor offences are referred to in specific articles regarding the gravity of the minor offence and the status of the offender. The most stringent sanctions are envisaged for minor offences committed by operators having significant market power. In accordance with the provisions of paragraph one of Article 232, legal entities, sole traders, or individuals who perform independent activities shall be fined up to five percent of the annual turnover generated in the relevant market in the preceding financial year for any minor offence referred to in the same article, whereas the responsible person of the offender shall face a fine ranging from EUR 1,000 to EUR 10,000.

These are followed by offences, subject to relatively high penalties ranging from EUR 50,000 to EUR 400,000, committed by legal entities meeting the criteria for a medium-sized or large company under the Companies Law (2009), whereas their responsible persons shall face a fine ranging from EUR 500 to EUR 10,000. Legal entities not meeting the criteria for medium-sized companies in accordance with the Companies Law

(micro and small enterprises), sole traders or individuals who perform independent activities shall face a fine ranging from EUR 1,000 to EUR 20,000 for the same minor offences, and their responsible persons a fine ranging from EUR 500 to EUR 10,000 (paragraphs two and three of Article 233 of the Electronic Communications Law, 2005).

This specific category covering as many as 85 offences comprises those related to the area of cyber security presented below, which may be committed by a legal entity, a sole trader, or a self-employed individual who: - fails to take appropriate technical and organisational measures to appropriately manage network and service security risks (paragraph one of Article 79), - fails to take the necessary measures to ensure the integrity of their networks (Article 80), - fails to notify the Agency of any breach of security or integrity (paragraph one of Article 81), - fails to provide the information necessary for the assessment of security or integrity of their services and networks or fails to allow a security audit to be carried out at their expense by a qualified independent organisation (Article 82), - fails to take appropriate technical and organisational measures to ensure the protection of their network and services (paragraph one of Article 145),- fails to take measures to ensure a level of security and protection appropriate to the envisaged risks and costs and in line with technical and technological development (paragraph two of Article 145), - fails to notify the users of any special risks to network security or services immediately upon learning of such risks or fails to inform them of all possible means to eliminate the risk, including an indication of likely costs, or does not enable rapid and effective access to protective measures to users (paragraph one of Article 146).

8. Administrative violations

The 2016 amendment to the Law of Minor Offences (2011) provided a legal basis in paragraph three of Article 1 of this law for the introduction of a special (third) type of prohibited conduct, i.e., administrative violations (GofRS c, 2016, p.14) to be regulated in accordance with the regulations from more strictly regulated sectors:

- regulations governing protection of competition (Prevention of Restriction of Competition Law, 2008),
- insurance supervision (Insurance Law, 2015),
- securities market (Market in Financial Instruments Law, 2018),

- anti-money laundering (Prevention of Money Laundering and Terrorist Financing Law, 2018) and
- banking supervision (Banking Law, 2015),

which fall within the competence of central regulatory bodies in the country: Competition Protection Agency (*i.e., AVK*), Securities Market Agency (*i.e., ATVP*), Insurance Supervision Agency (i.*e., AZN*), National Bank (*i.e., Banka Slovenije*) and Office for Money Laundering Prevention (*i.e., UPPD*), which may be regarded, in a broad sense, as sectors essential to the operation of financial markets (Tičar and Primec, 2018).

If compared with the other two types of unlawful conduct (criminal offences and minor offences), a characteristic of administrative violations is that they may be committed solely by legal entities with no reference to liability of direct offenders or responsible persons. Therefore, legal entities shall be held liable for infringements in accordance with the strict liability principle, i.e., liability without fault (intent and negligence) that must be proved in cases of liability of natural persons. Financial penalties of high amounts are laid down for offenders having mainly a preventative effect in the regulated sectors.

The Cyber Security Law (2018) and Electronic Communications Law (2005) do not stipulate any administrative violations.

9. Discussion and conclusion

The first law, which fully regulated cyber security in the Republic of Slovenia, was the Cyber Security Act from 2018. In addition to providing a complete set of rules relating to cyber security and ensuring a high level of security of network and information systems in the country, the purpose of the Act is to lay down security requirements and obligations of the addressees of the law to notify the incidents. The addressees of the law, required to comply with the provisions of the Cyber Security Law, are operators of essential services, digital service providers and state administration authorities managing the information systems. Moreover, public communication networks and publicly available electronic communication services, excluded from the Cyber Security Law as provided for by Directive 2016/1148/EC, and regulated in the Electronic Communications Law (2005), constitute an important part of information networks and systems.

A more in-depth analysis of the penalty provisions of the Cyber Security Law and Electronic Communications Law (in particular the provisions relating to the violations of Chapter VII of the Act) shows that similar offences are defined in both laws as key offences committed by the addresses of the law under the Cyber Security Law or operators under the Electronic Communications Law as a result of their failure to meet key security requirements (e.g. failure to adopt technical and organisational measures to manage network and service security risks, and prevent or reduce the impact of incidents, which should be proportionate to the probable risks) and their failure to meet the incident notification obligation.

