LEGAL REGULATION FEATURES OF THE FIGHT AGAINST CYBERTERRORISM AND PERSONAL DATA PROTECTION POLICIES IN UKRAINE AND ABROAD

Yurii Kohut
applicant higher education
degree of Doctor of Philosophy (PhD.),
Department of National Security,
Educational and Scientific Institute of law named
after Volodymyr the Great of Interregional Academy of
Personnel Management, Ukraine, Kyiv

Abstract. Article deals with the legal regulation features of the fight against cyberterrorism and personal data protection policies in Ukraine and abroad. Legal regulation of the use of personal data is essential in ensuring the quality of scientific research. The Law of Ukraine «On personal data protection» establishes both general rules applicable to any type of personal data processing and special rules applicable to the analysis of certain categories of personal data, such as information obtained during clinical trials. This paper provides an overview of new standards that regulate aspects of personal data processing in the context of research activities in Ukraine (personal health data, genetic, biometric information, etc.).
Keywords: *personal data protection, cyberattack, cybersecurity, law, personal data.*

Introduction

The Institution of Personal Data is a special institution for the right to privacy in the context of automation and the development of new information technologies.

The establishment of large computer centres and the concentration of different types of information therein have made it necessary to regulate the use and protection of personal information.

Personal data protection has received increasing attention worldwide, and some countries have developed considerable legislative and enforcement experience in this area, which should be used in Ukraine. In particular, legislation on the personal data protection has been developed for quite some time in Europe.

One of the first targeted laws on personal data protection (hereinafter PDP) was the German Land Law of Hessen "On data protection" of 1970, which later became a federal law. On the basis of the premise that the possession of information about citizens constitutes a «public force» the authors of the law rightly believed that automated processing of data without taking measures to protect it poses a threat to personal freedom and, as a consequence, poses a threat to civil society.

The Organization for Economic Cooperation and Development (OECD), which in 1980 adopted the Directive on the Protection of Privacy and International Exchanges of Personal Data, addressed the issue of the personal data protection at the international level.

The international recognition of the importance of the personal data issue was reinforced in 1981 by the adoption by the countries of the Council of Europe of the Convention on the Protection of Natural Persons in the Personal Data Automated Processing». In the context of the application of the latest information technologies and computer and telecommunications technologies the Convention takes the view that the rights and interests of the individual may be violated by the unauthorized use of personal information to the detriment of the individual, thereby negating its natural, vital rights, which are the foundation of human freedom. Consequently, these rights should be protected by the State.

Literature review. Today there are a lot of articles in the field of cybersecurity relating to the technical part of this issue. The number of studies that highlight scientific and organizational issues of implementing projects on cybersecurity is much smaller. Some countries define security goals only; others have efficient mechanisms of risk management in this area. There are different approaches to determining the protection of personal data and privacy. These national differences are influenced by cultural norms of the society and have different advantages and disadvantages. The implemented method of risk analysis allows comparing security systems, which may determine the degree of their readiness to participate in the project activities of cybersecurity.

Research methodology. The article contains an analysis of the problems encountered in establishing and developing legislation on the protection of personal data. It is, first of all, the approach connected with the interpretation of such processes as "cybersecurity", "cyber defence" and "cyberwar". A sociological approach to cybersecurity research involves the study of information conflicts of value and ideology. The multidisciplinary approach, or multidisciplinary approach, is known to be based on a generalized picture of the subject and to set out its research formats that go beyond disciplinary and interdisciplinary approaches.

Research results. In general, the system of European legislation on PSP consists of the already mentioned Council of Europe Convention "On the Protection of Natural Persons in the Automated Processing of Personal Data" of 28 January 1981 amended in 1999, which was the first international legal instrument in the field of personal data protection; Additional Protocol to the Convention "On the Protection of Natural Persons in the Automated Processing of Personal Data concerning Supervisory Authorities and Cross-Border Data Flows" of 8 November 2001 as well as Directive of the Council of the European Union 95/46/EC "On the protection of natural persons in the processing of personal data and on the free circulation of such data" 1995 and Directive 97/66/EC "On the processing of personal data and the protection of the rights of natural persons in the telecommunications sector" 1997. In particular, the use of personal data without the consent of Internet users is contrary to the Council of Europe Convention on the Protection of Natural Persons in Automated Processing of Personal Data.

