ppi 201502ZU4645
Publicación científica en formato digital
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185
Depósito legal pp 197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.40 | Nº 74
2022

Cuestiones Políticas Vol. 40, Nº 74 (2022), 585-606
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Peculiarities of personal data protection according to European and Ukrainian legislation

DOI: https://doi.org/10.46398/cuestpol.4074.32

Larysa Didenko *
Ekaterina Spasova **
Iryna Mykhailova ***
Olena Tserkovna ****
Volodymyr Yarmaki *****

Abstract

The article analyzes the peculiarities of the development of legal regulation of personal data protection in the EU countries and Ukraine. It analyzes how the European legislator's approach to personal data protection has changed. The need for changes was due to the development of information technologies and, as a result, increased risk of their use to interfere in private life. As a result, European legislation on personal data protection has been strengthened, which has become particularly noticeable after the adoption of the General Data Protection Regulation (hereinafter - GDPR). Special attention is paid to the principles of lawful, fair and transparent processing of personal data concerning: limiting the target; data minimization; accurate and up-to-date processing; limiting the storage of personal data in a form that allows identification; confidentiality and security of data storage; accountability and responsibility. The current Ukrainian legislation on personal data protection is analyzed. Finally, the correlation between the categories "right to privacy" and "personal data protection" was studied.

Keywords: personal data; information; private life; GDPR; right to privacy.

* Doctor of Law, Associate professor, Professor of the Department of Civil and Economic Law and Process of the International Humanitarian University, Odesa, Ukraine. ORCID ID: https://orcid.org/0000-0002-6806-5017

** Ph.D., Associate Professor of Civil Law Department of National University "Odessa Law Academy", Odesa, Ukraine. ORCID ID: https://orcid.org/0000-0002-8126-2306

*** Ph.D., Associate Professor, Professor of Department of Labor, Land and Commercial Law Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. ORCID ID: https://orcid.org/0000-0002-1273-3389

**** Ph.D., Associate Professor of the Department of Civil Law, Odessa State University of Internal Affairs, Odesa, Ukraine. ORCID ID: https://orcid.org/0000-0001-7923-8553

***** Ph.D., Associate Professor of the Department of Constitutional and International Law of the Educational and Scientific Institute of Law and Cybersecurity of the Odessa State University of Internal Affairs, Odesa, Ukraine. ORCID ID: https://orcid.org/0000-0001-5924-1085

Recibido el 09/07/22 Aprobado el 09/09/22

Peculiaridades de la protección de datos personales según la legislación europea y ucraniana

Resumen

El artículo analiza las peculiaridades del desarrollo de la regulación legal de la protección de datos personales en los países de la UE y Ucrania. Se analiza cómo ha cambiado el enfoque del legislador europeo en materia de protección de datos personales. La necesidad de cambios se debió al desarrollo de las tecnologías de la información y, como resultado, a un mayor riesgo de su uso para interferir en la vida privada. Por ello, se ha reforzado la legislación europea en materia de protección de datos personales, lo que se ha hecho especialmente notorio tras la adopción del Reglamento General de Protección de Datos (en adelante – RGPD). Se presta especial atención a los principios de tratamiento lícito, leal y transparente de los datos personales en lo concerniente a: limitar la meta; de minimización de datos; de procesamiento preciso y actualizado; de limitar el almacenamiento de datos personales en una forma que permita la identificación; de confidencialidad y seguridad del almacenamiento de datos; de rendición de cuentas y responsabilidad. Se analiza la legislación ucraniana vigente en materia de protección de datos personales. Finalmente, se estudió la correlación entre las categorías «derecho a la privacidad» y «protección de datos personales».

Palabras clave: datos personales; información; vida privada; RGPD; derecho a la privacidad.

Introduction

Increasing globalization and the development of the information society lead to the need to protect the private sphere of human life. The ability of a particular state to ensure the personal data protection determines its ability to be a guarantor of the relevant human rights and freedoms. However, human progress is increasingly identifying issues that need to be addressed. Therefore, the regulatory framework must be constantly updated, adapted to the latest technologies, especially if they put at risk interests of the whole society.

European Union law stipulates that the protection of individuals with regard to the processing of personal data is a fundamental right.

The issue of personal data protection from unauthorized processing is regulated, first of all, by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Ukraine joined it in 2006. Since then, the Verkhovna Rada has adopted the Law on Personal Data

Protection, given the relevant powers to the Verkhovna Rada Commissioner for Human Rights, and established measures of responsibility for violating legislative prohibitions. However, the right to privacy enshrined in the Constitution of Ukraine is still not fully guaranteed.

Economic and social integration as a result of the functioning of the internal market has led to a significant increase in cross-border flows of personal data. The exchange of personal data between public and private entities, including individuals, associations and businesses at the level of the EU, has increased.

Rapid technological development and globalization are creating new challenges for the protection of personal data. The scale of the collecting and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to use personal data on an unprecedented scale in order to carry out their activities. Individuals are increasingly providing access to personal information to the public. Technology has changed both the economy and public life and should further promote the free movement of personal data within the the EU and their transfer to third countries and international organizations, while ensuring a high level of personal data protection.

