Post-Soviet Estonia's information safety: lessons for Ukraine

Volodymyr I. Rozvadovsky*,
Liubomyr V. Zinych and Andriy A. Albu

Department of Constitutional, International and Administrative Law,
Vasyl Stefanyk Precarpathian National University,
Ivano-Frankivsk, Ukraine

*Corresponding author

Abstract: The relevance of the article lies in the fact that in the conditions of intensive expansion of information flow information security has become the least protected element of national security, especially in Ukraine. The purpose of the research is to study the effectiveness of the activity of state bodies, to analyse regulatory acts of the Republic of Estonia and to determine the possibility of their adaptation in Ukraine. The features of information security in the Republic of Estonia are considered in the article. It is noted that the main factors that have helped to increase the level of information security in Estonia are the developed information infrastructure, effective cybersecurity policy and reliable protection of personal data. Cybersecurity has been found to depend on combating cybercrime, improving critical infrastructure and e-services, and providing national defence. Practical recommendations are given regarding Ukraine's acquisition of Estonia's experience in the field of information security.

Keywords: information security; cyber security; information infrastructure; personal data; legal mechanisms.

Reference to this paper should be made as follows: Rozvadovsky, V.I., Zinych, L.V. and Albu, A.A. (2021) 'Post-Soviet Estonia's information safety: lessons for Ukraine', *Int. J. Electronic Security and Digital Forensics*, Vol. 13, No. 1, pp.53–63.

Biographical notes: Volodymyr I. Rozvadovsky has a PhD in Legal Sciences, Associate Professor and Head of the Department of Constitutional, International and Administrative Law, Educational and Scientific Law Institute of Precarpathian National University named after V. Stefanyk. His research interests is constitutional and legal aspects of the implementation of the powers of the Chairman of the Supreme Council of Ukraine in relations with public authorities; the development strategy of constitutionalism in Ukraine, constitutional, municipal law, the establishment of the institution of constitutional justice and jurisdiction, and the problems of decentralisation of local governments.

Liubomyr V. Zinych has a PhD in Legal Sciences, and a lecturer at the Educational and Scientific Law Institute of the Precarpathian National University named after V. Stefanyk. In 2013–2014, he graduated Educational and Scientific Law Institute of Precarpathian National University named after

V. Stefanyk, specialty ‘jurisprudence’, educational degree and ‘Master’, qualification ‘Lawyer Lecturer of Law’. In 2017, he defended a PhD thesis on specialty civil law and civil procedure.

Andriy A. Albu has a PhD in Legal Sciences, and a lecturer at the Educational and Scientific Law Institute of Precarpathian National University named after V. Stefanyk. In 2006–2011, he graduated from the Educational and Scientific Law Institute of Precarpathian National University named after V. Stefanyk with a specialty ‘jurisprudence’ and qualification ‘lawyer, teacher of law’. In 2016, he defended a PhD thesis on specialty civil law.

1 Introduction

The current realities of the development of information processes in the world demonstrate that information security is as important a component of national security as economic, military or political. In the conditions of intensive expansion of information flow, increase of information exchange facilities, waging of information wars, information security has become the least protected element of national security. Solving this issue remains a priority for the entire international community. Among the European Union countries, one of the most advanced and active in information policies is the Republic of Estonia. The Republic of Estonia leads Europe in the provision of public digital services. The national communications and transactions platform allows for 21st century governance by allowing transparency, e-security (inter alia privacy), e-security, entrepreneurship and, among other things, rising levels of prosperity, and well-being for all its citizens (Priisalu and Ottis, 2017; Li et al., 2019).

Ukraine and Estonia, as post-Soviet countries, have maintained bilateral friendly relations since independence in 1991. Ukraine and Estonia have similar views on the current problems of European and global security, common aspirations in the political, economic, social and other spheres (Embassy of Ukraine in the Republic of Estonia, https://estonia.mfa.gov.ua/ua). In addition, the experience of Estonia is extremely important for Ukraine because Estonia successfully confronts information aggression by the Russian Federation, but is significantly smaller in terms of territory and the amount of human and natural resources. First steps towards cooperation on interaction and exchange of experience in the field of cyberattack neutralisation are made between Ukraine and Estonia. The Republic of Estonia has also been a member of the North Atlantic Treaty Organization (NATO) since March 29, 2004, which is Ukraine’s strategic course.