The above-mentioned instruments are binding not only on the member countries of the European Union, but also serve as models for law enforcement in countries seeking membership of the European Community.

Over the past 30 years more than 20 European States have adopted personal data protection regulations that establish mechanisms for the legal regulation of personal data communications.

The basic principles of the personal data protection in European legal acts are: the collection and processing of personal data (PD) must be carried out correctly and legally; the use of the PD must be adequately defined for the purposes intended, their use must be limited in time, appropriate to the purpose; PD must be accurate; PD must be processed only with the consent of the data subjects; PD must be accessible to the data subjects, including to refine the data; PD must be adequately protected.

Unlike in the EU in the USA there is no federal legislation on the personal data protection at all. According to experts, United States intelligence agencies are prohibited from gathering personal information only on United States residents (which is also not observed in practice). This is not the case with other countries' residents. There is no guarantee that the above-mentioned personal data will not be used or used to harm residents of other States.

In July 2010 Ukraine ratified the Council of Europe Convention on the Protection of Natural Persons in Automated Processing of Personal Data and its Additional Protocol on Supervisory Authorities and Cross-border Data Flows. Ukraine has also adopted laws: «On the protection personal data (from 01.06.2010), "On access to public information" (from 13.01.2011) and "On information" (new version from 13.01.2011). However, despite the existence of a fairly extensive legal framework on the above-mentioned issues, effective personal data protection is not ensured in Ukraine.

Thus, on July 3, 2013 the Law of Ukraine "On the Protection Personal Data" was amended (entered into force from January 1, 2014), which negatively evaluated most

domestic experts on the protection of information with limited access.

First, under these legislative changes the State has removed any responsibility to protect the personal data of its residents. Thus, article 24 of this Law deleted the provision that "the State guarantees the personal data protection". Only the Commissioner for Human Rights (Ombudsman) of the Verkhovna Rada (together with the limited staff of its secretariat) and the courts (see art. 22 of the amended Law) now monitor compliance with PDP legislation. The Law has even removed the rule that the State Service for the Personal Data Protection, which must be recognized, also exercises control over PDP. In practice it also lacked the necessary authority and facilities to effectively perform PDP enforcement functions in the country. For example, owing to the heavy workload of the Public Service to date, applications for the registration of personal databases for only the end of 2011 are being processed (applications for 2012 and 2013 have not even started)!

As can be seen, the entities involved in the personal data protection of residents in Ukraine do not include the State, which is primarily required by international legal instruments to take part in this field of activity**.**

Second, the interpretation of the term "consent of the subject of personal data" for data processing has disappeared from article 2 of the Law. This is a dangerous development, as it is currently unclear what constitutes consent of the subject, and this can be interpreted differently depending on the circumstances, leading to abuse of the PDP in practice.

Third, the task of the so-called owners or managers of residents' personal data who process the data to protect the PD has now become formally more complex: the Ombudsman is required to submit not only a register of personal data belonging to a category that poses a particular risk to the rights and freedoms of the PD subjects (the procedure for the allocation of this category of data is also not defined and regulated in the Law), but also information on the person or structural subdivision of the organization responsible for organizing work related to the personal data protection during their processing, which will not ultimately improve the situation with regard to PDP in Ukraine.

Fourth, the Law of Ukraine "On the Personal data protection", as well as the changes introduced therein, do not focus on the peculiarities of the budget financing of the authorized bodies providing the PDP in the country, but these bodies (Human Rights Commissioner of the Verkhovna Rada, The Ukrainian State Service for the Personal data protection, established in December 2010) does not have an adequate material and technical base, a set of necessary organizational and information support tools and a staff of professional staff; which could effectively implement public policies in the area of PDP. It is also unclear how the actual limited pool of officials of the secretariat of The Human Rights Commissioner of the Verkhovna Rada, who is ignorant in PDP issues from 1 January 2014, on the basis of the above-mentioned Law, will carry out "exit and no-travel, scheduled and unscheduled checks of PD owners or managers" of residents, as well as carry out proper maintenance of the State Register of Personal Data Bases and applications for registration of such databases?

