Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2021, vol. 121, pp. 135–147

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2021.121.8

Teisės aktualijos / Problems of Law

Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France

Sviatoslav Kavyn

ORCID: https://orcid.org/0000-0002-6189-3848
Ivan Franko University of Lviv
1 University Street, Lviv, Ukraine, 79000
Postgraduate student, Department of European Law
Faculty of International Relations
Phone: + 380631756263
Email: kavinsviatoslav@gmail.com

Ivan Bratsuk

ORCID: https://orcid.org/0000-0003-0164-7407
Ivan Franko University of Lviv
1 University Street, Lviv, Ukraine, 79000
Associate Professor, Candidate of Law
Department of European Law
Faculty of International Relations
Phone: + 380631571488
Email: bratsuk@gmail.com

Anatoliy Lytvynenko

ORCID: https://orcid.org/0000-0001-7410-5292
Baltic International Academy of Riga
4/1 Lomonosova Street, Riga, LV-1019
Doctoral candidate, Department of Legal Sciences
MRes/PhD candidate at the School of Law
Robert Gordon University of Aberdeen
Garthdee House, Garthdee Road, Garthdee, Aberdeen AB10 7AQ, Scotland, UK
Phone: +371 224 853 58
Email anat.lytvynenko@gmail.com

This article is devoted to the study of information security in the EU member states, in particular Germany and France, in the context of the analysis of their national legislation, state, national programs and regulations. Particular attention is paid to the study of the features of regulatory and legal security of information security of Germany and France in the context of the study of their national legislation in terms of economic security as an inherent component of national security. In the course of this study the peculiarities of the functioning of the institutional and legal mechanism of cyber defense in the context of the multi-vector system of international security and legal regulation of international cooperation are analyzed. The article substantiates the expediency of developing an integrated, coordinated information policy of the EU member states in order to unify approaches to information security.

Received: 26/04/2021. **Accepted:** 04/10/2021

At the same time, the current realities of European Union policy require comprehensive research in the context of ensuring national interests, developing effective mechanisms for protecting the information space, and legal mechanisms for shaping the economic system as a strategic factor of national security. Accordingly, the approaches to information security adopted in the European Union are currently not unified due to the geopolitical specifics of the EU's countries. Therefore, the research, evaluation, and implementation of the positive experience of Germany and France in this area, according to the authors, is important in building the information security system of the European Union in the context of reliable protection against cyber threats.
Keywords: EU information security, information security, information space, EU legislation on information security, EU law.

Kibernetinio saugumo reguliavimas ir teisinis vykdymas Europos Sąjungos šalyse: Vokietijos ir Prancūzijos patirtis

Straipsnis skiriamas informacijos saugumo tyrimams ES valstybėse narėse, ypač Vokietijoje ir Prancūzijoje, analizuojami jų įstatymai, programos ir reglamentai. Ypatingas dėmesys skiriamas Vokietijos ir Prancūzijos informacijos saugumo reguliavimo ir teisinio saugumo ypatybių tyrimui, atsižvelgiant į jų įstatymų, susijusių su ekonominiu saugumu, kaip būdingą nacionalinio saugumo sudedamąją dalį, tyrimą. Šio tyrimo metu analizuojami kibernetinės gynybos institucinio ir teisinio mechanizmo funkcionavimo ypatumai tarptautinio saugumo daugiavektorių sistemos ir tarptautinio bendradarbiavimo teisinio reguliavimo kontekste. Pagrindžiamas integruotos ir suderintos ES valstybių narių informacijos politikos kūrimo tikslingumas siekiant suvienodinti požiūrį į informacijos saugumą.

Atsižvelgiant į dabartines Europos Sąjungos politikos realijas reikia išsamių tyrimų siekiant užtikrinti nacionalinius interesus, sukurti efektyvius informacinės erdvės apsaugos mechanizmus, teisinius ekonominės sistemos, kaip strateginio nacionalinio saugumo veiksnio, formavimo dėsningumus. Europos Sąjungos valstybių požiūris į informacijos saugumą dėl ES šalių geopolitinės specifikos šiuo metu nėra vienodas. Todėl, autorių teigimu, teigiami Vokietijos ir Prancūzijos patirties šioje srityje tyrimai, vertinimas ir įgyvendinimas yra svarbūs kuriant Europos Sąjungos informacijos saugumo sistemą siekiant patikimos apsaugos nuo kibernetinių grėsmių.
Pagrindiniai žodžiai: ES informacijos saugumas, informacijos saugumas, informacinė erdvė, ES teisės aktai dėl informacijos saugumo, ES teisė.

Introduction

National information security networks able to quickly accumulate the forces and means of public authorities to counter a wide range of threats have been established in many EU countries. The operation of these networks is clearly regulated by a legal framework. The experience of EU member states (including Germany and France, the regulatory frameworks of which are described in this article) shows that ensuring a high level of information security is possible only with the adoption of a thorough and effective system of regulations in this area, as well as an effective functioning of state control bodies, which will be responsible for ensuring information security in a particular country.

But the events of recent years clearly indicate the existence of a crisis in the field of information security, both at the international and regional levels. Therefore, the solution of the issues of proper legislative provision of information security comes to the fore. At present, there are legal frameworks in this area in the EU member states, but there is a problem in a certain inconsistency of the laws among the EU member states in the approaches to addressing certain issues of information security, which significantly reduces the effectiveness of legal regulation in this sphere.

