ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito 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.38 | *Nº Especial*

1era Parte
2020

Cuestiones Políticas Vol. 38, Nº Especial (1era parte) 2020, 44-62
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Protection of Personal Information in the Medical Sphere of Social Relations

DOI: https://doi.org/10.46398/cuestpol.38e.02

Mykola O. Yankovyi *
Hanna V. Foros **
Hanna V. Zaiets ***
Olena I. Pluzhnik ****

Abstract

The purpose of the work was to identify the main legal parameters of modern information. As material sources of research at work, not only the Ukrainian regulations in the field of medical relations information are used, but also relevant innovations in the legal regulation of medical information relations, which are produced in the countries of the European Union. It is established that in the normative legal acts of Ukraine, unlike in European legislation, there is no division of information about an individual into general data and vulnerable personal data. The laws of Ukraine do not contain the notion of "public figure", whose limits of criticism, according to the European Court of Human Rights, are broader for an ordinary person. Among the main conclusions, it stands out that, in order to guarantee the freedoms and rights of citizens, it is necessary in the regulations to classify groups, lists of personal data and access to them based on the secret classification to avoid ambiguities. The materials in the article have practical value for graduates of higher education institutions of police and medical specialties, among others.

Keywords: personal health information; right to protection of information; sensitive information; legal relationships, legal regime of medical information.

* Associate Professor, Candidate of Juridical Sciences, Professor at the Department of Criminology and Psychology, Odessa State University of Internal Affairs, Ukraine. ORCID ID: https://orcid.org/0000-0002-5178-084X. Email: m.yankovyi10@politechnika.pro

** Associate Professor, Candidate of Juridical Sciences, Professor at the Department of Cybersecurity and Information Support, Odessa State University of Internal Affairs, Ukraine. ORCID ID: https://orcid.org/0000-0002-9504-3681. Email: foros10@tanu.ro

*** Associate Professor, Candidate of Philological Sciences, Professor at the Department of Linguistic Didactics, Odessa National Polytechnic University, Ukraine. ORCID ID: https://orcid.org/0000-0001-5318-5780. Email: anyazaec@tanu.pro

**** Associate Professor, Candidate of Juridical Sciences, Professor at the Department of Criminal Law and Criminology, Odessa State University of Internal Affairs, Ukraine. ORCID ID: https://orcid.org/0000-0002-3223-2194. Email: 0997060070@ust-hk.com.cn

Recibido: 01/04/2020 Aceptado: 01/08/2020.

Protección de la información personal en el ámbito médico de las relaciones sociales

Resumen

El propósito del trabajo fue identificar los principales parámetros jurídicos de la información moderna. Como fuentes materiales de investigación en el trabajo no solo se utilizan las regulaciones ucranianas en el ámbito de la información de las relaciones médicas, sino también las innovaciones relevantes en la regulación legal de las relaciones de información médica, que se producen en los países de la Unión Europea. Se establece que, en los actos jurídicos normativos de Ucrania, a diferencia de la legislación europea, no existe una división de la información sobre un individuo en datos generales y datos personales vulnerables. Las leyes de Ucrania no contienen la noción de "figura pública", cuyos límites de crítica, según el Tribunal Europeo de Derechos Humanos, son más amplios para una persona común. Entre las principales conclusiones destaca que, para garantizar las libertades y derechos de los ciudadanos es necesario en la normativa clasificar grupos, listas de datos personales y el acceso a los mismos en función de la clasificación de secreto para evitar ambigüedades. Los materiales del artículo tienen valor práctico para los graduados de instituciones de educación superior de especialidades policiales y médicas, entre otros.

Palabras clave: información médica personal; derecho a la protección de la información; información sensible; relaciones legales, régimen legal de la información médica.

Introduction

The relevance of this article is that in general in the Ukrainian legislation the basic norms governing the circulation of personal information of persons were introduced ten or more years ago and have not been significantly revised at the legislative level by now. In contrast to a number of European countries, which have revised internal regulations in accordance with the General Data Protection Regulation since 2018, which came into force on 25 May 2018 and contains provisions and requirements for the processing of personal information of data subjects within the European Union. In addition, when applying to health care facilities, the patient agrees to the processing of their data, but the question arises as to how this data is protected, who has the right to access this personal data. Unfortunately, to date, this issue remains unresolved. All regulations that have been adopted do not cover the concept of vulnerable personal data of the patient and,

in general, there is no legal differentiation of types of personal medical information (Kerimov *et al.,* 2018a).