The Law of Ukraine "On the Personal data protection" was amended in 2015, 2017, 2018, 2020.

In addition to the above-mentioned legislative initiatives, on 24 July 2013 the Verkhovna Rada of Ukraine submitted to the Verkhovna Rada a draft decree on the establishment of the Temporary Special Commission (TSC) of the Verkhovna Rada of Ukraine (consisting of six persons, with the term TSC activity - six months) Investigation of the level of threat to the national security of Ukraine, data collection and retrieval programs of the United States Intelligence Services.

We believe that the establishment of a new State structure, a relevant Parliamentary Committee, various special commissions of inquiry, etc. in the field of PDP control will not fundamentally change the situation in the country to strengthen the protection of the residents of Ukraine against the illegal use of their confidential and personal data and will not improve the level of national security of the State as a result. This task is to be carried out by the special units of the State authorities responsible for ensuring the national security of the country, in particular the intelligence / counter-intelligence units of the Security Service, etc. As world practice has shown the system of personal data

protection must be developed and maintained at the appropriate level by intelligence agencies and the State National Security Agency, with adequate budgetary resources allocated to those services and authorities. For example, our nearest neighbor, Russia, recently allocated 40 million rubles to protect itself from cyberattacks by the law enforcement network. Russia has been able to provide a wide range of services to support the newest hardware and software complex, which received its code name "CADPS" ("Computer Attack Detection and Prevention System").

Thus, to date, the de facto Ukraine is not responsible for the PDP security, integrity and confidentiality*. It has fully transferred this responsibility to the owners, PD managers and third subjects (see art. 24 of the Law of Ukraine* "*On PDP*"). Unlike in European countries personal data protection in Ukraine becomes an exclusive corporate obligation of individual enterprises / organizations in our country.

But since the State is the main institution for the protection of human and civil rights and freedoms, including in the field of information, we believe that the result of legislative, law enforcement and other activities, regulate and control the behaviour of the parties involved in the circulation and processing of personal data, rather than transferring this responsibility to other actors in the PDP.

According to domestic information security experts, the Law on PDP requires immediate conceptual and systemic changes, without which its practical applicability and effectiveness cannot be guaranteed.

The use of the accumulated international experience makes it possible to establish personal data legislation in Ukraine, not only in the light of the standards achieved, but also in some cases, to propose more progressive legislation in comparison with the already existing regulatory options on selected issues in particular on the basis of the personal data ownership.

In addition to the legal framework on PDP cybercrime and cyberterrorism are also regulated in foreign countries.

In recent times in the international community including at the State level there has been talk about the serious threats to information security. In particular in the United States in February 2013, Internal Security Minister Janet Napolitano announced the threat of the "impending cyber apocalypse". The Minister called for a new law allowing the Government and the private sector to share information to prevent computer attacks. Such a law was rejected by Congress in 2012. It was rejected by the Congress because of numerous public protests.

In addition, the United States is preparing to promulgate a number of presidential decrees adopted as part of the new cybersecurity program. The program is expected to cover transport companies, municipal services and banking. Common cybersecurity standards for all federal agencies will also be proposed.

The National Strategy to Secure Cyberspace (NSSC) was previously published in the United States in 2003. The document was a part of the broader National Strategy for Homeland Security (NSHS) in response to the terrorist attacks on the 11 September 2001.

In the following years action plans and strategies to address cybercrime and cyberterrorism began to be developed throughout Europe. In 2005, Germany adopted the National Plan for Information Infrastructure Protection (NPIIP).

Subsequently, following a major cyberattack in 2007 Estonia was also one of the first EU member countries to publish a national cybersecurity strategy in 2008. Since then much work has been done at the national level, and in the last four years, ten EU member countries have published their national cybersecurity strategies, which in fact provide a model for addressing the challenge of cybersecurity within States.