For years, Estonia has been at the forefront of cybersecurity internationally. The NATO Cooperative Cyber Defense Center of Excellence (CCD CoE) and the EU Agency for Large-Scale IT Systems (EU-LISA) are both based in Tallinn. A number of influential international agreements that have been approved here in Tallinn (Ministry of Foreign Affairs of the Republic of Estonia, 2018). Despite the fact that Estonia and Ukraine have common information threats, it should be borne in mind that Estonia has taken its own path to information security. Many years of its experience demonstrate that protecting the information space requires the development of a comprehensive public policy in this area. Therefore, in our opinion, it is necessary to study the effectiveness of the activity of state bodies, to analyse regulatory acts and to determine the possibility of their adaptation in Ukraine. This article is devoted to the study of these features of information security.

The current state of information security of Ukraine is largely inconsistent with the level of security of information-protected countries, in particular Estonia. The critical state of cybersecurity, the underdeveloped information infrastructure system, the imperfect protection of personal data and a number of other issues lead to a detailed analysis of the legal aspects of Estonia's information security and an analysis of the possibility of borrowing this experience for Ukraine.

Information security issues and their components in relation to today's challenges and necessity have not been explored enough. The current state of development of this topic indicates that there is no consensus among scientists about the essence of information security, reinforces this fact that the definition in international instruments is also quite diverse. We emphasise that the state of information security in any state is rather unstable, since it depends on many factors, which may include socio-political events, economic and social state of society, so ensuring information security is a constant task (Roy and Das, 2017). Particular attention is paid to cyber security by Estonian scientists, which has become a major means of waging information wars. Estonia has powerful scientific security training schools, and Estonia's numerous scientific and practical projects, in conjunction with NATO and the European Union, have allowed the development of cyber-attack counteraction concepts. In the field of personal data, scientists have a vision that, in addition to privacy and security, there is a need to create a market for private data, where companies can offer leases/licensing of their data for future financial, advertising and other services, which is quite promising today (Lu et al., 2020; Chadwick et al., 2020).

Information security analysis in the Republic of Estonia was carried out by using general scientific and social-scientific research methods. These methods made it possible to find out the peculiarities, legal mechanisms of formation and activity of state bodies in the Republic of Estonia. In particular, the comparative method and the system analysis method were used. Using the comparative legal method, a comparison of legislation and scientific views of national and foreign scientists on information security was made. The systematic analysis method has revealed the problematic issues in the legislation of Ukraine and substantiated the possibility of borrowing Estonia's experience in the field of information security (Gheitasi et al., 2019).

2 A modern approach to protecting information security in Estonia

Information security is a concept that has been introduced into the scientific circulation for a long time, however, with the development of technologies has become especially relevant. The impetus for the active deployment of information security technologies were the Russian cyber-attacks on Estonian information resources in 2007. Estonia, as a country with a developed e-society, has, in a few years, formed a model of e-governance less vulnerable to external influence. Today in Estonia, the legal regulation of information security is carried out by the Constitution of Estonia, the Law 'On Public Information', the Law 'On Protection of Private Data', the Law 'On State Secrets and Classification of Foreign Information', the Law on Cybersecurity, the Cybersecurity Strategy for 2019–2022.

The Constitution of Estonia provides in § 44 for "Everyone is entitled to free access to information disseminated for public use". Pursuant to a procedure provided by law, all government agencies, local authorities, and their officials have a duty to provide information about their activities to any citizen of Estonia at his or her request, except for information whose disclosure is prohibited by law and information intended exclusively for internal use. Pursuant to a procedure provided by law, any citizen of Estonia is entitled to access information about himself or herself held by government agencies and local authorities and in government and local authority archives. This right may be circumscribed against the law to protect the rights and freedoms of others, to protect the confidentiality of a child's filiation, and in the interests of preventing a criminal offence, apprehending the offender, or of ascertaining the truths in a criminal case (The Constitution of the Republic of Estonia, 1992).

Restrictions on access to information established by the Estonian Constitution are indirectly aimed at ensuring information security, since the protection of private data and state secrets are considered as components of information security. Justifying the restriction on access to information, it should be noted that international law recognises that a State may exclude certain limited information from the category of general property that would disrupt the interests that the State may legitimately protect. These include, in particular, national security interests requiring that certain information must be 'secret' (i.e., so that it is known to several government or military representatives) for a limited time. However, these restrictions should always be such that democratic society cannot do without and satisfy the criterion.