Due to the emergence of the phenomenon of cross-border flows of personal data, there is an urgent need not only for legal regulation of personal data protection, but also for an effective mechanism of strict coercion for violations of personal rights. For this purpose, on April 26, 2016, the EU Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data protection regulation) was approved, which came into force on May 25, 2018.

Despite the fact that Ukraine does not have the status of a full member of the EU, according to the Regulation, the GDPR also applies to Ukraine in specific cases. This means, in turn, that European market-oriented businesses in Ukraine must adjust in detail their policy and process of processing and collecting personal data in accordance with the GDPR, and keep in mind that temporary difficulties in establishing a way to bring them to justice under the Regulation are not a reason to ignore the relevant rules.

One way or another, violators will face adverse consequences in the form of fines, termination of cost contracts with EU entities, and so on. In addition, given the granting of Ukraine the status of a candidate for EU membership, there is an urgent need to adapt Ukrainian legislation to European requirements, including in the field of personal data protection.

1. European Union legislation on personal data protection

Legislation on confidentiality and protection of personal data in the EU has changed significantly over the last two decades. The high-network world we live in today began to take shape in the mid-1990s. The Internet was still a fairly new concept for many people. Most companies had no websites. Concepts such as online platforms or online media did not exist and no one considered the issue of regulating the activities of such resources.

Smartphones, the latest technology and artificial intelligence have made a huge step in the development of mankind over the last 20 years due to new ways of obtaining and processing data. Accordingly, when something new appears in our society, the question immediately arises as to how this concept is enshrined in law, what risks can be predicted, whether fundamental human rights are violated, who is responsible for the violation, and so on.

As a result, courts and regulators have increasingly had to adapt old data protection laws to meet the ever-changing world.

Although basic international regulations already enshrine the basic principles of personal data protection and privacy, a clear mechanism for protecting the infringed right is always needed. Accordingly, for the EU states, the legislation should be uniform in the first place.

On January 28, 1981, Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted. This document set out the key principles of personal data processing, the rights of the individual in connection with the processing of personal data, the basic rules for cross-border data transfer. In 2001, the Additional Protocol to this international agreement was adopted, which detailed the provisions of the Convention on cross-border data transfer and contained new provisions on the need for the Parties to establish a supervisory body to monitor compliance with personal data protection legislation (Bem and Horodyskyi, 2018).

According to EU law, the right to protection of personal data is defined as one of the fundamental rights. This is confirmed in Article 16 of the Treaty on the Functioning of the EU (EU Member States, 1957), as well as in Art. 8 of the EU Charter of Fundamental Rights (European Commission, 2000).

Previously, the main legal act on personal data protection was the Data Protection Directive 95/46/EC adopted in 1995.

The provisions of Directive 95/46/EC did not provide for a strong data protection mechanism, and given the rapid technological development, it is necessary to create legislation that would be flexible even in the event of unforeseen technological changes. Accordingly, new legislation was

adopted in 2016 to adapt data protection rules to the digital age.

The General Data Protection Regulation (Regulation (EU) 2016/679) is a regulation within the framework of European Union legislation on the protection of personal data of all persons within the European Union and the European Economic Area. It also applies to the export of personal data outside the EU and the EEA. The GDPR is primarily intended to give EU citizens and residents control over their personal data. The Regulation replaced the 1995 Data Protection Directive and contains provisions and requirements for the processing of personal information of data subjects within the European Union (Presidency of the Council of the EU, 2015).

The GDPR is a regulation, not a directive, it does not require national governments to enact laws that make it effective, and it is directly binding and enforceable (Blackmer, 2016).

The EU's General Data Protection Regulation (GDPR) is the most important change in the regulation of data confidentiality over the last 20 years. The regulation allowed to fundamentally change the way data is processed in each sector - from healthcare to banking and beyond.

The regulation provides for clarifications and updates that will facilitate the operation of EU data protection law in the next decade. There have also been major changes in the burden of liability for violations of EU law. The regulation provides for significant fines of up to € 20 million, or 4% of annual global turnover, for enterprises in the previous financial year, whichever is higher.

In addition to the GDPR, the EU adopted other regulations that affect confidentiality and data protection. The first of these documents is Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (European Parliament and the Council of the EU, 2016). The NIS Directive is the first adopted at the level of the European Union on the protection of network and information systems (European Parliament and of the Council of Europe, 2016).

The adopted Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (European Parliament and the Council of the EU, 2019) may be revolutionary in understanding the nature of personal data.

EU Directive 2019/770 aims to strengthen consumer protection online and amends EU legislation on consumer protection in the digital single market and the New Consumer Policy package. The Directive covers agreements between traders and users in which a trader supplies or undertakes to supply digital content or a digital service in exchange for a price or the provision of personal data.

The directive should apply in cases where the consumer opens an account on a social network and provides a name and e-mail address. It should also apply where the consumer consents to the processing for marketing purposes of any material constituting personal data, such as photographs or publications uploaded by the consumer. Some scholars tend to consider say that the Directive actually recognizes personal data as a "currency" in the digital world (Nekit, 2020; Nekit, 2020).