In February 2013 the Government of Australia proposed a new national security strategy. The document refers to the need for cooperation between government and business in combating cyberthreats. Plans for a nationwide cybersecurity system were also announced by the Indian authorities.

The Council of Europe Convention on Cybercrime adopted in Budapest on 23 November 2001 was the product of many years of efforts by the Council of Europe. The Convention on Cybercrime was adopted in Budapest. It is one of the most important documents governing legal relations in the field of the global computer network and is the only document at this level so far. Its

adoption is a landmark in the history of the fight against cybercrime.

In February 2013 the European Commission with the EU High Representative for Foreign Affairs and Security Policy published the Cybersecurity Strategy with the draft Directive on Network and Information Security (DNIS). A strategy called "Open, Safe and Secure Cyberspace" represents the EU's comprehensive vision of how to prevent and respond to technical failures and cyberattacks the best. Concrete actions are aimed at increasing the resilience of information systems, reducing cybercrime and strengthening the EU's international policy on computer security (EU Cybersecurity plan to protect open internet and online freedom and opportunity. Press release. EUROPEAN COMMISSION, 2013).

In addition, the Cybersecurity Strategy presented by the European Commission requires each EU member State to establish a computer emergency response team.

However, despite the existence of general European declaratory legal instruments to protect cyberspace the EU does not currently have a single regulatory framework for cybersecurity systems. Moreover, national authorities often refuse to share information with foreign counterparts.

In February 2013 the European Commission proposed to the EU Parliament a bill to tighten the rules of cybersecurity by requiring Internet companies, such as search engines, banks, stock exchanges and a wide range of companies facing cybercrime, Mandatory reporting to public authorities. The Commission notes that this is not only a case of hacking, which can lead to security failures and data leaks, but also other types of incidents with such consequences. It's a human factor and it's just a mechanical failure. Practice shows that the legislative process in the European Parliament takes about two years, but as a result such laws are adopted with some changes.

In this context, recent discussions on the need for uniform legislation to protect PDP at the European level draw particular attention. Thus, on 22 January 2012 EU Commissioner for Justice Vivian Reading addressed the Munich International Conference on Internet Development announced that it would soon present its proposals on the possibilities of unified EU legislation in the personal data protection.

Information relations connected with ensuring cybernetic security in Ukraine as a whole are currently regulated by the laws of Ukraine "On Information" (1992), "On Scientific and Technical Information" (1993), "On Telecommunications" (2004), " On information protection in information and telecommunication systems" (1994), "On Access to Public Information" (2011), "On Access to Public Information" (2011) and others.

Thus, Ukrainian legislation already contains a number of legal norms aimed at the legal protection of Ukraine's cybersecurity. At the same time, the Law of Ukraine "On the Security of Information in the Information and Telecommunications Systems" is playing a key role in ensuring cybersecurity, which governs information security relations in information, telecommunication and information and telecommunication systems.

However, Ukraine was only in the process of establishing a legal framework to combat cyberterrorism. Thus, in May 2013 in first reading the Verkhovna Rada of Ukraine adopted the draft Law «On Amendments to the Law of Ukraine "On Fundamentals of National Security of Ukraine" concerning cybernetic security of Ukraine". In particular, the meeting noted the importance and urgency of addressing the issue of the legal framework for combating computer crime and computer terrorism. The project was withdrawn.

Denmark, the United Kingdom, Finland, Sweden and the Netherlands are currently the most vulnerable countries to cyber threats.

Discussion of research results. The cross-border nature of cyber threats has forced countries to engage in close international cooperation. For example, the European Information Security Agency operates in Europe (EISA).

As noted above, in Tallinn the Cooperative Cyber Defense Center of Excellence (CCDCE) was opened in middle of 2008 with the support of 7 NATO member countries. The main objectives of the Center are to conduct research, provide advisory services and train personnel for national cyberterrorism units. About 30 specialists from Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, Spain and the USA are permanently employed.

The Cyber Defence Management Authority (CDMA) became the NATO Member State cybersecurity focal point. It was established at the end of 2008 to coordinate the actions of

the participating countries after the 2007 cyberattack on Estonia. It is now the main advisory authority of the NATO Cybersecurity Council providing all members of the Alliance with advice on cybersecurity-related issues. Managed by the Cyber Defence Management Board, which consists of the heads of the NATO political, military, operational and technical heads responsible for cybersecurity.

