To the issue of personal information circulation in the national police databases

K. Ismailov
ORCID: 0000-0001-7765-6591

Odesa State University of Internal Affairs, Odesa, Ukraine

The urgency of the problem under consideration is due to the outdated legal framework of Ukraine in the sphere of personal information circulation, which has been in existence for more than 10 years, given the significant gradual changes that have already taken place and are planned in the legislation of the member states of the European Union. And with the advent of modern information and telecommunication technologies, the issues of processing of personified information become even more urgent in view of respect for fundamental rights and freedoms of citizens.

The purpose of the article is to analyze the current legislation of the European Union and Ukraine in the sphere of the circulation of personal information during the detection, prevention and investigation of offenses.

Research methods. To achieve this goal, a number of scientific methods were used, namely: theoretical - to study and analyze national and international legal acts, scientific and methodological literature, summarize information to determine theoretical and methodological bases of the research; logical analysis - to formulate basic concepts and conduct classification; specific historical - to demonstrate the dynamics of the development of protection of personalized information about a person; dialectics - to determine the content and features of the constituent elements in the sphere of personal information turnover; empirical methods - to summarize the best practices of EU countries.

Results of the research. The article analyzes the recent changes in the EU countries in the field of protection of fundamental rights and freedoms of citizens when processing personal data by law enforcement agencies. Particular attention is paid to the urgency of storing personal data in police databases. The article also gives examples of European countries’ law enforcement models in the area of the circulation of personal information. Attention is drawn to the basic principles of the processing of personal data, which are set out in the documents of the «Data Protection Package» adopted by the European Parliament, namely: legality, fairness and transparency; target restriction; minimizing data; accuracy; storage restrictions; integrity and confidentiality. The main provisions of the normative legal acts of Ukraine are presented, which reflect the norms regulating the sphere of turnover of personal data.

Practical importance. Thus, European legislation in the field of the circulation of personal information, which came into force in May 2018, significantly modernized the existing information relations. It is stated that in different EU countries there is an approach to regulating the timing of personal data retention in police bases, which should be compatible with the rights and freedoms of individuals. Changes in EU law go hand in hand with limiting the timeframes for finding information in police databases and differentiating information based on the nature of the crime, the person’s age, time elapsed, and the person’s behavior. Due to this, the legislator came to a balance between securing the right of privacy and property of a person for his personal data and the need to exercise the statutory functions of the state, performed...
in the interests of national security, protection of human rights and security.

It is necessary to introduce in Ukraine a new model of personal data turnover, which will be based on the modern realities of accumulation, processing, analysis and dissemination of information, by changing the provisions of regulations in the specified field in accordance with the principles set out in the documents of the «Data Protection Package», which provide creating conditions for ensuring a consistent international legal framework for the protection of personal data.

Keywords: personal data; information technologies; databases; data processing.

Introduction

Today, information plays an important role in various fields of human activity, society and in any country in the world, and the issue of collecting information about a person (personalized information) seems to be clearly regulated in both international and national legislation, but with the development of technologies such as the automated search, collection, accumulation, storage, processing, use and analysis or dissemination of information in the practice of law enforcement across countries raises questions about how to find fair balance between public and private interests regarding the processing of personal data.

At the same time, Ukraine's current legal system is closely connected with European development trends, and since the main legislative acts in this field in Ukraine were adopted 10 or more years ago, for example, the Laws of Ukraine «On Information» (1992), «On Protection of Personal Data» (2010), «On Access to Public Information» (2011), or the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (2010), or «On Protection human rights and fundamental freedoms» (1997), and given that there are a number European countries have been reviewing their national legislation in accordance with the General Data Protection Regulation [1], which entered into force on 25 May 2018, and contains provisions and requirements for the processing of personal information of data subjects within the European Union, and has been for several years for Ukrainian legislation, so today it is necessary to review the current national legislation on the circulation of personal data.

At the same time today, in the context of informatization of the society, the restructuring of the system of the National Police of Ukraine is being carried out. This situation causes additional scientific research.

Methodological Framework

The purpose of the article is to analyze the current legislation of the European Union and Ukraine in the sphere of the circulation of personal information during the detection, prevention and investigation of offenses.