At the same time, today in Ukraine, in the context of informatization of society, the entire state system is being restructured, with the aim of strengthening the role of analytical activities and as a result of accumulation and analysis of large arrays of personal data, which cannot but affect the collection, storage, analysis and dissemination of data (information). Therefore, the study of problems that arise in the processing of personal medical data and the application of the legal regime of information and medical social relations becomes increasingly relevant today. Issues of personal data are dealt with by such scientists as O.A. Bedenko-Zvaridchuk (2019), V. Brizko andmM. Shvets (2006), O.A. Dmitrenko (2012), K.Y. Ismailov (2020a; 2020b), A.A. Pismenytsky and V.D. Gapoty (2012), A.M. Chernobay (2006) etc.

The purpose of our work is to establish legal parameters that determine the status of subjects that are the owners of medical personal information databases. At the same time, there is a need to find out the ways of legitimizing on the legislative bases of these bases, as well as to determine the extent of legally significant issues concerning categorical apparatus and terminological legal defects that arise in the information and legal circulation in the medical sphere of social relations. In turn, such a direction of the study leads to the formulation of certain proposals to improve the national information law.

1. Materials and Methods

As material sources of research in the work, not only national legal acts in the information sphere of medical legal relations are used, but also corresponding innovations in the legal regulation of medical information relations, which are formed in the states of the European Union. Scientific research publications of scientists working about information and legal regulation of social relations and, in particular, in the medical sphere, are also used (Kerimov *et al.,* 2018b).

The methods which are used in this work are primarily formed under the influence of philosophical dialectics and rely on logical techniques that are often inherent in legal research and legal practice in law enforcement. In particular, the technical and legal method allows to generalize the analytical material aimed at streamlining information social relations in the medical sphere. Materialistic-dialectical approach makes it possible to focus in the work on the disclosure of structurally significant elements of the terminology of information relations, with the simultaneous comparison of their content features with adjacent and close to content categories that

have different legal mode of their turnover (Kerimov *et al.,* 2018c; Lapidus *et al.,* 2018a).

The methodological basis of the study is a set of methods and techniques of scientific knowledge. Their application is due to a systematic approach, which makes it possible to explore problems in the unity of their social content and legal form: logical-semantic method deepens the conceptual apparatus; structural-logical and comparative-legal method was used for the analysis of structural elements; theoretical – for the study and analysis of statistical information, scientific and methodological literature, generalization of information to determine the theoretical and methodological foundations of the study; logical analysis – to formulate the basic concepts and classification; comparative law method was used to compare the rules of foreign law; dogmatic method – to determine the content of legal terms used; concrete-historical – to demonstrate the dynamics of development; statistical method is used to analyze and summarize empirical information related to the research topic; dialectics – to establish the content and features of the constituent elements; empirical methods – to generalize experience; the method of forecasting was widely used in the work in the development of proposals. The empirical basis of the study consists of the laws of Ukraine and other domestic regulations, legal acts of the EU, the Council of Europe, and other international legal documents (Kerimov *et al.,* 2017; Lapidus *et al.,* 2018b).

1. Results and Discussion

1.1. Specifics of protection of personal data in Ukraine and Europe

The effect of the Law of Ukraine "On Protection of Personal Data" extends to all subjects of economic activity in the medical sphere, regardless of the form of ownership and departmental subordination. That is, not only budget health care institutions, but all private and private practitioners should register the databases of their personal data. In this regard, the Resolution of the Cabinet of Ministers of Ukraine dated 06.06.2012 No. 546 "On approval of the electronic register of patients" (Regulation of the Cabinet of Ministers of Ukraine, 2012) adopted by the National Action Plan for 2012 on the implementation of the economic reform program for 2012-2014, which provides for the establishment of an electronic register of patients (Decree of the President of Ukraine, 2010).

The electronic register of patients is the only state information system for collecting, registering, collecting information about a patient, and receiving medical care. The register is created with the purpose of increasing the

efficiency of medical care, ensuring timely delivery of it, modernization of primary medical care. The electronic register of patients does not cancel the registration of forms on paper. Collecting, processing, and entering into the register of patient data will be carried out solely with his consent (Kerimov *et al.,* 2019; Kerimov *et al.,* 2016).

The register is created with the purpose of increasing the effectiveness of medical care, ensuring the timeliness of its provision and the reliability of statistical information. It is the only information system for collecting, registering, storing, storing, updating, using, and disseminating through the dissemination, implementation, transmission, and destruction of information about an individual and his or her medical care. The registry is an information resource of the Ministry of Health, which is conducted using information technology, electronic document circulation and electronic digital signature. It is worth pointing out that institutions of health care of all forms of ownership are obliged to enter in the register information about:

1) An individual contained in the medical records approved by orders of the Ministry of Health.
2) A health care facility in which the patient was provided with medical assistance.
3) The type of medical care provided to the patient.
4) Medicines and medical products purchased for the treatment of the patient at the expense of the state and local budgets.
5) The consent of the patient to processing personal data in the form prescribed by the Ministry of Health.