Thus, the creation of an effective and reliable system for maintaining the information security of our country seems extremely important in the context of the transformation of international security and foreign policy of our country before joining the European Union. In addition, the study of the experience of EU member states in this area becomes important, carried out in order to adapt the information security standards that are currently implemented in EU member states in the context .

1. Review of the research on cybersecurity as a component of information security

In domestic and foreign literature, a number of authors have focused on the study of information security in their works, including D. Vasylenko, T. Tkachuk, O. Zozulya, B. Kormych, M. Gorka, V. Pilliteli, M. Niles, T. Olavsrud, R. Lucas, and others. A. Lytvynenko has studied the case law of the European Court of Human Rights on this issue. However, there was a lack of a comprehensive study and comparison of the experience of EU member states in the field of information security in order to borrow their experience in domestic law.

Diego Acosta Arcarazo and Cian C. Murphy note that after the Lisbon Treaty entered into force, it has given the European Union new powers in the field of international security law. At the same time, the Stockholm Program is the latest framework program of EU action in the field of justice and home affairs, in particular in matters of cooperation between national criminal justice systems. And the combination of the new Treaty and the Program has made security and justice key areas of the legislative development in the EU (Arcarazo, Murphy, 2014, p. 17). This is also emphasized by Raphael Bossong, who notes that the intensive exchange of information between security agencies is an important element of security cooperation between the countries of the European Union (EU) (Bossong, 2018, p. 6).

In light of the development of new IT technologies, cybersecurity comes to define a new age of information security aimed at the digital environment that we actually inhabit. Today, cybersecurity is not only the protection of information itself, but also the protection of the entire system in the information field, generally in the IT field (computer technology field), and is responsible for three factors: systems, processes, and people.

Prof. Dr. Udo Helmbrecht notes that providing the European Union's network and information systems in the legal field is important to support the Internet economy through the introduction of new initiatives that would further improve cyber resilience and respond to cybersecurity threats (Helmbrecht, 2018). In this context, Marek Gorka defines a cybersecurity strategy as a basic document created in a government context that reflects the interests and rules of cybersecurity. It also lays the groundwork for future legislation, policies, standards, guidelines, and other recommendations on security and cybersecurity (Gorka, 2018, p. 76). In addition, the cybersecurity strategy is a policy document needed for the effective provision of information security in general, without which, in terms of regulations, authorities and enterprises, it is quite difficult to work due to the diverse interpretation of legislation, which ultimately leads to serious lawsuits at both the national and international levels.

Information security is one of the components of sustainable development of the whole state, and scientists usually invest the same approaches to understanding the meaning of the term "information security". Thus, in particular N. R. Nyznyk, B. T. Belous under this term means "the state of legal norms and the corresponding security institutions that guarantee the constant availability of data for strategic decision-making and protection of information resources of the country" (Lipkan *et al*., 2006, p. 280). In essence, a similar view is supported by B. A. Kormich, who notes that information security should be understood as the "protection of statutory rules under which information processes take place in the state, providing constitutionally guaranteed conditions existence and development of man, the whole society and the state" (Kormych, 2004, p. 384). According this point of view, "information security" is the legislative and policy framework governing the use of information and communication technologies by institutions and agencies of the European Union in terms of their degree of information content and data privacy (Robinson, Gaspers, 2014, p. 1–2). This view is supported by K. Dempsey, who notes that information security is a legal and policy framework that regulates

the legal field and simultaneously regulates the use of information and communication technologies with the appropriate degree of responsibility for confidentiality of data (Nieles *et. al.*, 2017, p. 2–3). Finally, Michał Mazur quite aptly states that "information security, both real and legal, is a primary factor for the functioning of individuals and institutions, and especially for political organisms that are independent states and are based on legal regulations that can authorize the effective security of identified data" (Mazur, 2011, p. 64).

2. A legal platform for information security and the protection of the cyberspace in developing the economic security of the European Union

The modern concept of the strategic management of economic security arose in response to the challenges and threats of the external and internal environment, caused by the total digitization of society. The information society is characterized by a permanent improvement of information technologies and the rapid pace of their implementation in all spheres of public life. The result is the virtualization of much of public relations and an increasing dependence of countries on electronic networks and information systems. Important trends of the current stage are also the intensification of cross-border information flows, as well as the spread of various methods and means of information exchange, which are virtually uncontrolled. As a result, new informational threats and challenges are spreading, which require the immediate response and application of non-standard measures and solutions from the EU and each member state in particular. In this regard, information security is becoming a priority in shaping the EU's economic security.

In this context, the main directions of European information security policy have been formed, in particular: 1. The development of a European system of warning and informing about new threats. 2. The provision of technological support. Priority is given to the development of research on network and information security. 3. The support for market-oriented standardization and certification. 4. Legal support. 5. Strengthening security at the state level. 6. The development of international cooperation on information security. The main task of the EU is to strengthen the European Commission's dialogue with international organizations and partners on the issue of network security and, in particular, on the growing dependence on electronic networks.

In this context, the organization of the process of the strategic management of the EU's economic security involves the following sequence: defining strategic goals → strategic analysis → determining the list and priority of threats to economic security → assessing the level of economic security → modeling scenarios for both EU and national economies → strategy and tactics to ensure the economic security of the European Union and EU countries → development of measures, tools, and mechanisms for implementing the country's economic security strategy → monitoring and control.