Public interest, which means that they are always temporary (i.e., they are introduced only for a limited period) and the information will eventually become available to the general public (Nesterenko, 2012). Estonia's Law on 'Public Information' does not contain the term 'information security' and the term information security is used in § 43 'Protection of internal information':

1 A holder of information shall apply administrative and technical measures to ensure that information to which a restriction on access applies cannot be accessed by persons who do not have the right of access.

2 If a restriction on access applies to a document prepared on a computer, the person who prepares the document shall verify that the measures have been taken by the agency to secure the processing of data in order to restrict access' (Public Information Act, 2001).

The Cyber Space Protection Strategy in the Republic of Estonia emphasises the need to create a secure cyber space as a whole and focuses on information systems. The strategy is based on measures of a civilian nature, it is recommended to focus on regulation, education and cooperation. It is worth noting that both Ukrainian and Estonian scholars today do not have a consensus on understanding this concept. There are several approaches to defining the essence of information security, which are understood by the latter: the state of information space security; the process of threat and threat management, which ensures information sovereignty of Ukraine; state of protection of national interests of the country in the information environment or in the information sphere; security of the rules established by law, according to which information processes take place in the state; public relations related to the protection of vital interests of the individual and the citizen, society and the state against real and potential threats in the information space; an integral part of political, economic, defence and other components of national security (Lipkan, 2006).

Providing information security has become a global task and therefore is a subject to legal regulation not only in the laws of individual states, but also in international law. With regard to international instruments, including that Estonia is a member of NATO, the term 'classified information' is used in the acts of this organisation to refer to information sensitive to threats arising from unauthorised access, and therefore needs protection or at least restriction of access to it [Document C-V. 49: Security within the North Atlantic Treaty Organization (NATO), 2002]. Important in the context of information security of the state is the understanding of the essence of international information security. Today, international information security is understood to mean a state ensured by generally recognised and special principles and rules of international law, which includes violations of international peace and security of both individual states and the world community as a whole in the field of information and communication (Gritsun, 2016).

The laws of other countries often use the two terms 'security of information' and 'information security'. Researchers in the field of information security distinguish between security of Information and information security as follows, information security is much deeper in substance and wider in content. Information security can be viewed from the standpoint of protecting not only the interests of the state, but above all the individual and society (Voloshina, 2010). Therefore, having analysed the legislation and scientific views on information security, we believe that information security is a state of information safety in systems and applications which preserves data integrity and confidentiality, and resistance to external influences.

3 Security of the information environment as the main principle of activity of the legislative bodies of the Republic of Estonia

Providing information security is the main task of specialised state entities. The main body of information security is The Ministry of Economy and Communications of the Republic of Estonia and the Ministry of Internal Affairs of Estonia, which together with the Cyber Defense Unit of the Defense League, International Center for Defense Studies, Estonian Information System's Authority, provide cyber security to Estonia. Among the non-governmental organisations, the Estonian Association of Information Technology and Telecommunications (officially abbreviated as ITL) is a voluntary organisation whose primary objective is to unite the Estonian information technology and telecommunications companies and organisations to promote their cooperation in Estonia's development towards information society, to represent and protect the interests of its member companies and to express their common positions (ITL Estonia, https://www.itl.ee/index.php?page=181).

In Estonia, the enforcement of the Law on Public Information was entrusted to the Data Protection Inspectorate of the Ministry of Justice of Estonia. The legal status of the latter is determined by the law 'on protection of personal data' and 'public information'. The Inspection focuses more on the protection of personal data than the protection of the right of access to 'public information'. The responsibility of the inspectorate is to:

1 carry out state oversight of information providers on issues related to fulfilling information requests and disclosure of information

2 breach of supervisory proceedings on the basis of an appeal or on his own initiative.

Estonian citizens confirm the effectiveness of the Inspectorate's activity with regard to the ability to quickly add, modify or delete personal data about an individual that he or she wishes to distribute. A special place in information security belongs to the Computer Incident Response Center (hereinafter – CERT). CERT Estonia was established in 2006 as a specialised organisation that responds to computer incidents, assists users in reducing the negative consequences and takes safe measures when threatened.

The peculiarity of CERT is that this organisation does not work with users. In case of an incident, the user should contact a service provider, network administrator, or customer support. The objectives of CERT are:

a to identify the least secure elements in systems and applications

b providing assistance in the event of an incident

c coordination and response to an incident.