There is a special body in the EU for proper compliance with personal data protection legislation - the European Data Protection Board (EDPB). The Council is an independent European body that promotes the consistent application of data protection rules throughout the European Union and promotes cooperation between EU data protection authorities.

The European Data Protection Board consists of representatives of national data protection authorities and the European Data Protection Supervisor (EDPS). The Council aims to ensure the consistent application of the general data protection provisions in the European Union.

According to the reports of the European Data Protection Board, the greatest threat to individual freedom and dignity stems from the excessive information capacity of certain companies or controllers and the ecosystem of trackers and targets who are able to collect and use personal information (Kalitenko *et al.*, 2021). Just three months before the GDPR became completely coercive, the misuse of personal data became the main news and the subject of official investigations not only in the European Parliament but also internationally.

2. Principles and rules of personal data protection under the GDPR

Since in the Big Data era, legal relations arise at the intersection of jurisdictions, the personal data of any person, including a citizen of Ukraine, may be processed by economic entities of the EU, USA, etc. in accordance with the rules of these countries. Similarly, individuals and legal entities of Ukraine may process personal data of such persons by providing services via the Internet to personal data subjects from EU Member States.

Analysis of the provisions of the Regulation allows us to conclude that although Ukraine is not a member state of the EU, but the rules enshrined in the GDPR may directly affect the subjects of its jurisdiction (Kovinko, 2019).

The emergence of "Big Data" is attributed to Clifford Lynch, editor of the journal Nature, after the publication in September 2008 of a special issue. "Big Data" originated by analogy with the common concepts in the

business environment Big Oil and Big Ore. The emergence of "Big Data" indicates that the view of business has shifted from the extraction of natural resources to the extraction of information that has become a more valuable resource than natural raw materials (Oleksin, 2017).

The term "Big Data" is understood to mean a more powerful form of data mining based on huge amounts of information, high-speed computers and the latest analytical methods that can detect hidden and sometimes even unexpected correlations between facts and phenomena of reality (Kardash, 2019).

The provisions of the GDPR came into force on May 25, 2018. On the eve of the entry into force of the GDPR (April 2018), there was an interesting trend in Ukraine: a large number of companies providing services or selling goods to people in the EU suddenly mentioned that the GDPR was adopted two years ago. That made Ukrainian companies to panick and begin the process of bringing their activities in line with the requirements of the Regulation.

It should be agreed that the GDPR is a progressive normative document that significantly increased the level of personal data protection both in the EU and abroad. The Regulation restores the trust of the user, which allows businesses to quickly use the opportunities in the single European market of goods and services, in particular, in the field of information technology (Vanberg, 2021).

According to Art. 4 of the Regulation, "personal data" means "any data relating to an identified or identifiable individual (data subject); an identifiable natural person is an identifiable person, directly or indirectly, in particular by identifiers such as name, identification number, location data, online identifier or one or more factors that determine physical, physiological, genetic, mental, economic, cultural or social essence of such an individual.

Regarding the processing of personal data, it covers any operation or series of operations with personal data or sets of personal data with or without automated means, such as collection, registration, organization, structuring, storing, adapting or modifying, searching, reviewing, using, disclosing through transmission, distribution or otherwise, arranging or combining, restricting, erasing or destroying. Restriction of processing means the designation of stored personal data in order to limit their processing in the future.

The regulations introduced new concepts to the subject composition and processing of personal data, like controller, operator, processor, Data Protection Officer. In order to clearly distinguish between the concepts of controller and processor, it is necessary to start from the purpose of personal data processing. If an individual, company or institution sets the

purpose and means of personal data processing, it is the controller (data owner). If it processes data on behalf of the controller, it is the operator (data controller). The GDPR requires the appointment of Data Protection Officers (Hoofnagle *et al.*, 2019).

The processing of personal data is based on a number of principles that determine the legal basis for its implementation. These principles are set out in Art. 5 of Convention 108, Art. 6 of Directive 95/46/EC and Art. 5 of the Regulations. In fact, the principles are the rules that must be followed (with minor exceptions) by any owner in the course of any processing to which these documents apply (Vynogradova, 2006).

The principles of personal data processing are set in Art. 5 of GDPR, according to which personal data:

1. Must be processed in a lawful and transparent manner in relation to the data subject (legality, legitimacy and transparency).
2. Must be collected for specified, clear and legitimate purposes and not further elaborate in a manner incompatible with such purposes; further elaboration to achieve the objectives of the public interest, the objectives of scientific or historical research or statistical objectives cannot be considered incompatible with the primary objectives (target restriction).
3. Must be considered sufficient and appropriate and limited to only necessary, taking into account the objectives of the processing (data minimization).
4. Must be accurate and, if necessary, updated; all appropriate measures must be taken to ensure that inaccurate personal data, in view of the purposes of their processing, are erased or corrected without delay (accuracy).
5. Must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of their processing; personal data may be stored for longer periods as long as they are processed solely for public interest, scientific or historical research or statistical purposes, subject to appropriate technical and organizational measures provided by the Regulation to guarantee the rights and freedoms of the data subject (storage restrictions).
6. Must be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and against unintentional loss, destruction or damage, using appropriate technical and organizational tools (integrity and confidentiality).