The main information unit for the register is the form of primary accounting document No 025/o "Medical card of the outpatient patient", approved by the Order of the Ministry of Health of Ukraine dated February 14, 2012 No 110, registered with the Ministry of Justice of Ukraine on April 28, 2012 under No 661/20974 (Medical card of outpatient patient of the Ministry of Health of Ukraine, 2012).

The owners of register are health care institutions. They, with the consent of the patients to process their personal data, enter the information in the register, process it and provide protection of the personal data which are entered in the register. The exchange of information between health care institutions is carried out with the help of a telecommunication network with the provision of information security in accordance with the requirements of the legislation. Sources of registry formation are passport documents or other identification documents and primary records of health care institutions. The register is formed by creating electronic databases to maximize the automation of the accumulation and processing of information. The reason

for entering a physical person (patient) in the register is the fact of the patient's referral to the health care institution and his written consent to the processing of personal data.

The introduction of the electronic registry of patients raises a number of problems due to the lack of qualified staff, the lack of quality computer equipment, the poor quality of Internet services in hospitals and the high cost of maintaining the database, the lack of regulation and the specific order of the destruction of personal data of health workers and patients. It should be emphasized that, according to European standards, personal data is divided into general data (surname, name, date and place of birth, citizenship, place of residence) and personal (sensitive) personal data (physical and mental health data, ethnicity, racial affiliation, attitude to religion, political views, identification codes or numbers, fingerprints, tax status, convictions, images, sexual life, etc.).

There is no such division in the Ukrainian legislation, that is, the distribution of the surname and the name of the person can be carried out only with the written consent of the person. At the same time, the law does not provide for the possibility of distributing personal data if it is of public interest, which is a significant restriction of freedom of speech. This contradicts the provisions of other laws, for example, the Law of Ukraine "On access to public information". The law significantly complicates the regulation of these relationships. For example, it obliges to inform the subject of personal data about inclusion in the database of his personal data. At the same time, according to the Law, any processing of these data and so is possible after obtaining the consent of the subject for such processing. It remains unclear what the expediency of such a double notification, carried out exclusively in writing (Kuznetsov *et al.,* 2018).

In the European Union, on May 25, 2018, new data protection regulations entered into force called General Data Protection Regulation (GDPR) (Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into force of the General Data Protection Regulation, 2018). The regulation updates and modernizes the principles enshrined in the 1995 Data Protection Directive to guarantee the right to privacy. It gives EU citizens more rights as to how their personal information is used. All EU citizens have the right to see what information the company has about them and may require that this information be deleted. Taking into account the aspiration of Ukraine to join the EU, national legislation should also be oriented towards the relevant standards.

Companies operating in the EU should get a clear agreement on the collection of personal information, otherwise they will be faced with high fines. Companies should also provide information to all interested users about any breach of data and notify control authorities within 72 hours. Each EU member state should set up a supervisory authority and these

authorities will work together to ensure that companies comply with the rules. "Changes will give people more control over their personal data and facilitate access to them, designed to ensure that personal information is protected, regardless of where it is sent, where it is processed or stored, even outside the EU, as it often happens on the Internet" (The EU has entered into force new rules for the protection of personal data, 2018).

1.2. Mechanism of action of Ukrainian personal data protection

The Law of Ukraine (2010) "On Protection of Personal Data" applies to all economic entities in the medical sphere, regardless of the form of ownership and departmental subordination. That is, not only budget medical institutions, but also all private clinics and private practitioners should register the bases of personal data held by licensees.

To begin with, we need to find out what kind of information relates to personal data of a person and is processed in medical institutions and privately practiced medical staff? Personal data is the information or set of information about a patient, employee or partner (individual) that allows you to identify this person. Data on which a person can be identified include all passport details, as well as some other information: surname, name and patronymic; age or date and place of birth; residence; identification number (code); social status; benefits according to the law (single mothers, women with children up to three years, Chernobyl's, minors, pensioners, etc.); the fact of applying for medical assistance, receiving medical care or medical services by a person-patient, participating in clinical trials of drugs, etc.

With all these categories, information about a person is more or less confronted in the work of the staff of health care institutions and privately practicing medical staff in the provision of medical care or medical services. In order to reveal the specifics of personal data processing and the creation of personal data bases in a health care institution, one should shift away from understanding when, where exactly and by whom such activities are carried out (Pogosyan *et al.,* 2018).

At the first visit, submission of a resume by the applicant to fill a vacant position or sign any cooperation agreements / memoranda, a person (individual) gives you – a representative of a medical institution or a private practitioner-a medical practitioner most of the personal data mentioned above. Thus, the collection of personal data of a specific person occurs. When filling in the medical, personnel or accounting legal documentation, the processing and systematization of the information received, as well as the introduction of information into the general catalog – the formation

of a database of personal data in a particular direction (Zheltukhin, 2012; Bedenko-Zvaridchuk, 2019).