Today, in most countries, including countries of the European Union, cybersecurity legislation is under active development. The formation of legal support for cyber defense is based on national principles on the one hand and on the basis of a unified international platform on the other. In this context, an important factor in the development and formation of regulatory support for cybersecurity is that the issues related to improving cybersecurity cover different areas of law.

In this context, it should be noted that many countries have signed and are implementing an international agreement on what is considered a cybercrime, namely the Budapest Convention on Cybercrime (Convention On Cybercrime European, 2001). In particular, the Budapest Convention covers the following categories of cybercrime in the field of information security:

– the violation of confidentiality, integrity, and the availability of computer data and systems;
– computer-related crimes;
– copyright infringement.

This paper, which studies the legal framework for information security, is focused primarily on countries like Germany and France, because in our opinion, these member states have so far developed the highest level of legal standards of information security.

2.1. Germany

The German legal framework applicable to cybersecurity includes laws applicable to monitoring, detection, prevention, mitigation and incident management. It includes, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws and import / export controls, among others.

Cybersecurity is regulated by several German acts. The main legal act concerning cybersecurity is the German Security Act (IT-Sicherheitsgesetz) of 25 July 2015 / (Security Act (IT-Sicherheitsgesetz), 2015), which amended a number of laws, including the Act on Telemedia (Telemediengesetz) / Telemedia Act (Telemediengesetz) /, Telecommunications Act (Telekommunikationsgesetz) / Telecommunications Act (Telekommunikationsgesetz) /, EU General Data Protection Regulation (Datenschutz-Grundverordnung) / The EU General Data Protection Regulation (Datenschut) , Federal Law on Data Protection (Bundesdatenschutzgesetz) / Federal Data Protection Act (Bundesdatenschutzgesetz) /, and the Law on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) / Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) /, In addition, the sectoral cybersecurity sectors are regulated, for example, by The Banking Act (Kreditwesengesetz) / and the Securities Trading Act (Wertpapierhandelsgesetz). In this context, it should be noted that the disclosure of professional secrets is punishable under Art. 203 StGB (formerly the Strafgesetzbuch, p. 300) and is a crime of minor gravity. Interestingly, banking secrecy as such is not codified in this country and, according to case law, comes from Art. 2 (1) Grundgesetz Germany and does not require additional consolidation in the contract between the bank and the depositor (client) (OLG Frankfurt am Mein, 2004, paras. 34–36).

In addition to this official legislation, there are several important informal provisions on IT security in Germany. This is the BSI Baseline for Information Technology Security (Bundesamt für Sicherheit in der Informationstechnik – "BSI"), General Criteria for Information Technology Security Evaluation (2012), standardized as ISO / IEC 15408, and control of the information and related technology target ("COBIT"). In addition, The EU Cybersecurity Act Regulation (2019) provides the necessary powers to the European Union Agency for Cybersecurity ("ENISA") to establish cyber currency certification. Typically, ENISA will be the main point of contact on any cybersecurity issues.

The Federal Office of Information Security Act sets out specific cybersecurity requirements for critical infrastructure.

In this context, German and European legislation provides for a number of obligations for organizations to take measures to monitor, detect, prevent, and remedy the consequences of cyber incidents, in particular:

- According to section 13 (7) of the Telemedia Act. 13 (7) of the Telemedia Act, telemedia service providers must ensure that unauthorized access to the technical equipment used for their telemedia services is not possible and that the protection of personal data from external cyber attacks is ensured.

- According to section 109 (1) of the Telecommunications Act / According to Sec. 109 (1) of the Telecommunications Act, telecommunications service providers shall apply technical safeguards to protect the confidentiality and personal data of telecommunications and to protect telecommunications and data-processing systems from unauthorized access.
- Suppliers of multiple financial products are required to develop a risk management system focused on the IT sector (Section 25a of the Law on Banks (Kreditwesengesetz)) / (Sec. 25a of the Banking Act (Kreditwesengesetz)) / and (Section 80 of the Securities Trading Act (Wertpapierhandelsgesetz)) /.

The above requirements are provided by the Federal Office for Information Protection, the competent data protection authorities, and the Federal Network Agency.

- The Federal Office for Information Security is the main body for cybersecurity in Germany. This body plays a key role in precautionary security matters and is primarily responsible for receiving reports of security breaches in critical infrastructures.
- Data protection authorities ensure compliance with all relevant data protection laws. In Germany, each federal state has a separate data protection authority.
- The Federal Grid Agency enforces telecommunications laws and is responsible for receiving reports of security breaches in telecommunications networks and services.

If the organization responsible for the IT system under attack does not respond appropriately to the incident – depending on the type of offense – the person concerned may file a lawsuit against the injunction to enforce the defendant's contractual and other obligations under the law. In addition, the person concerned may file a civil claim for damages if the incident arose due to the lack of an appropriate IT security model.