To these principles the principle of accountability is added: the controller is responsible for adhering to the above principles and must be able to prove it (accountability).

It is important to pay attention to each of the principles of data processing. Thus, the essence of the principle of lawful, fair and transparent processing of personal data is that the person who collects personal data must have a clear explanation of the purpose for which he or she collects this data and how the data will be used. In addition, at the request of the data subject, details concerning the processing of one's data must be provided. For example, if the subject asks what kind of his or her personal data is stored at a certain enterprise or who holds the position of personal data protection officer in this structure, such information should be available.

It is reflected in details in the case law of the European Court of Human Rights. Thus, according to Art. 8 of Convention 108, interference with the rights guaranteed by it (this is the right to respect for privacy, which includes, inter alia, the right to protection of personal data) is possible only if it is exercised "according to the law". Such a provision not only requires that the relevant measures have a basis, but also requires the quality of such a "law", requiring that it be available to the person concerned and predictable in terms of the consequences of its application (Yesimov, 2013).

The accessibility requirement is usually met if one or another legal act has been made public. With regard to the requirement of predictability, the ECtHR found that a rule is "predictable" if it is worded with sufficient clarity to enable a person to regulate his or her behavior with appropriate assistance (Rotaru v. Romania, 2000).

The principle of goal limitation implies that the processing of information should always have its legitimate purpose. For example, when hiring, the prospective employee usually fills out a questionnaire, which consists of a number of items, but in reality the employer in most cases only needs the name, phone, e-mail and possibly the address to deliver postal items. Thus, this principle states that organizations should not collect any piece of data that does not have a specific purpose.

Clarity of purpose formulation is the main step in ensuring the legality of processing. Thus, any action taken on personal data must meet the specific purpose of their processing. Therefore, it is the goal that sets the basic limits of processing necessary to give the data subject a picture of how the data will be processed, and thus the ability to control their processing.

The purpose of personal data processing cannot be the fact of processing. There are often situations when the goal is "the need to keep records", "accumulation of as much information as possible" and others. In such case, there is a situation where accounting is conducted for the sake of accounting (Bem and Horodyskyi, 2018).

In M.K. v. France (2013) the applicant was detained for theft and fingerprints were taken. Later the case was closed. The applicant asked the prosecutor to remove his fingerprints, but was refused. The courts upheld the prosecutor's decision, given the need to accumulate as many samples as possible to compare and facilitate investigations.

The ECtHR stated that the purpose of the fingerprint processing in that database was so broad that it effectively authorized the collection of fingerprints of the entire population, which was clearly disproportionate. Thus, the State, in the Court's view, went beyond its discretion and did not balance the interests of the individual with the public, which led to violation of Art. 8 of the Convention.

In accordance with the principle of data minimization, organizations must ensure that the data they store and process is adequate, relevant and limited. Today, companies collect a lot of personal information for various reasons, such as understanding consumer demand for certain groups of goods. Based on this principle, organizations should be confident that they retain only the minimum amount of data required for their use (Bhaimia, 2018).

Only data that need to be processed to achieve the goal should be processed and, even if certain data are used to achieve the goal, their processing will be illegal if it can be achieved without processing the data. Moreover, the principle of proportionality should cover the entire process of any processing of personal data.

The processing of personal data must not take longer than is necessary for the lawful purposes for which they were collected or further processed. Also, the level of organizational and technical protection of personal data should be proportional to the nature and volume of personal data processed (Tsekoura and Panagopoulou, 2020).

The principle of accurate and up-to-date processing requires data controllers to constantly verify that the information being processed remains accurate, valid and fit for its purposes. Personal data processed by the owner must be accurate and reliable. This obligation of the owner implies that reasonable steps will be taken by the owner to keep the personal data of the subject up to date, and the personal data subject has the right to ask the owner to correct his personal data. At the same time, certain deviations from this principle are allowed depending on the sphere of activity in question (medical information, information on a person's involvement in the commission of a crime, etc.).

The principle of limiting the storage of personal data in a form that allows identification prevents unnecessary redundancy and data replication. It limits the movement and duration of data storage and requires an understanding of how the subject will be identified if data records are

compromised. In addition, this principle includes the implementation of a special data retention policy, which, inter alia, contains restrictions on the storage of data simultaneously in several places. For example, companies should prohibit their employees from storing copies of the customer list on a local laptop or transferring data to external devices such as USB. That is, having several illegal copies of the same data in several places will be considered a serious violation of the GDPR.

The principle of confidentiality and security of data storage protects the integrity and confidentiality of data by ensuring the reliability of its storage (which applies to IT systems, paper records and physical security). The data collection and processing organization is currently fully responsible for implementing security measures that are commensurate with the risks of individual data subjects. Negligence is no longer an excuse under the GDPR, so companies must spend considerable resources to prevent both intentional and unintentional data breaches.

The principle of accountability and responsibility supposes that organizations should be able to demonstrate at all times to public authorities that they have taken all necessary measures commensurate with the risks faced by data subjects. The level of compliance may be different for each company. It all depends on how big the company is, how many people have access to personal data, how high is the risk of data leakage, etc. (Tikkinen-Piri *et al.,* 2018).