It should be noted that the personal data of one person (individual) can fall into different bases and bases of your treatment-and-prophylactic institution. Accordingly, processed, systematized, and formed in the database of information will be different employees of your health center. For example, a Doctor Ivanov, an employee of your hospital, filed a staff member with his personal data on employment. During the process, your employee received some medical care or medical service, and his personal data got into the database of patients of your hospital (Pogosyan *et al.,* 2019).

Later, you held a seminar with the participation of a speaker of a leading specialist in his field of medical knowledge – a doctor of the highest category, Ph.D. I.I. Ivanov. After the lecture you paid, you paid the doctor I.I. Ivanov's fee based on the cooperation agreement. And the personal data of your employee has fallen into the database of partners, individuals. Private practitioners usually process, systematize personal data and form them in appropriate bases individually (Portnova and Portnova, 2019).

Processing of personal data is any action or set of actions performed in whole or in part in the information system (automated) and / or in personal data files that are associated with the collection, registration, accumulation, storage, adaptation, modification, renewal, use and distribution (distribution, realization, transfer), impersonation, destruction of information about an individual.

The database of personal data is a named set of ordered personal data in electronic form and / or in the form of personal data files. In a medical institution, personal data of persons can be processed by the person responsible for keeping the personnel records, the medical registrar at the person's address to the medical institution, the medical staff of the departments and offices, the staff of the department of statistics, accounting, private practitioners, etc. (Portnova, 2018; Portnova, 2019).

In accordance with Article 2 of the Law of Ukraine "On Protection of Personal Data" (Law of Ukraine, 2010), the owner of the database of personal data is a natural or legal person, which by law or with the consent of the subject of personal data granted the right to process these data. The BPD owner approves the purpose of processing personal data in this database, establishes the composition of these data and the procedure for their processing, unless otherwise specified by law.

That is, all health care institutions, regardless of the forms of ownership and departmental subordination, as well as private practitioners, are the owners of personal data bases. A personal data base manager is a natural or legal person who has the right to process this data by the owner of the

personal data base or by law. Usually, the manager of the personal data base in a medical institution has an employee, who will be required to process personal data, their formation in the database, updating the data, etc. The list of such persons is given in the answer to the previous question.

A third person is any person, with the exception of the subject of personal data, the owner or keeper of the database of personal data and the authorized state body for the protection of personal data, which the owner or manager of the personal data database transfers personal data in accordance with the law. For example, the third party will be the pharmaceutical company, which handles presents to pregnant women and newborns in the postpartum department. The personal data of the indicated patients are formed in the appropriate base of the hospital, and transferred to this pharmaceutical company.

There are several types of personal data bases in a health facility. The treatment and prevention institution can have three types of databases with sub bases, namely: 1) the database of personal data of employees; 2) the database of personal data of patients; 3) the database of personal data of partners – individuals.

Legally stipulated subjects and the sequence of the registration of the databases of personal data of a medical institution. According to the Law, the registration of personal data bases is carried out by the owner of the personal data base by submitting a corresponding application to the State Service for the Protection of Personal Data. By the time of submission of the respective application, the owner or his authorized person must develop a Regulation on the processing and protection of personal data in a medical institution and appoint responsible persons, to make changes in their job descriptions. The application for the registration of personal data bases indicates:

- Application for entering the database of personal data into the State Register of personal data bases.
- Information about the owner of the database of personal data.
- Information about the name and location of the database of personal data.
- Information about the purpose of processing personal data in the database of personal data.
- Information about other managers of the database of personal data.
- Confirmation of the obligation to comply with the requirements for the protection of personal data established by the legislation on the protection of personal data.

There is a certain procedure for confirming the fact of receiving an application and registering personal data bases. Thus, the State Service for the Protection of Personal Data on the next business day from the date of receipt of the application for registration of the personal data bases informs the applicant about its receipt. Within ten working days from the day the application is received, the State Service for Personal Data Protection decides to register a personal data base or refuse to register. In the case of a positive decision, the owner of the personal data base shall issue a document of the established sample on the registration of the personal data base in the State Register of personal data bases named a certificate.

The State Service for the Protection of Personal Data refuses to register a personal data base if the application for registration does not meet the requirements for the volume and quality of information to be contained in the application. Regarding the rights that a patient or legal representative of a patient has in the processing of personal data, in this aspect, the patient, personally, and lawful representative, in cases determined by law, have the right:

1) Provide voluntary consent to the processing of personal data of a patient.
2) To be informed about the collection and processing of personal data of the patient.
3) Be informed about the location of the database of personal data containing his personal data, its purpose and name, location and / or residence (residence) of the owner or manager of this database.
4) to receive information about the conditions for granting access to personal data, including information about third parties to which his personal data, contained in the appropriate database of personal data, are transferred.
5) Access to their personal data contained in the relevant database of personal data.
6) receive no more than thirty calendar days from the date of receipt of the request, except in cases provided by law, the answer as to whether his personal data is stored in the appropriate database of personal data, as well as to obtain the contents of his personal data stored.
7) Make a motivated request for the change or destruction of their personal data by any owner and manager of this database if these data are processed illegally or are unreliable.
8) to protect their personal data from unlawful processing and accidental loss, destruction, damage in connection with the deliberate concealment, failure to provide or late delivery thereof, as well as

protection against the provision of information that is unreliable or defame honor, dignity and business reputation an individual.