2.2. France

The following are the most important laws in the field of cybersecurity in France that have formed its regulatory platform:

- Godfrain Law № 88-19 of 15 January 1988 / The Godfrain Law n ° 88-19 of January 15, 1988 /.
- Data Protection Act № 78-17 of 6 January 1978 / FDPA (Loi Informatique et Libertés) № 78-17 of 6 January 1978 / This Law has been successively amended by two laws. The first amendments were made by Law № 2004-575 of June 21, 2004. The final amendments were made by Law № 2018-793 of June 20, 2018, which transposes the GDPR and Resolution 2018-1125 of 12 December 2018.
- Law on a Digital Republic № 2016-1321 of October 7, 2016 / Law for a Digital Republic n ° 2016-1321 of October 7, 2016 / This Law was amended in 2018 by Law № 2018-493 of 20 June 2018, transposing the GDPR.
- The Network and Information Systems Security Act ("NIS Act"), which transposes the NIS Directive № 2018-133 of 26 February 2018, as amended by Decree № 2018 -384 of May 23, 2018, which describes in detail the application of the NIS Law, as well as lists the sectors, types of operators and critical infrastructures. It is also necessary to note the Decree of September 14, 2018, which defines the safety rules (together with the "NIS Rules").

In addition to the abovementioned legislative platforms, the following laws have adapted criminal law to certain forms of cybercrime and created specific investigative tools, in particular:

- Law on Daily Security (known as LSQ № 2001-1062 of 15 November 2001), / Law on Daily Security, LSQ № 2001-1062 of November 15, 2001 /, Law on Internal Security (№ 2003-239 of 18 March 2003) / Law on Internal Security n ° 2003-239 of March 18, 2003 /.

- Law on the Adaptation of the Judicial System to the Development of Crime in Modern Conditions (№ 2004–204 of March 9, 2004) /, Law on Copyright in information society (known as the Law of David of August 1, 2006 № 2006–961) / Law on Copyright in the Information Society № 2006–961 August 1, 2006 /.
- Law strengthening the fight against organized crime and terrorism (№ 2016-731, June 3, 2016) / Law strengthening the fight against organized crime and terrorism № 2016-731, of June 3, 2016 /.

In France, critical infrastructures are defined by law (Law № 2013-1168 of 18 December 2013, Law № 2016-41 of 26 January 2016, Law on NIS / Law n ° 2013-1168 of December 18, 2013, Law n ° 2016- 41 of January 26, 2016, NIS Act) /), and must meet specific legal requirements. This mostly applies to the following infrastructures:

- Professionals covered by professional secrecy. During the period of 1810–1994, the violation of professional secrecy was punishable under Art. 378 of the Criminal Code (Napoleon's Code). It included both a ban on testifying in court about the patient's health and any other out-of-court disclosures (Lytvynenko 2020b, p. 105–111).
- Basic Service Operators ("OES"), who are appointed by the Prime Minister in various sectors under the NIS Rules.
- Digital service providers ("DSP"). According to the NIS Rules, these infrastructures must appoint a representative in the national territory of ANSSI if the supplier itself is established outside the European Union and has no representative within the European Union.

According to the GDPR, the controller and the processor must take appropriate technical and organizational measures to ensure a level of security commensurate with the identified risk. NIS rules also require that OES and DSP:

- form and maintain a list of network and information systems required to provide basic / digital services;
- identified risks to the security of information systems;
- ensure an appropriate level of security in accordance with existing risks, as well as implement technical and organizational measures necessary to prevent, manage and reduce risks;
- avoid incidents and minimize their impact to ensure the continuity of their services;
- Identify IT security risks that may affect their operations.

CNIL monitors the proper application of FDPA and GDPR by data controllers and operators. It also provides opinions on bills or regulations. CNIL has significant power in monitoring and investigating incidents.

Finally, CNIL has significant powers over administrative and financial penalties and can make such decisions as the temporary or permanent suspension of data processing.

Regarding the application of the NIS Rules, ANSSI is the national body responsible for responding to cybersecurity cases targeting strategically important institutions. The Ministry of Defense and the Ministry of the Interior also take on the role of preventing all forms of cybercrime.

In some areas, cybersecurity prevention measures need to be substantially stringent. This is especially true for critical infrastructures that must comply with the NIS Rules or infrastructures that process confidential data (for example, health data or data related to criminal convictions, offenses, or security measures).

The financial services sector must meet several requirements, such as auditing IT systems, strengthening its resilience to cyber risks, developing protection adapted to the complexity of cyber attacks, and submitting several applications to ANSSI (Ministerial Order of 28 November 2016).

Under French law, the general rule of civil liability is set out in Article 1240 of the French Civil Code, according to which any act causing harm to another obliges the person who caused it to remove

or compensate him. Moreover, under the GDPR (Article 79), a civil action can be brought in the event of an incident if the controller or data controller has not complied with the requirements of the GDPR. Finally, under the FDPA, the data subject has the right to authorize a non-profit body, organization or association to stop the breach and obtain compensation (Article 37).

3. The case law of the European Court of Human Rights in the field of information security

The territorial jurisdiction of the ECtHR extends to all signatory states to the European Convention on Human Rights, and the substantive jurisdiction of the Court relates to human rights violations enshrined in its provisions, including its additional protocols.

At present, only a small number of cases involving the Internet address the issue of "jurisdiction". In particular, we can mention the case of Breyer v. Germany (Breyer v. Germany, 2020). In this case, the National Legal Obligation of Service Providers to Keep Personal Data of Users of Their Prepaid Mobile SIM Cards was examined.