The provisions of the Regulation apply to the processing of personal data, which is carried out for persons who are in the EU at the time of processing, or persons who directly process the personal data of others and are in the EU. The provisions of the Regulation also apply to companies that provide only the possibility of providing services or selling goods to persons located in the EU. In addition, it should be noted that according to the Regulations, belonging to a certain citizenship does not matter. Only the physical presence of individuals or businesses (their representative offices) in the EU matters.

3. Legal regulation of personal data protection in Ukraine

Ukrainian legislation is characterized by the implementation of international standards into the system of principles of data protection, which constitute personal information. The Constitution of Ukraine provides for the right to secrecy of correspondence, telephone conversations, telegraph and other correspondence (Article 31), information privacy (Article 32). A ban on interfering in personal and family life has been established, restrictions on the processing of confidential information have been imposed, and access to personal information and protection of

one's rights have been guaranteed. These instructions are reflected in other legislative acts and are interpreted in the decisions of the Constitutional Court of Ukraine (Baranov *et al.*, 2000).

The decision of the Constitutional Court of Ukraine of January 1, 2012 № 2-rp / 2012 provided an official interpretation of the provisions of Part 2 of Art. 32 of the Constitution of Ukraine, in particular: it is impossible to define absolutely all types of behavior of individuals in the spheres of personal and family life, as personal and family rights are part of natural human rights that are not exhaustive and are implemented in various dynamic property and non-property relations phenomena, events, etc.

The right to privacy and family life is a fundamental value necessary for the full prosperity of a person in a democratic society, and is seen as the right of an individual to independence from the state, local governments, legal entities and individuals. Collection, storage, use and dissemination of confidential information about a person without consent by the state, local governments, legal entities or individuals is an interference in one's personal and family life. Such interference is permitted only in cases specified by law and only in the interests of national security, economic prosperity and human rights (Constitutional Court of Ukraine, 2012).

In view of the above, the Constitutional Court of Ukraine in fact equates personal and private life. Providing clarification of parts 1 and 2 of Art. 32 of the Constitution of Ukraine, the Constitutional Court of Ukraine uses the terms "private life" and "personal life" as synonyms. This decision is a formal source of legal provisions on personal data protection under Ukrainian legislation.

In addition, the Civil Code of Ukraine according to Art. 301, 303, 304, 306, 307, 308 provides for the possibility to protect private rights by all available means, including self-defense (Verkhovna Rada of Ukraine, 2003). The Criminal Code of Ukraine establishes liability for violation of privacy (Art. 182 of the Criminal Code of Ukraine). In this regard, the Criminal Code of Ukraine is more progressive in terms of terminology than even the Constitution of Ukraine, as it uses term "private", not "personal" (Verkhovna Rada of Ukraine, 2001).

By the Law of Ukraine of July 6, 2010, Ukraine ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol. Thus, Ukraine has undertaken to ensure respect for human rights and freedoms, in particular, the right to privacy under Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

In order to specify the human rights guaranteed by the Constitution of Ukraine and determine the mechanisms of its implementation the Verkhovna Rada of Ukraine adopted the Law of Ukraine "On Personal Data

Protection" which entered into force on January 1, 2011. This Law regulates legal relations on personal data protection and processing and aims to protect the fundamental human rights and, including the right to privacy in connection with the processing of personal data (Verkhovna Rada of Ukraine, 2010).

The definition of personal data is given in Art. 2 of the Law "On Personal Data Protection", according to which personal data is information or a set of information about an individual who is identified or can be specifically identified.

In fact, this definition echoes the one, enshrined in Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, which states that it is information relating to a specific or identifiable person. In the GDPR, the concept of "personal data" is expanded, which is determined by current practice, including ECtHR decisions.

Taking into account the experience of the personal data protection system in Ukraine, the Verkhovna Rada of Ukraine adopted the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Improving the Personal Data Protection System", which entered into force on January 1, 2014. This Law, in order to ensure the independence of the Personal Data Protection Authority, as required by the Council of Europe, empowers the Commissioner for Human Rights to monitor compliance with personal data protection legislation.

There are also bylaws approved by the Order of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine:

- Standard procedure for personal data processing, which regulates the basic requirements for the organization of personal data processing by owners, as well as the Clarification approved by the Commissioner of the Verkhovna Rada of Ukraine for Human Rights;
- The procedure for the Commissioner of the Verkhovna Rada to monitor compliance with the legislation on personal data protection, which contains, inter alia, provisions on the procedure for verification by the supervisory authority of persons processing personal data;
- The procedure for notifying the Verkhovna Rada Commissioner for Human Rights about the processing of personal data, which poses a special risk to the rights and freedoms of personal data subjects, about the structural unit or responsible person organizing work related to the protection of personal data during their processing, and also disclosure of the specified information;
- On approval of the Procedure for processing personal data in the information automated system "Accounting for the transfer and

receipt of data from Eurojust", adopted pursuant to the Primary Act "On Ratification of the Cooperation Agreement between Ukraine and the European Organization of Justice" from February 8, 2017, and the International Act "Agreement on Cooperation between Ukraine and the European Organization of Justice" of July 26, 2016.