9) Apply for the protection of their rights regarding personal data to bodies of state power, bodies of local self-government, whose powers include the protection of personal data.

10) To apply remedies in case of violation of the legislation on protection of personal data.

The rights of the patient to protect personal data may also be performed by a legal representative.

According to the Civil Code of Ukraine, the legal representative of a person is: 1) parents (adoptive parents) are the legal representatives of their juvenile and infant children; 2) the guardian is a legal representative of a juvenile and a person recognized as incapacitated / disabled. A lawful representative in cases established by law may be another person (The Civil Code of Ukraine, 2003). Disposition of personal data of an individual, limited in civilian capacity or recognized as incapacitated, is carried out by her legal representative (Law of Ukraine, 2010). The following authorities monitor the compliance with the legislation on the protection of personal data within the limits of the powers provided for by law:

- Authorized state body for the protection of personal data – the State Service for the Protection of Personal Data.
- Other bodies of state power and bodies of local self-government.
- parliamentary oversight over observance of human rights with regard to the protection of personal data is carried out by authorized with the rights of people of the Verkhovna Rada of Ukraine in accordance with the law.

Consequently, business entities in the practice of medical practice should remember that now among the controlling bodies that will come to you with planned and unscheduled inspections, there was another government agency – the State Service for the Protection of Personal Data. The occurrence of legal liability is possible in case of violation of the legislation on the protection of personal data by the heads of medical institutions or privately practicing medical workers.

1.3. Legislative regulation of protection of personal data in Ukraine

From January 1, 2012, the Law of Ukraine "On Protection of Personal Data" (Bedenko-Zvaridchuk, 2019) provides for legal liability for violation of the legislation on the protection of personal data, namely: criminal; administrative-legal; civil law. In accordance with the Law of Ukraine (2011) "On Amendments Certain Legislative Acts of Ukraine Regarding Strengthening Liability for Violation of the Personal Data Protection Law" of 02.06.2011, No. 3454-VI the following legislative acts of Ukraine were amended. The Code of Ukraine on Administrative Offenses (1984) is supplemented by Articles 188-39 and 188-40 with the following content: Article 188-39. Violation of legislation in the field of protection of personal data.

Failure to notify or late communication of the subject of personal data about his rights in connection with the inclusion of his personal data in the database of personal data, the purpose of collecting these data and the persons to whom these data are transmitted entails imposing a fine on citizens from two hundred to three hundred tax-free minimum incomes of citizens and on officials, citizens – business entities – from three hundred to four hundred non-taxable minimum incomes of citizens.

Failure to notify or untimely communication of the specially authorized central executive authority on the protection of personal data about the change of information submitted for the state registration of the personal data base entail imposing a fine on citizens from one hundred to two hundred tax-free minimum incomes of citizens and on officials, citizens, subjects of entrepreneurial activity, from two hundred to four hundred tax-free minimum incomes of citizens.

Repeated infringement during the year from the number provided for in paragraphs 1 or 2 of this article, for which the person has already been subject to administrative collection, entails imposing a fine on citizens from three hundred to five hundred tax-free minimum incomes of citizens and on officials, citizens, business entities, from four hundred to seven hundred non-taxable minimum incomes of citizens.

Avoiding the state registration of personal data base entails imposing a fine on citizens from three hundred to five hundred tax-free minimum incomes of citizens and on officials, citizens, subjects of entrepreneurial activity, from five hundred to one thousand non-taxable minimum incomes of citizens. Failure to comply with the law on the protection of personal data of the order of protection of personal data in the database of personal data, which led to unlawful access to them, entails the imposition of a fine of 300 to 1000 tax-free minimum incomes of citizens.

Article 188-40. Failure to comply with legal requirements of officials of the specially authorized central executive body on personal data protection.

Failure to comply with legal requirements of officials of the specially authorized central executive body on the protection of personal data concerning the elimination of violations of the legislation on the protection of personal data, entails imposing a fine on officials, citizens, entrepreneurs from one hundred to two hundred non-taxable minimum incomes of citizens (Guliyev *et al.,* 2018).

Article 182 of the Criminal Code of Ukraine (2001) is set out in the following wording: Article 182. Infringement of privacy.