In June 2004, amendments to the Telecommunications Act introduced a legal obligation for telecommunications service providers to collect and store the personal data of all their customers. The applicants challenged this obligation in the Federal Constitutional Court, which found that such an obligation was incompatible with the Basic Law.

The Court found that the legal obligation under Article 111 of the Telecommunications Act did not contravene Article 8 of the Convention. This decision is noteworthy because it concerns a new problem of personal data protection. It also contains a comprehensive review of case law under Article 8 concerning the protection of privacy in the collection of personal data, in particular the principle of information self-determination (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 2017).

As to the nature of the interference with the rights provided for in Article 8, the Court reiterated that the mere storage of data concerning a person's private life per se constitutes an interference with the right to privacy (see ECtHR in Leander v. Sweden, 1987); however, the right to privacy is by no means absolute, and in some cases may be legitimately restricted. In this connection, the European Court also drew attention to the conclusion of the Federal Constitutional Court of Germany that the degree of protection of the right to information self-determination under national law was not limited to information.

As to the lawfulness of the interference, the Court found that the storage of the data itself was justified by the Law (section 111 of the Telecommunications Act), which was sufficiently clear and predictable.

In assessing proportionality, the Court confirmed that, in the context of national security, national authorities exercised a degree of discretion in choosing the means to achieve a legitimate aim in the absence of a consensus among the Council of Europe countries on the retention of prepaid SIM customers. The Court thus agreed that the obligation to keep subscribers' information under section 111 of the Telecommunications Act as a whole was an appropriate response to changes in the conduct of communications and in the means of telecommunications.

In conclusion, the Court concluded that the interference was, although not trivial, limited in nature. In this context, the Court emphasized certain guarantees.

First, the Court noted that there was no technical danger to the retention of data, the duration of such retention was limited to the end of the calendar year and the retained data were essentially limited to the information necessary to clearly identify the subscriber concerned.

Second, the Court has examined the possibilities for future access to the use of stored data, in particular information requests that may be made under Articles 112 and 113.

The Court explained that the level of verification and control was important, but not decisive, as an element of assessing the proportionality of the collection and storage of a limited set of data, such as in this case. With regard to the applicable regime in particular, the Court noted that the Federal Network Agency was competent to verify the admissibility of data transmission if necessary, that each search query and relevant search information was recorded in order to monitor data protection by the relevant independent data protection authorities.

According to A. Lytvynenko, there are plenty of examples of lawsuits concerning the disclosure of professional secrets in the practice of the European Court of Human Rights, in particular cases related to the disclosure of banking secrecy, as well as a large part concerning medical secrecy (Lytvynenko, 2020, p. 185–215). Banking secrecy belongs to the field of professional secrecy, as well as a number of others (e.g., legal or medical secrecy). In the case of *Michaud v. France*, the EctHR indeed recognizes that the confidentiality of the legal relationship between a lawyer and a client is covered by Art. 8 (1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms. At the same time, the concept of "privilege" in the interpretation of the ECtHR, judging by the case of *Michaud v. France*, applies to all information arising from the legal relationship between a lawyer and a client (*Michaud v. France*, Judgment, 2012). Thus in the case of the ECtHR's *G.S.B v. Switzerland*, the plaintiff, a US and Saudi national living in Miami, California, sued the ECtHR in Switzerland because his bank account details had been transferred to the ATF (Swiss Federal Tax Service) as part of a request from Switzerland for administrative assistance from the American side. The ECtHR stated that since the relevant agreements had been signed and ratified between the United States and Switzerland, it could not be said that the data was collected illegally. In addition, the Court also unequivocally agreed that all the plaintiff's bank details belonged to his "personal data". The court also ruled that the "interference" was indeed sanctioned under bilateral agreements between the United States and Switzerland (*G.S.B. v. Switzerland*, 2015).

A. Lytvynenko also notes that the issues of information security in the field of intellectual property protection are also important (Lytvynenko, 2020, p. 185–215). Thus, in the case of *Coty Germany Gmbh v. Stadtsparkasse Magdeburg* (2015), the Federal Court of Germany referred the case to the European Court of Justice with a request on how to interpret the provisions of Art. 8 (3) (e) Directive № 004/48 / EC on the protection of intellectual property rights (Directive № 2004/48 / EC), which may be interpreted by a court as derogating from national law, which in turn allows the bank not to provide information on the name and address of the bank account holder under Art. 8 (1) (c) of this Directive (Directive № 2004/48 / EC). The European Court of Justice noted that the contents of Art. 8 (1) (c) of EU Directive № 2004/48 / EC on the enforcement of intellectual property rights ; it appears that in the event of an infringement of an intellectual property right and a reasoned request from the plaintiff, the court may order that information on the origin of the infringement be provided by any person who provides services on a commercial basis. The court then raises the question of how to properly combine the rights of some (in relation to intellectual property) with the fact that the confidentiality of these depositors of the bank may be significantly affected. The European Court of Justice assessed the situation as follows: the provisions of the German Code of Civil Procedure, which allowed banks not to testify or provide information in civil proceedings, did not have any exceptions to the rules, which precluded the plaintiff's satisfaction of intellectual property rights. Because of this, in the opinion of the court, the provisions do not correspond to the fair balance specified in Art. 8 EU Directive № 2004/48 / EC on the protection of intellectual property rights. Therefore, the European Court of Justice ruled that the provisions of Art. 8 (3) (e) of the EU Directive 2004/48 / EC should be interpreted as derogating from a provision of national law, which would allow banks to freely and unrestrictedly use banking secrecy as a justification for refusing to provide the information requested by the claimant.