The Law of Ukraine "On Personal Data Protection" is the main among the whole set of acts aimed at personal data protection in Ukraine. Previous bylaws were adopted for its implementation. The Law of Ukraine "On Personal Data Protection" contains the concept of personal data, their processing, defines the subjects of these legal relations. It establishes the rules of any operations with personal data (automated or non-automated), provides for the powers of regulatory authorities, the possibility of bringing offenders to justice, and so on.

The Law does not apply to the creation of personal databases for personal, creative and journalistic purposes. With regard to journalistic activity, it is worth mentioning the exception when there is a clear and gross violation of the right to respect for the private life of others, because in this case the sanctions provided by law may be applied. There is a fine line between public and private life, between the protection of personal data and freedom of expression. The decision of the European Court of Human Rights in *Von Hannover v. Germany* distinguished between facts that can contribute to the development of a democratic society and those that constitute the sphere of privacy.

Regarding the essence of information protection, another act is also applicable in Ukraine, it's the Law of Ukraine "On Information", according to which information protection is a set of legal, administrative, organizational, technical and other measures to ensure the preservation, integrity of information and proper access to it (Verkhovna Rada, 1992).

Talking about data protection under Ukrainian legislation, the concept of "processing" is of particular importance. After all, it includes the collection, registration, accumulation, storage, adaptation, modification, renewal, use and distribution, depersonalization, destruction of personal data. That is, any transactions with personal data, both in Ukraine and abroad, are automatically recognized as processing personal data.

There is a debate among Ukrainian scholars about the definition of the term "personal data". Thus, V. Bryzhko notes that it is a set or individual information about an individual who is identified or can be identified (Bryzhko, 2004). G. Vynogradova, believes that personal data is a set of documented or publicly announced information about an individual (Vynogradova, 2006).

At the same time, A. Marushchak, in defining the concept of "personal data", uses the term "confidential personal information". However, personal

data may only be considered confidential on the basis of law or at the request of a person. Thus, information concerning the exercise of official authority by a person holding a public office is not confidential. Therefore, personal data should not be equated with confidential. It should also be noted that not all information can be classified as confidential. There are many cases when different laws provide for the openness of certain information, such as information about the position and work contacts, disposal of budget funds, information from open registers, etc. (Marushchak, 2007).

In general, Ukrainian legislation includes more than 3,000 of legal acts, the scope of which covers the processing of information about an individual. However, as a rule, they specify the content of personal data in accordance with the type of legal relations that fall within the scope of their regulation (civil, labor, administrative, criminal procedure, etc.). Therefore, the list of such data differs depending on the scope of the act. The Law of Ukraine "On Personal Data Protection" also does not establish the exact set of information that needs protection, so any information about a person can be perceived as such.

The right to privacy in Ukraine is not just about information privacy. In addition to information privacy, the Constitution of Ukraine also guarantees the inviolability of housing, secrecy of correspondence, telephone conversations, telegraph and other correspondence, and the prohibition of subjecting a person to medical, scientific, and other experiments without his or her free consent. Thus, the most important aspects of privacy protection are reflected in many articles of the Constitution of Ukraine (Kardash, 2019).

Ukraine is on a long way to create a system of personal data protection on the Internet. There is already a need to clarify the provisions of the law on consent to data processing and to strengthen the responsibility of online resources for violations. The first steps in this direction should be the establishment of an independent regulatory body and the implementation of the standards set out in the General Data Protection Regulation into national law.

In November 2018, the two-year Twinning Ombudsman project, funded by the European Union for one and a half million euros, was completed in Ukraine. One of the directions of the project was the reform of personal data protection in Ukraine, and the result of their work was the draft of a new Law on Personal Data Protection, aligned with the regulation of personal data protection in the EU, conclusions and methodologies for effective reform. Unfortunately, as of early 2022, it has not been adopted yet.

Since September 2017, the EU-Ukraine Association Agreement has been in force, the purpose of which is to open the markets of Ukraine and the European Union and to establish cooperation between them. Among

other requirements, Art. 15 of the Agreement requires that the protection of personal data in Ukraine be brought into line with European and international standards.

4. Problems and prospects for improving personal data protection in Ukraine

Personal data, protection is significantly relevant in terms of the development of the information society and the spread of new information and communication technologies that provide real opportunities for total control over human privacy (Kardash, 2019). Considering that, the current model of personal data protection in Ukraine needs to be improved.

Ukraine, which is gradually integrating into the EU, already has the relevant basic provisions aimed at creating a quality system of personal data protection. None the less, Ukraine still needs to do a lot of work, and this applies not only to the actions of the state, but also to the private sector. It is necessary to start with the adoption of a new law or amendments to the existing Law "On Personal Data Protection". These include detailing the "right to forget" and the prohibition of information processing, the addition of the right to temporarily restrict processing and the right to "mobility" of data, as well as the system for filing complaints, individual and collective lawsuits. It is important to introduce the extraterritoriality of the Ukrainian data protection system, i.e. for the law to apply to foreign companies. And for Ukrainian companies, internal information security rules should be developed.

The powers of a specialized body on personal data protection in Ukraine should also be reviewed. Institutionally, it is worthwhile to create a specialized information commissioner (separate from the Verkhovna Rada Commissioner for Human Rights), which would have the appropriate independence.