The result of Computer Emergency Response Team for Estonia (CERT-EE) was the detection in 2018 of a threat to collect and send to the Russian Federation servers personal data of Estonian citizens when using the Yandex Taxi application. As is known in Russia, the requirements of the European Union regarding personal data are not applied, and this makes it possible to use this data by special services (Yandex Taxi to Introduce App-Based Ride Ordering Service in Tallinn, 2018).

Considering the different models of information management, it is worth considering the experience of the countries where the Ombudsman or Commissioner for Information has been introduced. Canada's Information Commissioner, for example, controls the implementation of the Access to Information Act in Canada. In general, the Information Commissioner model introduced in Canada is considered to be a very effective tool in protecting the right of access to information. This is manifested both in the efficiency of the consideration of cases by the information commissioner, as well as in the development of its recommendations for state institutions, as well as recommendations on the need for further reform of information legislation (Nesterenko, 2012).

In this regard, Ukrainian scientists note that the introduction of the Commissioner Institute is very complicated, since the Constitution does not provide for the possibility of creating specialised ombudsmen. Therefore, to create this institute it is necessary to amend the Constitution of Ukraine. Today the Institute of Information Commissioner is only at the stage of its formation, so it is considered expedient to introduce the position of representative The Commissioner for Human Rights, who will deal with the protection and protection of information rights (Razumkov, 2018). The effectiveness of the activities of special bodies for monitoring compliance with the right of access to public information within the executive branch is evaluated by experts in different ways. Discussions about their real independence in their activities and decision-making are ongoing. The information security model established in Estonia has proven to be effective and efficient, and the fact that all public authorities and private entities interact with each other to prevent and overcome negative consequences is relevant.

4 Fundamental cybersecurity features in Estonia

According to the latest data from the National Cybersecurity Index of Europe submitted by the Estonian Academy of Electronic Governance, Estonia ranks first in Europe in the capacities of cyber threat analysis and information, contribution to global cyber security, protection of digital services, protection of personal data, cyber incidents report, cyber crisis management, and military cyber operations, the index team said on its website (Estonia Ranks First in the World in the National Cyber Security Index, 2018).

According to the European Union's cybersecurity strategy, cybersecurity is the safeguards and actions used to protect cyberspace from both civilian and military points of view from threats that could be adversely affected or could harm its interconnected networks and information infrastructure. Cybersecurity is intended to preserve the integrity and accessibility of networks and infrastructure, as well as the confidentiality of information contained therein to ensure its accessibility, integrity, authenticity, confidentiality and falsity (DOD Dictionary of Military and Associated Terms, 2017). The Cybersecurity Law applies in Estonia (1) (Cybersecurity Act, 2018). This Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents (Personal Data Protection Act, 2018).

§7. Security measures of service provider's system:

1. A service provider shall permanently apply organisational, physical and information technological security measures:
   - For preventing cyber incidents
   - for resolving cyber incidents
   - for preventing and mitigating an impact on the continuity of the service or the security of the system due to a cyber incident or for preventing and mitigating a possible impact on the continuity of another dependant service or the security of a system.
2. Upon the application of security measures, the service provider is required to:
   - prepare a system risk assessment in which they shall set out a list of risks affecting the security of the system and the continuity of the service and causing the occurrence of cyber incidents, determine the severity of consequences of a cyber incident occurring upon the realisation of risks, and describe the measures for resolving a cyber incident
   - ensure the existence and timeliness of a documented system risk assessment, security regulations and description of the application of security measures
   - ensure the monitoring of the system for detecting actions or software compromising its security and communicate information about the actions or software compromising the security of the system to the Estonian Information System Authority
   - take measures for reducing the impact and spread of a cyber incident, including restriction of the use of or access to the system, if necessary
   - check the sufficiency and compliance of the application of security measures and document the results
   - preserve the documents provided for in clause 5 of this subsection no less than three years as of the creation thereof.

3 If the service provider authorises another party to administer the system or uses another party to host the system, the service provider is responsible for the application of the security measures of the system by the other party.

4 The description of the security measures of the system used for the provision of a service and the requirements for the preparation of a risk assessment shall be established by a regulation of the minister responsible for the area.