Under both acts, minor offence proceedings are conducted using an expedited procedure, whereby the amount of a fine imposed on an offender may be higher than that indicated as the minimum fine for an individual offence, departing in this way from the general rule under the Law of Minor Offences (2011) stipulating that within the framework of expedited proceedings an offender shall be imposed the lowest fine prescribed if a scale of penalties is applied. In order to determine the sanction for a minor offence relating to cyber security, a minor offence authority (inspector) will take into consideration general rules applying to the determination of a sanction from Article 26 of the Law of Minor Offences (2011) and the levels of the prescribed scale of penalties for specific minor offences under the Cyber Security Law (2018) and Electronic Communications Law (2005), thus being able to impose, based on the power set out in both (special) laws, a fine whose amount will exceed the minimum prescribed level.

A legal entity (or another legal form: a sole trader or an individual who performs independent activities) shall be punished as a perpetrator or a responsible person of the entities, except for state authorities which are not held liable as legal entities in accordance with the Law of Minor Offences (2011, Article 13a) for minor offences. Their responsible persons shall solely be punished (Article 39 of the Cyber Security Law).

It is important to point out the difference in the level of fines, which is considerably higher for minor offences under the Electronic Communications Law (2005) than for minor offences under the Cyber Security Law (2018). For example, a fine imposed on an offender under the Cyber Security Law (2018), a legal entity meeting the criteria for medium-sized or large companies according to the ZGD-1, may range from EUR 10,000 to EUR 50,000. The fine imposed on an offender, which is also a legal entity (a medium-sized or large

company following the criteria laid down in the ZGD-1) from EUR 50,000 to EUR 400,000, indicating how important it is to ensure the secure operation of public communication networks and prevent any disruptions in the provision of publicly available electronic communication services.

As stated in the previous paragraph, a fine exceeding its lowest prescribed level may be imposed on an offender even though the minor offence proceedings are conducted using an expedited procedure and a scale of fines is prescribed, which seems justified because of the massive growth in volumes of sensitive data (confidential information, trade secrets, personal data, etc.) on the internet (Planinšek and Skok, 2018) and the cyberattacks becoming part of our everyday lives. According to the SI-CERT data, the number of cyber incidents in the Republic of Slovenia has increased in recent years. The figures on specific types of incidents show a considerable increase in corporate fraud, with the so-called phishing scams being prevalent. Simultaneously, the number of intrusions has gone down (see SI-CERT, 2020, for more details).

List of References

Banking Law, (2015), "Zakon o bančništvu, ZBan-2", Official Gazette of the Republic of Slovenia, No. 25/15 et seq.

Bernik, I. et al, (2013), "*Sodobni aspekti informacijske varnosti*"; urednika Bernik, I., Markelj. B. Ljubljana: Fakulteta za varnostne vede.

Chang, S. E. & Lin, C., (2007), »Exploring organizational culture for information security management«. *Industrial Management & Data Systems*, 107(3), 438-458.

Čas P. & Orel N., (2018), "Zakon o prekrških (ZP-1) s komentarjem in upoštevanimi spremembami do novele ZP-1J". Ljubljana: Lexpera, GV Založba.

Companies Law, (2009), "Zakon o gospodarskih družbah, ZGD-1", Official Gazette of the Republic of Slovenia, No. 65/09 et seq.

CWofSA, (2021), Available from: https://www.gov.si/teme/informacijska-varnost/ (Accessed 12 February 2021).

Cyber Security Law, (2019), "Zakon o informacijski varnosti, ZInfV", Official Gazette of the Republic of Slovenia, No. 39/19.

European Commission, (2013), "Proposal of NIS Directive", https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52013PC0048&from=sl (Accessed 28. July 2020).

Electronic Communications Law, (2005), "Zakon o elektronskih komunikacijah, ZEkom-1", Official Gazette of the Republic of Slovenia, No. 113/05 et seq.

ENISA (2020). "Threat Landscape 2020", https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (Accessed 8. March 2021).

European Court of Human Rights in the judgment in *Sunday Times v. the United Kingdom,* Application No. 6538/74, dated 26 April 1979.

Filipič K., (2018), "Zakon o prekrških (ZP-1) s komentarjem in upoštevanimi spremembami do novele ZP-1J", Ljubljana: Lexpera, GV Založba.

GofRS a, (2016), "Government's Cyber Security Strategy", Vlada RS. https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf (Accessed 28. July 2020).

GofRS b, (2016), "Predlog zakona o informacijski varnosti". https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=8587 (Accessed 5.August 2020).

GofRS c, (2016), "Predlog Zakona o spremembah in dopolnitvah Zakona o prekrških ZP-1J", http://vrs-3.vlada.si/MANDAT14/VLADNAGRADIVA.NSF/18a6b9887c33a0bdc12570e50034eb54/1d31e571387b9809c1257f6400269369/$FILE/ZP-1J_VG_st_1.pdf (Accessed 5. August 2020).

Hagen, J. M., Albrechtsen, E., Hovden, J., (2008), »Implementation and effectiveness of organizational information security measures«. *Information Management & Computer Security*, 16(4), 377-397.