To achieve this goal, a number of scientific methods were used, namely: theoretical - to study and analyze national and international legal acts, scientific and methodological literature, summarize information to determine theoretical and methodological bases of the research; logical analysis - to formulate basic concepts and conduct classification; specific historical - to demonstrate the dynamics of the development of protection of personalized information about a person; dialectics - to determine the content and features of the constituent elements in the sphere of personal information turnover; empirical methods - to summarize the best practices of EU countries.

The study was conducted within the framework of the Scientific research work No. 0116U006767 «Legal and administrative principles of cybercrime» of the Department of Cyber Security and Information Assurance of Odesa State University of Internal Affairs.

Results and discussion

In order to clarify in more details the issue of legislative regulation of processing of personal data, it is necessary to determine the fundamental international legal acts that regulate these legal relationships.

For example, the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol thereto, which Ukraine ratified in 2010, and which it has undertaken to cover the main international document in the field of the circulation of personal information to ensure that human rights and freedoms are respected. The mentioned Convention defined the observance of the rights and fundamental freedoms of each person, regardless of their nationality or place of residence, in connection with the automated processing of personal data concerning him, in particular his right to privacy [2, Art. 1]. In this context it is also necessary to highlight Art. 5 (e) of the Convention, which provides that personal data subject to automatic processing must be stored in a form which permits identification of data subjects no longer than is required for the purposes for which they are required [2, Art. 5].

According to Art. 5 of the Convention on the Protection of Human Rights and Fundamental Freedoms, everyone has the right to liberty and security of person. No one shall be deprived of his liberty except in such cases and in accordance with the procedure laid down by law [3, Art. 1]. Also Article 8 of the same Convention stipulates that public authorities may not interfere with the exercise of this right, except when the interference is carried out by law and is necessary in a democratic society in the interests of national and public security or the economic well-being of the country, to prevent disturbance or crime, for the protection of health or morals or for the protection of the rights and freedoms of others [3, Art. 8].

With regard to the basic principles of processing personal data, which are set out in the documents of the «Data Protection Package»:
- legality, fairness and transparency: the data must be processed lawfully, fairly and in an accessible form with respect to the data subject;
Fundamental and applied researches in practice of leading scientific schools - ISSN 2708-0994

Volume 38, Number 2, 2020

- purpose limitation: data must be collected for a definite, specific and legitimate purpose and not subject to further processing that is incompatible with that purpose. Further processing for archiving purposes for scientific, research, historical or statistical purposes may not be incompatible with the original purpose;

- minimizing data: be relevant and limited to data that is relevant and necessary to achieve the purpose for which they are processed;

- accuracy: to be accurate and, if necessary, to keep up-to-date;

- storage restriction: be stored in a form that allows the data subject to be identified for no longer than is necessary for the purpose for which it is being processed;

- integrity and confidentiality: be processed in such a way as to provide adequate protection of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organizational measures [4, p. 42].

The aforementioned «Data Protection Package» includes a separate Police and Criminal Justice Data Protection Directive, which establishes rules for the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection of offenses, including protection against the prevention of threats and public security, also contains rules for the exchange of personal data at national, European and international levels. According to Art. 5 of the mentioned Directive Member States should provide for appropriate time limits for the deletion of personal data or for the periodic review of the need to store personal data. Procedural measures should ensure that these deadlines are met.

Directive in accordance with Art. 6 clearly distinguishes different categories of data subjects into:

- persons for whom there are serious grounds for believing that they have committed or are about to commit a criminal offense;

- persons convicted of a criminal offense;

- a victim of a criminal offense or a person for whom certain facts give rise to believe that he or she may be a victim of a criminal offense;

- other parties to the criminal offense, such as persons who may be called upon to testify in the course of criminal investigations or further criminal proceedings, persons who may provide information about criminal offenses, or contacts or associates of one of the persons who are suspected of committing a crime or committing it [5, Art. 5, Art. 6].

That is, the Directive specifies a direct rule on defining the storage period and reviewing data and delineates different categories of data subjects [5].

Therefore, now it is necessary to amend the Ukrainian legislation in accordance with the principles set out in the documents of the «Data Protection Package», which provide for the creation of conditions for ensuring a harmonized international legal framework for the protection of personal data and includes the following documents:

- Regulation (EU) 2016/679 of 27.04.2016 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation)» [6];

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27.04.2016 «On the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminals, the execution of criminal penalties, and also the free movement of such data and the cancellation of Council Framework Decision 2008/977 / JHA» [5];


International law should also include the case law of the European Court of Human Rights, which in recent years has been demanded to launder, inclining more to respecting democratic principles of individual liberty than to ensuring the security of citizens by law enforcement agencies, by using police personal information collected in the databases.