Conclusions

Information security is a phenomenon that has existed in legal systems for several centuries. Initially, it concerned the non-disclosure of patient health information or legal secrecy (which courts in the early 19th century called "office secrecy"), which included all the information a lawyer received from his client – not necessarily within the confines of his office (Sieur Hardy c. Sieur Jean, p. 106); the lawyer would be prohibited from disclosing such information, even as a witness at trial, except for a number of exceptions elaborated in jurisprudence (usually the provisions of criminal codes or lawyers' professional ethics did not contain such provisions – it was given to the courts). Subsequently, when information becomes a commodity, it was recognized by the courts as property (Exchange Telegraph Co. v. Gregory & Co., p. 264) and became a subject of offenses and crimes more and more often. This is especially true regarding the rapid development of information systems and complex computer technologies, when information security offenses are becoming more predatory, and the weak level of information systems security can cause significant damage to individuals, businesses, and government agencies. That is why, since the 1970s, the information policy of many countries around the world includes system-forming information security strategies, on the basis of which relevant legislation is developed and adopted to strengthen the level of information security in both the public and private sectors.

In the context of defining information security in relevant international legislation, it can be noted that in light of the globalization of the information space, the emphasis of information security lies in the field of cybersecurity, which requires a qualitatively new regulatory platform for information security relations within the framework of protecting national security and mechanisms for eliminating threats by legal means.

Cross-border cases present a cross-border element that raises, inter alia, questions about the circumstances in which a court may exercise jurisdiction over a defendant who is registered in another state where the alleged crime has been lodged or a civil offense committed over the internet. These issues should be decided primarily by national courts that apply the relevant principles of private international law to a jurisdiction that does not directly concern the European Court of Human Rights.

Based on the analysis, the following trends can be identified:

- Domestic security requirements evolve and often arise from national cybersecurity strategies, but all countries adopt legislation and instead rely on the development of industry standards to establish a level of actual security requirements. Although it should be noted that the absence of a strict law does not necessarily mean the absence of cybersecurity measures.
- There is an important difference and therefore some significant contradictions between the requirements of internal security, on the one hand, and the interests of national security on the other. The first concerns the level of security that the country seeks to achieve, but at the same time is neutral with regard to information service operators and their nationality and citizenship. The second type of measures is based on the interests of national security and on what will logically be used to eliminate the perceived risks associated with operators from certain countries.

Sources

Legislation

Act on the Federal Office for Information Security (BSI Act - BSIG) (undated) [online]. Available at: https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz.html [Accessed 09 July 2020].

Act on the Protection of Privacy in Electronic Communications (undated) [online]. Available at: https://www.finlex.fi/en/laki/kaannokset/2004/en20040516 [Accessed 09 July 2020].

Adequate and effective cybersecurity: state of play. Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organized by the Austrian Presidency of the Council of the European Union. Vienna, Austria 3rd December 2018.

BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

Common Criteria for Information Technology Security Evaluation CCMB-2012-09-001.

Convention On Cybercrime European Treaty Series – No. 185 Budapest, 23.XI.2001.

Directive № 2004/48/EC, Art. 8 (1) (c); Art. 8 (3)(e).

FDPA (Loi Informatique et Libertés) № 78-17 vid 6 sichnja 1978 p.

Law adapting the judiciary to developments in crime № 2004-204 of March 9, 2004).

Law for a Digital Republic n°2016-1321 of October 7, 2016.

The Network and Information Systems Security Act ("NIS Act").

Law n°2013-1168 of December 18, 2013, Law n°2016-41 of January 26, 2016, NIS Act)/.

Law on Daily Security, LSQ № 2001-1062 of November 15, 2001.

Law on Internal Security n°2003-239 of March 18, 2003.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Security Act (IT-Sicherheitsgesetz) of 25 July 2015.

The Godfrain Law n°88-19 of January 15, 1988.

The EU Cybersecurity Act Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Judicial practice

Breyer v. Germany, №. 50001/12, 30 January 2020.

Exchange Telegraph Co. v. Gregory & Co, [1896] 1 K. B. 147, Law J. Rep. (n.s.) 262.

G.S.B. v. Switzerland, [2015] ECHR 1122, App. № 28601/11, Judgment of 22 December 2015, par. 8–98.

I v. Finland, [2008] ECHR 623, par. 5–47.

Jour. des aud. de la Cour de Cass., etc. Ann. 1816.135.

Leander v. Sweden, 26 Березня 1987, § 48, Серія A №. 116.

Le Sieur Hardy c. le Sieur Jean, Cour Royale de Rouen, 5 aout 1816, Jur. Comm. 1817.106 (T5).

M.N. & Others v. San Marino, [2015] ECHR 661, App. № 28005/12, Judgment of 7 July 2015, par. 50–95.

Michaud v. France, Judgment of 6 Dec. 2012, App. № 12323/11, par. 80–92.

Ministerio Fiscal, C-207/16, 2 Жовтня 2018, EU:C:2018:788.