Inspection Law, (2007), "Zakon o inšpekcijskem nadzoru, ZIN", Official Gazette of the Republic of Slovenia, No. 40/07 et seq.

Insurance Law, (2015), "Zakon o zavarovalništvu, ZZavar-1", Official Gazette of the Republic of Slovenia, No. 93/15 et seq.

Law of Minor Offences, (2011), "Zakon o prekrških, ZP-1", Official Gazette of the Republic of Slovenia, No. 29/11 et seq.

Lobnikar, B., Prislan, K., Markelj, B. & Banaturi, E., (2012), "Informacijsko-varnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji", *Varstvoslovje* 14, št. 3, 345-363.

Ma, Q., Schmidt, M. B., & Pearson, J. M., (2009), »An integrated framework for information security management«, *Review of Business*, 30(1), 58-69.

Markelj, B. & Bernik, I., (2011), "Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav." *Zbornik 18. konference Dnevi slovenske informatike* (7 str.). Ljubljana: Slovensko društvo Informatika.

Markelj, B., Školc, G., Erčulj, I.V. & Zgaga, S., (2018), "Pametni avtomobili in kibernetska kriminaliteta". *Revija za kriminalistiko in kriminologijo*, 69(3), 215-231.

Markelj, B. & Završnik, A., (2016), "Kibernetska korporativna varnost mobilnih naprav: Zavedanje uporabnikov v Sloveniji", *Revija za kriminalistiko in kriminologijo*, 67(1), 44–60.

Market in Financial Instruments Law, (2018), "Zakon o trgu finančnih instrumentov, ZTFI", Official Gazette of the Republic of Slovenia, No. 77/18 et seq.

Meško, G., (2018), "On Some Aspects of Cybercrime and Cybervictimization", *European Journal of Crime, Criminal Lae and Criminal Justice* 26, 189-199.

Meško, G. & Bernik, I., (2011), "Cybercrime: Awareness and fear: Slovenian perspectives". *European intelligence and security informatics conference* (str. 28– 33). Atene: IEEE Computer Society Press.

NIS Directive, (2016), "Directive 2016/1148/EC of the European Parliament and of the Council of 6 July 2016", Official Journal of the EU 194/2016.

OGRS 29/2018, (2018), "The Decree on cyber security in the state administration", Official Gazette of the Republic of Slovenia, No. 29/18.

OGRS, 39/2019, (2019), "Decree determining essential services and the detailed methodology for determining essential service operators", Official Gazette of the Republic of Slovenia, No. 39/19.

OGRS 39/2019a, (2019). "Rules on security documentation and security measures of operators of essential services", Official Gazette of the Republic of Slovenia, No. 32/19

OGRS 39/2019b, (2019), "Rules on security documentation and security measures of state administration authorities", Official Gazette of the Republic of Slovenia, No. 32/19

Orel N. & Čas P., (2017), "Materialnopravna ureditev prava prekrškov, postopek o prekršku, praktična uporaba materialnopravnih določb in postopka iz ZP-1", Ministrstvo za javno upravo, https://ua.gov.si/media/1317/u%C4%8Dno-gradivo-prekr%C5%A1ki-_%C4%8Das_orel.pdf (Accessed 5. August 2020).

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C., (2014), »Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)«. *Computers & Security*, 42, 165-176.

Planinšek J. & Skok T., (2018), "Pravni vidiki kibernetske varnosti (1. del)", *Pravna praksa, št. 7*, 2019, str. 16-18.

Prevention of Money Laundering and Terrorist Financing Law, (2016), "Zakon o preprečevanju pranja denarja in financiranja terorizma, ZPPDFT-1", Official Gazette of the Republic of Slovenia, No. 68/16 et seq.

Prevention of Restriction of Competition Law, (2008, "Zakon preprečevanju omejevanja konkurence obsega, ZPOmK-1", Official Gazette of the Republic of Slovenia, No. 36/08 et seq.

Selinšek L., (2003), "Predpisovanje prekrškov v odlokih samoupravnih lokalnih skupnosti skladno z ZP-1". *Lex localis, 1*(3), 103-119.

SI-CERT, (2020), "Report on cyber security 2019", https://www.cert.si/wp-content/uploads/2020/07/Poro%C4%8Dilo-o-kibernetski-varnosti_2019_.pdf (Accessed 6.August 2020).

Soomoro, Z., Shah, M. & Ahmed, J., (2016), »Information security management needs more holistic approach«. *International Journal of Information Management* 36 (2), 215-225.

Škrubej, K., (2001), "Jezik prava kot socialnovrednostni privilegij", *Podjetje in delo* 6-7/2001, Ljubljana p. 1179.

Tičar B. & Primec A., (2018), "Pravna ureditev prekrškov in administrativnih kršitev v gospodarstvu (de lege lata)", *Gospodarski subjekti na trgu in evropske dimenzije, Portorož, 17. do 19. maj 2018*. Maribor: Pravna fakulteta.

Tomše, S. & Markelj, B., (2020), "*Informacijska varnost: Etično hekanje*", Ljubljana: GV Založba.