Particularly interesting in the context of considering our issue is the case of «Gaughran V. the United Kingdom». From the case file, it follows that F. Gogran complained to the court about the removal of his DNA profile, fingerprints and photograph in accordance with the policy of indefinitely storing the personal data of any person convicted of a recorded offense constitutes a disproportionate and unjustified interference with law. respecting his private and family life, provided for by Art. 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms. Thus, in a judgment of the national court of 13 November 2012 it was stated that the storage of the applicant's biometric data by the police constituted an interference with his rights within the meaning of Art. 8 of the Convention, but such interference was proportionate to the offense and the court noted that the applicant's photograph was stored in a separate database not used to identify persons by means of identification technology or otherwise, and the court cited the 11 reasons that justified it, here are some of them:

1. Creating a database of information on convicted felons is a very useful and proven resource in the fight against crime.

2. The rights and expectations of convicted persons differ significantly from those of non-convicted persons.

3. A person can only be identified by fingerprint and DNA sample by an expert using special equipment.

4. Legislation severely restricts the use of data contained in the database.

5. Data retention serves the additional purpose of abandoning a convicted felon.

However, according to the judgment of the European Court of Human Rights in that case, dated February 13, 2020, No. 45245/15, as to whether the reasons given by the national authorities for justifying the measure of indefinite detention were «relevant and sufficient», the Court notes that the more data is stored, the more crimes are uncovered, which is confirmed by statistics. In this context, the Court considers that accepting such an argument in the context of a permanent storage scheme would in practice be tantamount to justifying the retention of information about all the population and their deceased relatives, which would certainly be excessive and irrelevant. The Court also finds

Ismailov, K. To the issue of personal information circulation ...
that the indiscriminate nature of the authority to maintain the DNA profile, fingerprints and photographs of the accused or a person convicted of an offense, even if they were carried out, without reference to the seriousness of the offense or the need for indefinite detention and in the absence of a real review opportunity between competing public and private interests. The Court recalls its finding that the State retained a somewhat broader appreciation of the preservation of fingerprints and photographs. However, this expanded margin is not sufficient to conclude that the retention of such data may be proportionate in circumstances which include the absence of any appropriate safeguards, including the absence of a real review. Thus, the respondent State exceeded the acceptable assessment in this regard, and the delay being delayed is a disproportionate interference with the applicant’s right to respect for his private life and cannot be considered necessary in a democratic society, accordingly, a violation of Art. 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms [8].

Here are some examples of regulating biometric data storage in other countries. Just as in England - Wales, Northern Ireland, Ireland and Scotland provide for permanent retention of personal data. However, there are several states which provide for such information to be withheld until a person dies. This is Austria: five years after death or at the age of 80; Denmark: two years after death or at the age of 80; Estonia: ten years after death; Finland: ten years after death; Lithuania: 100 years after inclusion or ten years after death; Luxembourg: ten years after death; The Netherlands: ten years after death and 80 years after juvenile conviction; Romania five years after death or 60 years; Slovakia: 100 years after date of birth.

Where else is this form used in the following countries: Belgium: 30 years after placement; France: 40 years after serving or after 80 years; Hungary: 20 years after serving the sentence; Latvia: age 75; Poland: 35 years after sentencing; Germany: DNA profiles are reviewed ten years from now and removal is subject to court decision; Italy: 20 years after the incident, but no profile can be retained for more than 40 years; and Sweden: ten years after the sentence [9].