OLG Frankfurt am Mein, Urt. v. 25.05.2004 – 8 U 84/04.

Plon (Societe) v. France, [2004] ECHR 200, App. № 58148/00, Judgment of 18 May 2004, par. 12–53.

Reichsgericht, III Strafsenat, Urt. v 22 Oktober 1885 g. B. Rep. 2421/85, ERG St. Bd. 13, S. 60, 61–64.

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App. №. 931/13, 27 June 2017 [Grand Chamber] (at § 137)

Special literature

Kormich, B. A. (2004). *Informacijna bezpeka: organizacijno-pravovi osnovi*: navch. posibnik dlja stud. vishhih navch. zakl. K.: Kondor, 384 s.

Lipkan, V. A., Maksimenko, Ju. Je., Zhelihovs'kij, V. M. (2006). *Informacijna bezpeka Ukraini v umovah evrointegracii*: Navchal'nij posibnik. K.: KNT, 280 s.

Litvinenko, A. A. (2020). Zahist personal'nih danih u sferi bankivs'koj taemnici: praktika sudiv dejakih krain anglosakson'skoj i kontinental'noj pravovih simej, suchasna praktika evropejs'kogo sudu z prav ljudini ta praktika evropejs'kogo sudu spravedlivosti. *Pravo i suspil'stvo*, 1, chastina 2, 185–215.

Chernuhin, I. O. (2014). Dosvid Federativnoj Respubliki Nimechchini v pobudovi sistemi zahistu infrastrukturi. *Informacijna bezpeka ljudini, suspil'stva, derzhavi*, 1(14), 27–43.

Shemchuk, V. V. (2019). Zarubizhnij dosvid zabezpechennja informacijnoj bezpeki derzhavi. Porivnjal'no-analitichne pravo, 2, 188–191.

Lytvynenko, A. A. (2020). Data privacy in the sphere of medical confidentiality: the historical and contemporary case-law of the United States, the European Court of Human Rights and selected Continental Europe states. *Topical Problems of State and Law*, Vol. 83, 100–134.

Murphy, C. C., Arcarazo, D. A. (2014). Rethinking Europe's Freedom, Security and Justice. In: Cian C Murphy and Diego Acosta Arcarazo ed. 2014. *EU Security and Justice Law*. After Lisbon and Stockholm, Oxford and Portland, Oregon: Hart Publishing, 1–17.

Nieles, M., Dempsey, K., Pillitteri (Yan), V. (2017. *An Introduction to Information Security*. Special Publication 800-12 Revision 1. Gaithersburg: National Institute of Standards and Technology (NIST).

Mazur, M. (2011). The Legal Basis of Informational Security in Face of Modem World Reality or Only a Myth. In: The Academy of Economic Studies of Moldova, Information Security Laboratory, International Conference (8th edition), Security Information 2011. Kishinev, Republic of Moldova, 4 May, Kishinev: Editorial-Polygraphic Department of ASEM, 64–66.

Robinson, N., Gaspers, J. (2014). *Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies*. Brussels: RAND Corporation.

Robinson, R. (2018). Intelligence Support for EU Security. Options for Enhancing the Flow of Information and Political Oversinght. SWP Comment 2018/C51, December 2018, 8, 1–8.

Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France

Sviatoslav Kavyn
(Ivan Franko University of Lviv)

Ivan Bratsuk
(Ivan Franko University of Lviv)

Anatoliy Lytvynenko
(Baltic International Academy of Riga, Robert Gordon University of Aberdeen)

S u m m a r y

The events of recent years clearly indicate the existence of a crisis in the field of information security, both at the international and regional levels. Therefore, it seems that a solution is needed to addresss the issues of a proper legislative provision of information security. Currently, there are legal frameworks in the EU in this area, but there is a problem in a certain inconsistency of the EU's legislation in approaches to addressing certain issues of information security, which significantly reduces the effectiveness of legal regulation in this area.

The article is devoted to the study of information security in the EU in the context of the analysis of their state, national programs and regulations. This study analyzes the features of the functioning of the institutional and legal mechanism of information security in the EU in the context of a multi-vector system of international security. The expediency of developing an integrated coordinated information policy of the EU member states in order to unify approaches to information security is substantiated.

Particular attention is paid to the analysis of legal norms that provide effective cybersecurity protection as a component of the information security of the state. In particular, the peculiarities of the functioning of the institutional and legal mechanism of cyber defense in the context of legislative regulation of international cooperation between state institutions and national security structures are analyzed. The necessity of developing a coherent cyber security policy of the European Union in the context of the general information policy of the EU in order to unify approaches to information security and improve the regulatory framework for information security in the field of cyber security is substantiated.

The study analyzes the legal platform for information security and the protection of cyberspace in the formation of the economic security of the European Union as an immanent component of national security, in particular in terms of diversifying external relations in a multi-vector system of international security.

Particular attention is paid to the study of the case law of the European Court of Human Rights in the field of information security. In particular, the case law of the European Court of Human Rights in cases related to the internet is considered.

At the same time, the current realities of European Union policy require comprehensive research in the context of ensuring national interests, developing effective mechanisms for protecting the information space, and legal mechanisms for forming a system of economic security as a strategic factor of national security. Accordingly, the approaches to information security adopted in the European Union are currently not unified due to the geopolitical specifics of the EU. Therefore, the research, evaluation, and implementation of the positive experience of Germany and France in this area are important in building the information security system of the European Union.