Estonia is undertaking cyber security efforts in areas such as combating cybercrime, developing critical infrastructure and e-services, and enhancing national security. The worldwide trend today is to create cyber police units and Computer Incident Response Centers in countries, the main task of which is to combat cyber crime. Authors believes that in order to implement cyber security measures it is necessary to strengthen the responsibility for both administrative and criminal responsibility for information offenses. In addition to the detailed legal regulation, the NATO-EU Joint Coordination Organisations, which include the NATO Joint Cyber Security Center of Excellence, the European Agency for the Operational Management of Large IT Systems and others to prevent cyber attacks in Estonia, play an important role. Estonian experts are also testing vulnerability to cyber attacks and modeling the hacking process, as well as developing more sophisticated software and hardware for detecting cyber attacks.

5 Estonian legal system regarding the protection of personal data

The success of Estonia in the protection of personal data is undeniable, as evidenced by the development of the concept of opening the world's first Embassies of data in foreign countries. The protection of personal data is carried out by the Law of the Republic of Estonia on Personal Data Protection (2007), Regulation (EU) 2016/679 of the European Parliament and of the Council, Directive 95/46/EC (General Data Protection Regulation).

The authority in charge of data protection in Estonia is the Estonian Data Protection Inspectorate. The legislation regulates the powers in detail, rights and responsibilities of the controller. It is important that the owner of the personal data has legal capacity to prevent the dissemination, misrepresentation of his personal data, and this is not least guaranteed by clear rights and duties of the controller of personal data. Also, in special cases, law enforcement agencies have the right to appoint a data protection specialist under a service agreement to protect important information.

Tasks of data protection: A data protection specialist shall perform at least the following tasks:

1 inform and advise the law enforcement authority and officials and employees who process personal data on behalf of the latter in connection with their obligations under this Acts and other data protection standards of the European Union or its member states

2 ensure consistency with this Act, if necessary, with data protection standards of the European Union or its member states and internal controller policies that concern the principles of personal data protection and awareness-raising and training of officials and employees involved in processing of personal data

3 provide advice as to the data protection impact assessment and monitor its performance pursuant to § 38 of this Act

4 cooperate with the Estonian Data Protection Inspectorate

5 act as the contact person in the issues of personal data processing for the Estonian Data Protection Inspectorate, including in the course of the earlier consultation.

In the scientific literature of Jaan Priisalu, Rain Ottis explains the need to create a private data market in Estonia. One possible solution is to organise the enterprise data market, where companies and researchers are able to present data use and licensing/rental/sales related proposals, assign pricing models, where patients are then able to choose to either license, rent, sell or to withdraw their data from use (Priisalu and Ottis, 2017). Authors believes that this proposal is promising and will be implemented in the future in Estonia and other European countries.

6 Factors of creating information security using the example of Estonian experience

Having analysed the experience of the Republic of Estonia in information security, there are several factors that have formed the basis for the creation of a secure information environment. Firstly, only a comprehensive information policy enables the security of enterprises, institutions, organisations and the state as a whole. At the same time, the developed system of 'e-society' in Estonia has made it necessary for the participation of practically all state bodies in providing information security through compliance with technical, legal and organisational requirements. Within the framework of information policy, the large-scale interaction of the state with private structures plays an important role, which has helped to attract the latest information security technologies. As a result, information security has become a matter for the entire Estonian society.

Secondly, Estonia has made every effort to ensure cyber security (as a component of information security) and has created favourable conditions for the arrival of foreign IT companies with significant capital and innovations. As a result, the state received new economic and technological revenues. Estonia's cyber security is driven by efficient cryptographic and software systems. In Estonia, cyber-attack vulnerability testing and hacking simulation technology are used by experts to increase security and prevent cyber attacks in Estonia, as well as create secure software environments for sharing information.

Thirdly, in the context of information security, considerable attention in Estonia is given to the protection and use of personal data, which is carried out as transparently as possible, using digital signatures and encrypted messages. The person has the right at any time to correct or delete personal data by contacting the Data Protection Inspectorate. Estonia is moving towards creating a market model of private data that allows personal data holders to license/lease data. The most advanced information infrastructure, the detailed cyber security strategy, which is adopted every four years, and the reliable system of personal data protection has enabled Estonia to become an advanced information protected country. Estonia's distinguished experience is useful for Ukraine in overcoming crisis phenomena in the information field and adopting legal acts.

7 Conclusions and recommendation

Summarising the study, authors can say that the experience of Estonia shows that a developed information security system contributes to the well-being and welfare of society and increases the level of trust in public institutions. Authors believe that raising the level of information security will help a number of the following measures:

1 To create a working group with the involvement of international experts to develop the concept of information security and regulatory support for its activities.