In the national legislation of Ukraine it is possible to distinguish several normative acts in the field of observance of human rights concerning the protection of personal data of individuals. First, it is the Constitution of Ukraine, according to which human rights and freedoms and their guarantees determine the content and orientation of the state’s activities (Article 3); public authorities and local self-government bodies, their officials are obliged to act only on the basis, within the powers and in the manner provided by the Constitution and laws of Ukraine (Article 19); no one may interfere with his personal and family life except in cases provided for in the Constitution of Ukraine (Article 32); The constitutional rights and freedoms of the individual and the citizen cannot be restricted except in the cases provided for in this Constitution (Article 64). Note the provisions of Art. 32 of the Constitution, since its provisions must regulate the legal relationship of the topic we have studied, namely:

- it is not allowed to collect, store, use and disseminate confidential information about a person without his / her consent, except in cases determined by law and only in the interests of national security, economic well-being and human rights.
- Everyone has the right to get acquainted in state authorities, local self-government bodies, institutions and organizations with information about themselves that is not a state or other protected by law.
- Everyone is guaranteed judicial protection of the right to refute false information about himself and his family and the right to seek the removal of any information, as well as the right to compensation for material and non-pecuniary damage caused by the collection, storage, use and dissemination of such false information [10].

For the first time in Ukraine, the right of access to public information was embodied in the Law of Ukraine «On Information» (1992), which regulates relations concerning the creation, collection, receipt, storage, dissemination, destruction and protection of information. The aforementioned law also defines the basic terms: document, protection of information, subject of power, and also established the types of information in content. In 2011, legislators from the law «On information» removed all provisions on access to public information and passed a special law «On access to public information» [11].

With regard to the Law «On Access to Public Information», which defines the procedure for exercising and securing the right of every person to have access to information held by the authorities, other providers of public information specified by that law, and information constituting public information interest, it simplifies and standardizes the order of processing information requests (Article 19), providing that the requester has the right to contact the information manager with a request for information, regardless of whether send him personally or not, without explanation request. However, the request for information may be individual or collective and may be submitted verbally, in writing or in any other form (by mail, fax, telephone, e-mail) at the request of the requester [12].

In order to ensure the unconditional implementation by the executive authorities of the law of Ukraine «On Access to Public Information», the exercise of the constitutional right of a person to freely collect, store, use and disseminate information, Decree of the President of Ukraine of May 05, 2011 No. 547/2011 «Issue of providing executive bodies with public access authorities», which has identified 14 points for the implementation of the said law, here are some of them:

- approve instructions for accounting, storage and use of documents and other material media containing information constituting official information;
- take measures to prevent unauthorized access to the available information on the identity of others [13].

Other clauses of the said decree also do not contain information about the timeliness or mechanism of personal data removal at the initiative of a person.

In addition, in accordance with paragraph 40 of its Regulation, the National Police of Ukraine, in accordance with its tasks, carries out information-search and information-analytical work, as well as processing of personal data within the powers stipulated by law [14]. And according to Part 2 of Art. 26 and § 7 h. 1 Art. 26 of the Law of Ukraine «On National Police», the police updates and maintains up-to-date database (banks) of data included in
All of the above leads to the introduction in Ukraine of a new model of personal data turnover based on the current realities of accumulation, processing, analysis and dissemination of information, by changing the provisions of legal acts in this field. Therefore, it is now necessary to amend the Ukrainian legislation in accordance with the principles set out in the documents of the «Data Protection Package», which provide for the creation of conditions for ensuring a harmonized international legal framework for the protection of personal data.

References

1. General Data Protection Regulation. URL: https://en.wikipedia.org/wiki/%D0%97%D0%BD%D0%B0%D0%B3%D0%B0%D1%81%D0%BD%D0%BE-%D1%82%D0%B5 %D0%B3%D0%B0%D0%BD%D0%B0%D0%B4%D0%B5%D1%80%D0%B0%D0%BD%D0%B2 %D1%81%D0%B0%D0%B7%D0%B0%D0%B1%D0%BD%D0%B8%D0%BD%D0%B0 # cite_note-14

2. On the protection of individuals with regard to the automated processing of personal data: Convention No. 2083/VI of 20.01.1991, No. 108, was ratified by law. URL: https://zakon.rada.gov.ua/laws/show/994/326


8. The Case of ‘Gaughan v. the United Kingdom’ from 02/13/2020 # 45245/15 URL: https://hudoc.echr.coe.int/engh(22%22%22[%22001- 2008/02/22]])

9. The ECHR has declared inadmissible the indefinite storage in the personal database. URL: https://zib.com.ua/en/141566-bezstrokovoe_zberigannya_v_policeyskiy_bazi_zberezhennih_dan.html?fbclid=IwAR07AaOtW53Mn-p55n5Sn5Sm4W0q8hGReixiiK1K1_mGkldd


15. On protection of personal data: the Law of Ukraine of 01.06.2010 № 2297- VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17