Kibernetinio saugumo reguliavimas ir teisinis vykdymas Europos Sąjungos šalyse: Vokietijos ir Prancūzijos patirtis

Sviatoslav Kavyn
(Lvovo nacionalinis Ivano Franko universitetas)

Ivan Bratsuk
(Lvovo nacionalinis Ivano Franko universitetas)

Anatoliy Lytvynenko
(Tarptautinė Baltijos akademija, Aberdyno Roberto Gordono universitetas)

S a n t r a u k a

Pastarųjų metų įvykiai aiškiai rodo esant krizę informacijos saugumo srityje tiek tarptautiniu, tiek regioniniu lygiu, todėl kyla tinkamo teisinio informacijos saugumo reguliavimo būtinybė. ES šioje srityje yra teisiniai pagrindai, tačiau problema – ES teisės aktų neatitiktis sprendžiant tam tikrus informacijos saugumo klausimus, o tai mažina šios srities teisinio reguliavimo efektyvumą.

Straipsnis skiriamas informacijos saugumo studijoms ES, todėl jame analizuojamos ES valstybės, jų nacionalinės programos ir reglamentai. Analizuojami informacijos saugumo institucinio ir teisinio mechanizmo veikimo ES ypatumai daugialypio tarptautinio saugumo sistemos kontekste. Pagrindžiamas integruotos suderintos ES valstybių narių informacijos politikos kūrimo tikslingumas siekiant suvienodinti požiūrį į informacijos saugumą.

Daug dėmesio skiriama teisės normų, užtikrinančių veiksmingą kibernetinio saugumo, kaip valstybės informacijos saugumo sudedamosios dalies, analizei. Visų pirma analizuojami kibernetinės gynybos institucinio ir teisinio mechanizmo veikimo ypatumai valstybinio institucijų ir nacionalinio saugumo organizacijų tarptautinio bendradarbiavimo teisinio reguliavimo kontekste. Pagrindžiama būtinybė kurti nuoseklią Europos Sąjungos kibernetinio saugumo politiką atsižvelgiant į bendrą ES informacijos politiką: tuo siekiama suvienodinti požiūrį į informacijos saugumą ir pagerinti informacijos saugumo reguliavimo sistemą kibernetinio saugumo srityje.

Tyrime analizuojama teisinė informacijos saugumo ir elektroninės erdvės apsaugos platforma formuojant Europos Sąjungos ekonominį saugumą kaip imanentinis nacionalinio saugumo dėmuo, ypač kalbant apie išorės santykių įvairinimą daugialypėje tarptautinio saugumo sistemoje.

Ypatingas dėmesys skiriamas Europos Žmogaus Teisių Teismo praktikos informacijos saugumo srityje studijoms. Visų pirma atsižvelgiama į Europos Žmogaus Teisių Teismo praktiką bylose, susijusiose su internetu.

Atsižvelgiant į dabartinės Europos Sąjungos politikos realijas reikia išsamaus tyrimo siekiant užtikrinti nacionalinius interesus, sukurti efektyvius informacinės erdvės apsaugos mechanizmus, teisinius ekonominio saugumo sistemos formavimo mechanizmus, kaip strateginiam nacionalinio saugumo veiksniui. Europos Sąjungos valstybių požiūris į informacijos saugumą nėra vienodas dėl geopolitinės ES specifikos. Kuriant Europos Sąjungos informacijos saugumo sistemą itin svarbu tirti, vertinti ir įgyvendinti teigiamą Vokietijos ir Prancūzijos patirtį šioje srityje.

Anatoliy A. Lytvynenko is a PhD candidate and teaching assistant at the Ivan Franko National University of Lviv, a PhD candidate at the Faculty of Law of the Baltic International Academy in Riga, and a PhD candidate at the Robert Gordon University of Aberdeen. In 2022, he will be defending his doctoral thesis titled *The Concept of Sensitive Personal Data: A Comparative Analysis of National and International Case-Law*. In 2018, he began his PhD studies at the department of Law at RGU University of Aberdeen, Scotland under the specialty of medical law. The preliminarily title of his forthcoming doctoral thesis is *Could Various Rights of Patients be Summoned under the Umbrella of the Right to Autonomy?* His main research interests include medical law, data privacy law, history of law, bioethics law, and banking law.

Anatolijus A. Lytvynenko yra Lvovo Ivano Franko nacionalinio universiteto doktorantas ir dėstytojas, Baltijos tarptautinės akademijos Rygos teisės fakulteto doktorantas ir Aberdyno Roberto Gordono universiteto doktorantas. 2022 m. jis gins daktaro disertaciją „Slaptų asmens duomenų samprata: lyginamoji nacionalinės ir tarptautinės teismų praktikos analizė“. 2018 m. įstojo į doktorantūrą Aberdyno Roberto Gordono universitete, Škotijoje, pagal specialybę medicinos teisė. Jo doktoranto darbas preliminariai vadinamas „Ar įvairios paciento teisės gali būti surinktos po teisės į autonomiją skėčiu?“. Pagrindinės autoriaus mokslinių tyrimų kryptys yra medicinos teisė, duomenų privatumo teisė, teisės istorija, bioetikos teisė ir bankų teisė .