Illegal collection, storage, use, destruction, distribution of confidential information about a person or illegal alteration of such information, except cases provided by other articles of this Code, shall be punishable by a fine of five hundred to one thousand non-taxable minimum incomes, or correctional labor for a term up to two years, or arrest for a term up to six months, or restraint of liberty for a term up to three years (Gordadze *et al.,* 2018).

The same acts committed repeatedly or if they caused significant damage to the rights, freedoms and interests of a person protected by law, shall be punishable by arrest for a term of three to six months, or restraint of liberty for a term of three to five years, or imprisonment for the same term. Significant damage in this article, if it is material damage, is considered to be such a harm that exceeds the non-taxable minimum income of citizens by one and more times (Allalyev, 2019).

Also, it should not be forgotten that violations in the field of personal data protection may lead to a person being brought to civil liability on a general basis (for example, non-pecuniary damage). The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data requires that the parties to the Convention ensure that personal data subject to automatic processing meet the following requirements:

- received and processed fairly and lawfully; are stored for specified and legitimate purposes and their use is not incompatible with these purposes.
- Adequate, relevant, and not excessive in relation to the purposes for which they are stored.
- Accurate and, if necessary, relevant.
- Are stored in a form that allows the identification of data subjects no more than is required for the purposes for which the data are stored.

In addition, the Convention prohibits the automatic processing of confidential data, such as data revealing racial origin, political views, religious or other beliefs, as well as data on health, sexual life or criminal experience without proper guarantees in domestic law. The Convention imposes strict restrictions and reservations on the application of provisions like those mentioned above. Any restrictions must be prescribed by law and be necessary in a democratic society in the interests of a legitimate aim proclaimed in the Convention, such as national security, public security, or the cessation of a crime. The concept of "necessity", as understood in international human rights standards, considers the proportionality of the achieved goal.

Conclusion

The legislator did not use the definition of personal data that meets European standards. Namely, personal data is divided into general data (surname, name and patronymic, date and place of birth, citizenship, place of residence) and sensitive personal data (health data – history of the disease, diagnoses, etc., biometric indicators ethnicity, attitude to religion, beliefs, affiliation with public associations, identification codes or numbers, personal symbols, signature, fingerprints, voice recordings, photographs, salary or other statutory income data, deposits and accounts in banks , property, the content of the tax return, the credit history, the data on the conviction and other forms of bringing the person to criminal, administrative or disciplinary responsibility; the results of examinations, professional and other testing, etc.), and laws on information, access and protection should prohibit the collection, storage, use and dissemination without the consent of the data subject of the most vulnerable personal data.

The lack of division of information about an individual into general data and sensitive personal data leads to anecdotal consequences. For example, the distribution of any personal data, including even the surname and the name of a person, may only be made with her written consent. And according to Article 6 § 9 of the Law on the protection of "the use of personal data for historical, statistical or scientific purposes may only be carried out in an impersonal manner". That is, you can not specify any personal data, even name and surname, textbooks, or any scientific work!

All three laws do not contain the concept of "Public person", the limits of criticism of which, in the position of the European Court of Human Rights, are wider than the ordinary person. Accordingly, such people may, without their consent, distribute more personal data if they are important to society. From the general prohibition on the dissemination of personal data without the consent of a person in the Access Act, there is an exception only with

respect to persons who are applying for employment or holding elected positions in government bodies or who occupy the position of a public servant, an employee of the local government of the first or second category (Article 6 § 6).

And this exception concerns only the data on the income declarations of these individuals and their family members (among other things, the draft exception concerns still biographical data, but then they were removed). And, according to Article 5 § 4 of the Protection Law, all personal data of a person who claims to take or hold an elective office (in representative bodies) or a civil servant of the first category does not belong to the restricted information. Obviously, these exceptions do not coincide, and both are considerably narrower than the concept of "public person". The law on protection does not at all include the possibility of distributing personal data, if this information is publicly necessary, and this contradicts the laws on information and access.

The situation changed radically in the summer of 2011, when on June 2 parliamentarians adopted a memorandum of understanding "On amendments to some legislative acts of Ukraine on increasing liability for violation of the legislation on the protection of personal data" (the law came into force on January 1, and later the entry into force was postponed). Fines up to 17 thousand UAH did not please anyone, and many rushed to register all sorts of databases. But, firstly, not everyone managed to do this (and many did not know about any registration), and secondly, with "databases" had to face even such "irresponsible" category of citizens as schoolchildren. In particular, many citizens were surprised at the need to sign a "voluntary agreement on the use of all kinds of data on their children to create personal data bases (BPDs) in schools". The fact of such BPD is not particularly surprising as directors also do not want to pay fines.

In addition, in order to ensure the freedoms and rights of citizens, it is necessary to enshrine in regulations the classification of groups, the list of personal data and the mode of access to them, depending on the classification to avoid ambiguity. The materials of the article have practical value for graduates of higher educational institutions of police and medical specialties, lawyers-practitioners, police officers of the criminal unit and specialists in the field of protection of personal information.