In addition to conducting inspections and imposing fines, such a commissioner should have a more effective arsenal of legal remedies for supervision in the relevant field. It is necessary to provide for the right to address the court the demand to stop violation of the right to privacy in the field of personal data, the ability to block Internet resources in court. It is also necessary to improve the procedure for notification of the processing of personal data - the notification must be carried out before the start of the relevant actions.

To protect the infringed right, the right to lodge a complaint with the supervisory authority should be provided for. Such a body should be authorized to consider complaints and make appropriate decisions based on the results of investigations.

In order for the data protection provisions to be effective and enforced, the GDPR provided for severe coercion and sanctions for breaches. The smallest amount of the fine according to GDPR is 20 million euros or 4% of the gross income of the controller and / or operator, while in accordance with the legislation of Ukraine, the maximum amount of the fine in the field of personal data protection is 34000 UAH (Kovinko, 2019).

Currently, Ukraine does not have a clear mechanism for imposing fines in accordance with EU legislation. However, it can be predicted that violations of the GDPR by Ukrainian controllers / operators may lead to the following scenarios: refusal to open a foreign bank account if the database contains information about violations of GDPR by individuals or legal entities of Ukraine; prohibition of the subject of EU law to continue the flow or transfer of data in Ukraine (in fact - this is actually the termination of contractual relations); those controllers / operators of Ukraine who comply with the provisions of the Regulation will be more competitive in the market, as they will be more trusted by users and contractors from the EU.

Ukrainian legislation requires, among other things, the adoption of a new Law of Ukraine "On Personal Data Protection", developed taking into account the provisions and practices of the GDPR and EU legislation in the field of ePrivacy. Updated legislation should also provide for:

- increasing the requirements for the security of personal data processing;
- granting individuals, a greater number of rights in relation to their personal data;
- ensuring transparency of personal data processing: individuals should be informed about who, when and how will process their personal data;
- increasing the requirements for the procedure for obtaining the consent of an individual to the collection, use and transfer of personal data;
- marketing mailings (including email, SMS and messengers), calls and other contacts will be allowed only with the consent of the individual (with some exceptions);
- introduction of general rules for the use of cookies, which can be collected only with the prior consent of the individual.

The obligation to maintain a register of personal data processing and, in certain cases, to give a more significant role to the person responsible for compliance with data protection legislation in the company (a position similar to the Data Protection Officer in the EU).

Conclusions

The world practice in the legislative regulation of the private sphere and personal data protection is developing differently, but the necessity to pay attention to data protection and security is constantly growing. As a result of recognition of such necessity the General Data Protection Regulation was adopted in the EU. Over the past years, a number of countries have passed special laws that establish rules for the protection of private data of individuals, the possibility of their circulation and processing.

By adopting stricter regulation of personal data relations, EU Member States have ensured security not only among themselves but also when cooperating with individuals outside the European Union.

Ukraine, which is gradually integrating into the EU, already has the relevant basic provisions aimed at creating a quality system of legal protection of personal data. The Law on Personal Data Protection is the main one for Ukraine. Personal data according to Ukrainian legislation is any information about an individual that allows you to identify a person, and processing is any operation performed with such information.

However, the current model of personal data protection in Ukraine needs to be improved. First of all, it is about the powers of a specialized body that need to be reviewed. Institutionally, it is worthwhile to create a specialized information commissioner, which requires appropriate amendments to the Constitution of Ukraine.

The highlighted results of the study of some theoretical and practical problems of personal data protection related to the adoption of the GDPR help to identify key legal requirements directly related to Ukraine and identify basic aspects needed to adapt Ukrainian legislation to new EU legislation on personal data protection. In particular, it is necessary to take into account the principles of personal data processing defined by the Regulations. Among the principles provided for in the Regulations: the principle of lawful, fair and transparent processing of personal data; the principle of limiting the goal; the principle of data minimization; the principle of accurate and up-to-date processing; the principle of limiting the storage of personal data in a form that allows identification; the principle of confidentiality and security of data storage; the principle of accountability and responsibility.

Therefore, taking into account the experience of the EU, Ukraine must soon bring the legislation in the field of personal data protection in line with the GDPR. In turn, organizations, companies, bodies and institutions should be responsible for any breach in the field of data protection.

Bibliographic References

BARANOV, Alexandr; BRYZHKO, Valeriy; BAZANOV, Yuriy. 2000. Human rights and protection of personal data. KhPG-Folio. Kharkiv, Ukraine.

BEM, Markian; HORODYSKYI, Ivan. 2018. Personal data protection standards in the social sphere. BiV. Lviv, Ukraine.

BHAIMIA, Sahar. 2018. "The General Data Protection Regulation: the Next Generation of EU Data Protection" In: Legal information management. Vol. 18, No. 1, pp. 21-28.

BLACKMER, William. 2016. "GDPR: Getting Ready for the New EU General Data Protection Regulation" In: Information Law Group. Vol. 1. Available online. In: https://www.bib.irb.hr › 904737.0469_001.pdf. Consultation date: 15/06/2022.