In addition, there are several monitoring and decision-making authorities in the field of cybersecurity of NATO countries. The most important of these are:

- The North Atlantic Council, which is the highest political authority overseeing NATO cyber defence policies and actions;
- Defence Policy and Planning Committee (DPPC). This Committee develops strategic proposals for Council approval (e.g., the development of the NATO Cybersecurity Policy or the NATO decision to establish the Cyber Defence Management Authority).

It is also worth mentioning the NATO Consultation, Control and Command (NC3) Board, which is the main authority for consultation on technical and production aspects of cyber defence. Together with the Military Authorities (NMA). These authorities are responsible for approving operational requirements, as well as acquiring and implementing NATO cybersecurity capabilities (Revskyi, 2011.).

It should be noted that while prior to the attack on Estonia NATO focused on protecting the communications systems used by the Alliance, after 2007 NATO's aim was to protect communications systems, directly used by its members, which has led to the development of assistance mechanisms for those countries requiring support to protect their computer systems, in particular through the dispatch of rapid reinforcement teams (RRTs).

Conclusions

However, the NATO member countries continue to bear the primary responsibility for the safety and security of their communications systems.

The consequence of the policy of «reboot» was that international organizations and the United States began to actively involve Russia in the preparation of a convention on cyberwar. One of its main tasks is the attempt to remove «civic» objects from the cyberattacks on the Internet. In addition, the possibility of establishing an international tribunal to try.

The decision to start working on cyberwar rules was launched in May 2010 at the first Cybersecurity Summit in Dallas.

In conclusion, I would like to emphasize the following: to deny today the existence of cyberterrorism in its various manifestations, as a serious threat that challenges the international community, is reckless and short-sighted. The challenge for States is not only to clearly identify the problem, but also to develop effective legal and technical means to combat it.

References

1. EU Cybersecurity plan to protect open internet and online freedom and opportunity. Press release. EUROPEAN COMMISSION. Brussels, 7 February 2013. Available at: http://europa.eu/rapid/press-release_IP-13-94_en.htm [Access date: 15.06.2020].
2. Revskyi A. D. Cyberterrorism - virtual instrument of real war. European Security Centre bulletin. 2011. Vol. 23 (39) p 12-15.
3. National Strategy for Homeland Security (2002). Available at: https://www.dhs.gov/publication/first-national-strategy-homeland-security
4. National Infrastructure Protection Plan (NIPP) 2013: Partnering For Critical Infrastructure Security And Resilience. Available at: https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
5. On telecommunications. Law of Ukraine. Information of the Verkhovna Rada of Ukraine [Pro telekomunikatsii. Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy], 2004, № 12, ст. 155. Available at: https://zakon.rada.gov.ua/laws/show/1280-15#Text
6. On scientific and technical information. Law of Ukraine. Information of the Verkhovna Rada of Ukraine. [Pro naukovo-tekhnichnu informatsiiu. Zakon Ukrainy. Vidomosti Verkhovnoi Rady

Ukrainy], 1993, № 33, ст.345. Available at: https://zakon.rada.gov.ua/laws/show/3322-12#Text
7. On information. Law of Ukraine. Information of the Verkhovna Rada of Ukraine. [Pro informatsiiu. Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy], 1992, № 48, ст. 650. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text
8. On personal data protection. Law of Ukraine. Information of the Verkhovna Rada of Ukraine. [Pro zakhyst personalnykh danykh. Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy], 2010, № 34, ст. 481. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text
9. On access to public information. Law of Ukraine. Information of the Verkhovna Rada of Ukraine. [Pro dostup do publichnoi informatsii. Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy], 2011, № 32, ст. 314. Available at: https://zakon.rada.gov.ua/laws/show/2939-17#Text
10. On information protection in information and telecommunication systems. Law of Ukraine. Information of the Verkhovna Rada of Ukraine. [Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh. Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy], 1994, № 31, ст. 286. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text