2 Provide for the creation of a single national electronic information resource in the concept of information security.

3 Introduce a unique national identifier for the individual.

4 To create a single secure web portal of electronic services with the possibility of creating electronic offices of individuals for receiving administrative services.

References

Chadwick, D.W., Fan, W., Constantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X-S. (2020) 'A cloud-edge based data security architecture for sharing and analysing cyber threat information', *Future Generation Computer Systems*, Vol. 102, No. 1, pp.710–722.

Cybersecurity Act (2018) *Riigi Teataga* [online] https://www.riigiteataja.ee/en/eli/523052018003/consolide (accessed 11 July 2019).

Document C-V. 49: Security within the North Atlantic Treaty Organization (NATO) (2002) [online] http://www.freedominfo.org/documents/C-M(2002)49.pdf (Accessed 11 July 2019).

DOD Dictionary of Military and Associated Terms (2017) [online] https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (accessed 11 July 2019).

Embassy of Ukraine in the Republic of Estonia [online] https://estonia.mfa.gov.ua/ua (accessed 11 July 2019).

Estonia Ranks First in the World in the National Cyber Security Index (2018) [online] https://estonianworld.com/security/estonia-ranks-first-in-the-world-in-the-national-cyber-security-index/ (accessed 11 July 2019).

Gheitasi, K., Ghaderi, M. and Lucia, W. (2019) 'A novel networked control scheme with safety guarantees for detection and mitigation of cyber-attacks', in *18th European Control Conference, ECC 2019*, Naples, Italy, pp.1449–1454.

Gritsun, O.O. (2016) *International Legal Support for International Information Security*, Taras Shevchenko National University, Kyiv.

ITL Estonia [online] https://www.itl.ee/index.php?page=181 (accessed 11 July 2019).

Law of the Republic of Estonia on Personal Data Protection (2007) [online] https://www.riigiteataja.ee/akt/130122010011 (accessed 11 July 2019).

Li, Y., Wang, C-Z., Huang, G-Q., Zhao, X., Zhang, B. and Li, Y-C. (2019) 'A survey of architecture and implementation method on cyber security situation awareness analysis', *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, Vol. 47, No. 4, pp.927–945.

Lipkan, V.A. (2006) *Information Security of Ukraine in Conditions of European Integration*, CST, Kyiv.

Lu, H., Zhang, G. and Shen, Y. (2020) 'Cyber security situation prediction model based on GWO-SVM', *Advances in Intelligent Systems and Computing*, Vol. 994, No. 1, pp.162–171.

Ministry of Foreign Affairs of the Republic of Estonia (2018) *Cyber Security* [online] https://vm.ee/en/cyber-security (accessed 11 July 2019).

Nesterenko, O. (2012) *Information in Ukraine: The Right of Access*, 'Acts', Kyiv.

Personal Data Protection Act (2018) [online] https://www.riigiteataja.ee/en/eli/523012019001/consolide (accessed 11 July 2019).

Priisalu, J. and Ottis, R. (2017) 'Estonian experience', *Health Technologies*, Vol. 7, No. 1, pp.441–451.

Public Information Act (2001) [online] https://www.riigiteataja.ee/en/eli/514112013001/consolide (accessed 11 July 2019).

Razumkov, T.V. (2018) 'Problems of administrative and legal support of the right to free speech in Ukraine and ways of their solution', *Actual Problems of Improving the Current Legislation of Ukraine*, *Collection of Scientific Articles*, Vol. 48, pp.178–190.

Roy, R. and Das, D. (2017) 'Dilution of social media privacy: security vulnerabilities and psychological implications', *Media Watch*, Vol. 8, No. 3, pp.401–412.

The Constitution of the Republic of Estonia (1992) [online] https://www.riigiteataja.ee/en/eli/530102013003/consolide (accessed 11 July 2019).

Voloshina, N.M. (2010) 'The notion of 'security of information' and 'information security' in modern scientific space', *Modern Information Technologies in the Field of Security and Defense*, Vol. 2, No. 8, pp.53–56.

Yandex Taxi to Introduce App-Based Ride Ordering Service in Tallinn (2018) https://news.err.ee/827618/yandex-taxi-to-introduce-app-based-ride-ordering-service-in-tallinn (accessed 11 July 2019).