BRYZHKO, Valeriy. 2004. "Organizational and legal issues of personal data protection". National Academy of the State Tax Service of Ukraine. Kyiv, Ukraine.

CONSTITUTIONAL COURT OF UKRAINE. 2012. Decision of the Constitutional Court of Ukraine No. 2rp/2012 dated January 20, 2012. Available online. In: http://zakon3.rada.gov.ua/laws/show/v002p710-12. Consultation date: 15/06/2022.

ECHR. 2000. Rotaru v. Romania [GC]. Application No. 28341/95. Available online. In: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}. Consultation date: 15/06/2022.

ECHR. 2004. Von Hannover v. Germany. Application No. 59320/00. Available online. In: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-61853%22]}. Consultation date: 15/06/2022.

ECHR. 2013. M.K. v. France. Application No. 19522/09. Available online. In: https://hudoc.echr.coe.int/fre#{%22itemid%22: [%22001-119075%22]}. Consultation date: 15/06/2022.

EU MEMBER STATES. 1957. Consolidated version of the Treaty on the Functioning of the European Union. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT. Consultation date: 15/06/2022.

EUROPEAN COMMISSION. 2000. EU Charter of Fundamental Rights. Available online. In: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en. Consultation date: 15/06/2022.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EU. 2016. Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0801-20211117. Consultation date: 15/06/2022.

EUROPEAN PARLIAMENT AND THE COUNCILOF THE EU. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148. Consultation date: 15/06/2022.

EUROPEAN PARLIAMENT AND THE COUNCILOF THE EU. 2019. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital service. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770. Consultation date: 15/06/2022.

HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. 2019. "The European Union general data protection regulation: what it is and what it means" In: Information and communications technology law. Vol. 28, No. 1, pp. 65-98.

KALITENKO, Oxana; ANIKINA, Galyna; SPASOVA, Ekaterina; SHAHAKA, Olexandra. 2021. "The restrictions of the freedom of information during the Covid-19 pandemic" In: Cuestiones Políticas. Vol. 39, No. 70, pp. 426-445.

KARDASH, Anna. 2019. "Constitutional and legal protection of personal information (comparative and legal aspect)": Doctoral Thesis. Kharkiv, Ukraine.

KOVINKO, Natalia. 2019. "Extraterritorial effect of GDPR: risks for Ukrainians and practical recommendations for the government" In: Young scientist. Vol. 4, No. 68, pp. 371-374.

MARUSHCHAK, Andriy. 2007. "Information law: access to information". Legal Norm. Kyiv, Ukraine.

NEKIT, Kateryna. 2020. "Personal data and industrial data as objects of the right to property: assessing the possibilities" In: Journal of Civil Studies. Vol. 36, pp. 57-65.

NEKIT, Kateryna. 2020. "Social media account as an object of virtual property" In: Masaryk University Journal of Law and Technology. Vol. 14, No. 2, pp. 201-226.

OLEKSIN, Serhiy. 2017. "Big Data - is personal data a threat?" In: Legal newspaper. Vol. 42, pp. 20-24.

PRESIDENCY of the COUNCIL of the EU. 2015. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) dated June 11, 2015. Available online. In: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Consultation date: 15/06/2022.

TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Iouni. 2018. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies" In: Computer law & security review. Vol. 34, No. 1, pp. 134-153.

TSEKOURA, Talita-Maria; PANAGOPOULOU, Ferenik. 2020. "GDPR: a critical review of the practical, ethical and constitutional aspects one year after it entered into force" In: International journal of human rights and constitutional studies. Vol. 7, No. 1, pp. 35-51.

VANBERG, Aysem Diker. 2021. "Informational privacy post GDPR - end of the road or the start of a long journey?" In: International journal of human rights. Vol. 25, No. 1, pp. 52-78.

VERKHOVNA RADA OF UKRAINE. 1992. "On Information": Law of Ukraine № 2657-XII dated October 2, 1992. Available online. In: https://zakon.rada.gov.ua/laws/show/2657-12#Text. Consultation date: 15/06/2022.

VERKHOVNA RADA OF UKRAINE. 2001. Criminal Code of Ukraine: Law of Ukraine of April 5, 2001 Available online. In: https://zakon.rada.gov.ua/laws/show/2341-14. Consultation date: 12/09/2020.

VERKHOVNA RADA OF UKRAINE. 2003. Civil Code of Ukraine: Law of Ukraine of January 16, 2003 Available online. In: https://zakon.rada.gov.ua/laws/show/435-15. Consultation date: 12/09/2020.

VERKHOVNA RADA OF UKRAINE. 2010. "On Personal Data Protection": Law of Ukraine No. 2297-VI dated June 1, 2010. Available online. In: https://zakon.rada.gov.ua/laws/show/2297-17#Text. Consultation date: 12/09/2020.

VYNOGRADOVA, Galyna. 2006. Legal regulation of information relations in Ukraine. Yurinkom Inter. Kyiv, Ukraine.

YESIMOV, Serhiy. 2013. "Protection of personal data in the context of the development of dynamic systems" In: Scientific Bulletin of the State University of Internal Affairs. Vol. 3, pp. 198–207.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.40 Nº 74

Esta revista fue editada en formato digital y publicada en octubre de 2022, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org