Acknoweledgements

The study was conducted within the framework of Scientific research work No. 0116U006767 "Legal and administrative principles of cybercrime" of the Department of Cyber Security and Information Assurance Faculty of Training for Criminal Police of Odesa State University of Internal Affairs.

Bibliographic References

ALLALYEV, Ruslan. 2019. "Religious origins of the rule of law conception in the United States" In: Amazonia Investiga. Vol. 7, No. 14, pp. 212-217.

BEDENKO-ZVARIDCHUK, Olena. 2019. Protection of personal data in the medical sphere in questions and answers. Available online. In: http://www.mif-ua.com/archive/article/25846. Consultation date: 25/07/2020.

BRIZKO, Valeriy; SHVETS, Mykola. 2006. Systematic informatization of law enforcement: European regulations acts and approaches to streamlining information relations in connection with automated data processing. Pan Tot LLC. Kyiv, Ukraine.

CHERNOBAY, Antonina Mykolayivna. 2006. Legal means of protection of personal data of the employee: thesis of the candidate of Law Sciences. National University "Odessa Law Academy". Odesa, Ukraine.

CODE OF UKRAINE ON ADMINISTRATIVE OFFENSES. 1984. Available online. In: https://cis-legislation.com/document.fwx?rgn=8653. Consultation date: 26/07/2020.

DECREE OF THE PRESIDENT OF UKRAINE. 2010. Program of Economic Reforms for 2012-2014: A prosperous society, a competitive economy, an effective state, No. 187. Available online. In: http://zakon1.rada.gov.ua/laws/show/n0004100-10. Consultation date: 26/07/2020.

DMITRENKO, Oleh Antonovych. 2012. "Management information in the context of public administration decisions" In: Economy and State. Vol. 12, pp. 138-140. Available online. In: http://nbuv.gov.ua/UJRN/ecde_2012_12_39. Consultation date: 24/07/2020.

GORDADZE, Guram; KERIMOV, Vagif; GIRUTS, Maksym; POSHIBAEVA, Alexandra; KOSHELEV, Vladimir. 2018. "Genesis of the asphaltite of the Ivanovskoe field in the Orenburg region, Russia" In: Fuel. Vol. 216, pp. 835-842.

GULIYEV, Ibrahim; KERIMOV, Vagif; MUSTAEV, Rustam; BONDAREV, Andrey. 2018. "The estimation of the generation potential of the low permeable shale strata of the Maikop Caucasian series" In: Socar Proceedings. No. 1, pp. 4-20.

ISMAILOV, Karen. 2020a. "To the issue of personal information circulation in the National police databases" In: Fundamental and Applied Researches in Practice of Leading Scientific Schools. Vol. 38, No. 2, pp. 41-45.

ISMAILOV, Karen. 2020b. "Training of police officers to search and analize significant information from open sources (example of chat-bott applications)" In: Sciences of Europe. Vol. 5, No. 48, pp. 17-25.

KERIMOV, Vagif; GORDADZE, Guram; LAPIDUS, Albert; GIRUTS, Maksym; MUSTAEV, Rustam; MOVSUMZADE, Eldar; ZHAGFAROV, Fyrdaves; ZAKHARCHENKO, Maryia. 2018a. "Physicochemical properties and genesis of the asphaltites of Orenburg oblast" In: Solid Fuel Chemistry. Vol. 52, No. 2, pp. 128-137.

KERIMOV, Vagif; LAPIDUS, Albert; YANDARBIEV, Nurdyn; MOVSUMZADE, Eldar; MUSTAEV, Rustam. 2017. "Physicochemical properties of shale strata in the Maikop series of Ciscaucasia" In: Solid Fuel Chemistry. Vol. 51, No. 2, pp. 122-130.

KERIMOV, Vagif; LEONOV, Mikhail; OSIPOV, Alexander; MUSTAEV, Rustam; HAI, Vu. 2019. "Hydrocarbons in the basement of the South China Sea (Vietnam) shelf and structural-tectonic model of their formation" In: Geotektonika. Vol. 53, No. 1, pp. 42-59.

KERIMOV, Vagif; MUSTAEV, Rustam; BONDAREV, Andrey. 2016. "Evaluation of the organic carbon content in the low-permeability shale formations (as in the case of the Khadum suite in the Ciscaucasia region)" In: Oriental Journal of Chemistry. Vol. 32, No. 6, pp. 3235-3241.

KERIMOV, Vagif; MUSTAEV, Rustam; OSIPOV, Alexander. 2018b. "Peculiarities of hydrocarbon generation at great depths in the crust" In: Doklady Earth Sciences. Vol. 483, No. 1, pp. 1413-1417.

KERIMOV, Vagif; RACHINSKY, Mykhayl; MUSTAEV, Rustam; SERIKOVA, Uliana. 2018c. "Geothermal conditions of hydrocarbon formation in the South Caspian basin" In: Iranian Journal of Earth Sciences. Vol. 10, No. 1, pp. 78-89.

KUZNETSOV, Nykolai; KERIMOV, Vagif; OSIPOV, Alexander; BONDAREV, Andrey; MONAKOVA, Aleksandra. 2018. "Geodynamics of the Ural foredeep and geomechanical modeling of the origin of hydrocarbon accumulations" In: Geotectonics. Vol. 52, No. 3, pp. 297-311.

LAPIDUS, Albert; KERIMOV, Vagif; MUSTAEV, Rustam; MOVSUMZADE, Eldar; SALIKHOVA, Irina; ZHAGFAROV, Fyrdaves. 2018a. "Natural bitumens: physicochemical properties and production technologies" In: Solid Fuel Chemistry. Vol. 52, No. 6, pp. 344-355.

LAPIDUS, Albert; KERIMOV, Vagif; TRET'YAKOV, Valentyn; TALYSHINSKII, Rashyd; ILOLOV, Akhmadsho; MOVSUMZADE, Eldar. 2018b. "Extraction of Asphaltite with Toluene" In: Solid Fuel Chemistry. Vol. 52, No. 4, pp. 256-259.

LAW OF UKRAINE. 2010. On the Protection of Personal Data, No. 2297-VI. Available online. In: https://zakon.rada.gov.ua/laws/show/2297-17#Text. Consultation date: 24/07/2020.

LAW OF UKRAINE. 2011. On Amendments to Certain Legislative Acts of Ukraine to Increase Liability for Violations of the Personal Data Protection, No. 3454-VI. Available online. In: https://zakon.rada.gov.ua/laws/show/3454-17#Text. Consultation date: 27/07/2020.

MEDICAL CARD OF OUTPATIENT PATIENT OF THE MINISTRY OF HEALTH OF UKRAINE. 2012. Instruction on filling in the form of primary registration document No. 025/o; Order, Form, Instruction No. 110. Available online. In: http://zakon1.rada.gov.ua/laws/show/z0669-12. Consultation date: 20/07/2020.

PISMENYTSKY, Andriy Antonovych; GAPOTY, Volodymyr Dmytrovych. 2012. General theory of information law. MMD Publishing House LLC. Melitopol, Ukraine.

POGOSYAN, Vardhes. 2018. "Philosophies of social behavior research: meta-analytic review" In: Wisdom. Vol. 11, No. 2, pp. 85-92.

POGOSYAN, Vardhes. 2019. "Change and variability of phenomena in complex social systems". In: Wisdom. Vol. 13, No. 2, pp. 95-103.

PORTNOVA, Irina; PORTNOVA, Tatiana. 2019. "Stylistic features of European architecture of XX – beginning of XXI century in the light of current trends of the time" In: Journal of Mathematics and Computer Science. No. 1, pp. 51-60.

PORTNOVA, Tatiana. 2018. "Synthesized nature of fine arts and ballet theater: System analysis of genre development" In: European Journal of Science and Theology. Vol. 14, No. 5, pp. 189-200.

PORTNOVA, Tatiana. 2019. "Information technologies in art monuments educational management and the new cultural environment for art historian" In: TEM Journal. Vol. 8, No. 1, pp. 189-194.

REGULATION OF THE CABINET OF MINISTERS OF UKRAINE. 2012. On Approval of the Regulation on the Electronic Patient Register, No. 546. Available online. In: https://zakon.rada.gov.ua/laws/show/546-2012-п#Text. Consultation date: 22/07/2020.

STATEMENT BY VICE-PRESIDENT ANSIP AND COMMISSIONER JOUROVÁ AHEAD OF THE ENTRY INTO FORCE OF THE GENERAL DATA PROTECTION REGULATION. 2018. Available online. In: http://europa.eu/rapid/press-release_STATEMENT-18-3889_en.htm. Consultation date: 24/07/2020.

THE CIVIL CODE OF UKRAINE. 2003. Available online. In: https://zakon.rada.gov.ua/laws/show/1540-06#Text. Consultation date: 24/07/2020.

THE CRIMINAL CODE OF UKRAINE. 2001. Available online. In: https://zakon.rada.gov.ua/laws/show/2341-14. Consultation date: 26/07/2020.

THE EU HAS ENTERED INTO FORCE NEW RULES FOR THE PROTECTION OF PERSONAL DATA. 2018. Available online. In: https://www.eurointegration.com.ua/news/2018/05/25/7082191/. Consultation date: 21/07/2020.

ZHELTUKHIN, Ehor. 2012. Personal data: Fines for "just because". Available online. In: https://sud.ua/ru/news/publication/39050-personalnie-dannie-shtrafi-za-prosto-tak. Consultation date: 24/07/2020.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.38 NºEspecial

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