S. P. Lapta, PhD in law, associate professor, Kharkiv National University of Internal Affairs
D. V. Pashniev, PhD in law, associate professor, Kharkiv National University of Internal Affairs

INVIOLABILITY OF ELECTRONIC PERSONAL DATA IN THE COURSE OF THE EXAMINATION OR SEARCH

One of the fundamental norms enshrined in the Constitution of Ukraine (the Articles 29, 30) is the right to personal integrity of individuals and security of housing. This right is defined in a number of international acts, particularly in the Art. 3 of the Universal Declaration of Human Rights (1948), the Art. 5 of the Convention on Human Rights and Fundamental Freedoms (1950), the Art. 9 of the International Covenant on Civil and Political Rights (1966), the Art. 289 of the Civil Code of Ukraine and others. The specified detailed normative regulation emphasizes the importance and fundamental nature of inviolability of individuals and the housing, which, according to the Art. 3 of the Constitution of Ukraine, along with several other personal non-property benefits are enrolled to the highest social values and have the appropriate priority.

However, the state can reasonably restrict that right. The list of regulations that allow to do it – is no less impressive and varied: the Laws of Ukraine "On Legal Regime of the State of Emergency", "On State Registration of Material Rights to Immovable Property and Their Limitations", "On Securing Creditors' Claims and Registration of Encumbrances", the Civil Code of Ukraine, the Criminal Procedural Code of Ukraine and others.

At the same time, according to the Art. 8 of the European Convention on Human Rights [1], state authorities can not intervene for private and family life of a person, his home and correspondence, except the cases, when intervention is carried out in accordance with the law and is necessary in a democratic society in

the interests of national security and public safety or the economic welfare of the state, to prevent disorders or crimes, for the protection of health or morals or for the protection of the rights and freedoms of others.

Perhaps the most spread cases of reasonable restrictions of the inviolability of individuals and their housing are those that are carried out during criminal prosecution, and especially during the conduction of such investigative actions as examination and search. Particular attention should be paid to limitations associated with such an object of protection as personal data. This object has been recently under a great attention, the relevant Law "On Personal Data Protection" [2] has been adopted. According to the Art. 2 of this Law the object of protection is information or aggregate data about an individual, who is identified or can be specifically identified.

In modern conditions of the development of computer technologies and their penetration into the normal life of any person, a lot of personal data is processed and stored directly not only in computer devices, but also remotely – in the storages of subjects that provide telecommunication services. However, the access to them is also kept on personal digital devices of a person, such as personal and tablet computers, laptops, netbooks, smartphones, etc. At the beginning of referred service's development, the access to personal information was usually carried out after entering own login and password by a person. Now different technologies are used for making the access of a person to his data, the essence of which is in keeping keys to access to such information on the device. Accordingly, if the device is defined as a personal one without the access of unauthorized persons, the owner should not enter the login and password to access the remote storage of own data each time, because the device makes it independently using the stored keys. Such information may include personal data of not only the owner of the device, but also those referring others, who provided their permission for the access to the owner of the device.

It should be noted that within the criminal prosecution the access to personal data and their sources, their reception and introduction into criminal procedure is

rather strictly regulated by the norms of the Criminal Procedural Code of Ukraine [3] (hereinafter – the CPC).

In particular, according to the Art.168 of the CPC temporary withdrawal of electronic information systems or their parts, mobile terminals of the communication systems for studying physical properties that are significant for the criminal proceedings, shall be carried out only if they are directly specified in the court decree.

The Art. 162 of the CPC establishes a list of items and documents containing secrets protected by the law, including "personal data of a person being in his personal possession or in a personal data base that is held by the owner of personal data". According to p. 5 and p. 6 of the Art. 163 of the CPC temporary access to such data should be available in a particular procedure, by the investigating judge or court's decree.

Legally protected secrets contained in the items and documents, include:

– personal correspondence of an individual and other personal records;

– information that is kept in the carriers and providers of telecommunications, communication, the subscriber, provision of telecommunication services, including reception of services, their duration, content, transmission routes, etc.

However, there are quite often cases in practice, of using the access provided by a computer device to personal data to get them to bypass the procedure defined by regulations. The computer device that is on the search or examination scene, is sometimes perceived by law enforcement officials, not only as a thing that is important for the investigation, physical evidence, but also as a simple mean of the access to other information remotely stored. This is not surprising since the authors faced educational materials containing recommendations that advised to act this way in tactical purposes of the investigation.

This situation has occurred because the norms of the CPC are not directly deny the performance of such measures in the course of defined investigative (search) actions; and generally the procedure of handling computer tools and

related to them information with restricted access is not regulated. And not limited opportunity to view information with restricted access through a device located on the spot of the event, is often perceived by law enforcement officers as open information and, therefore, - the absence of any limitations to familiarize with it.

However, the analysis of procedural norms that has been previously accomplished, clearly implies that the procedure of actions in case of identifying a computer device at the examination or search scene should be the following: this device must be seized and studied during the expertise, and if data specifying the possibility of storing another information on other storages (social networks, clouds, disks, etc.) are found out, then this data can be obtained only by temporary access to items or documents in accordance with the Art. 159-166 of the CPC. This will ensure not only the admissibility of such data as evidence, but the legal procedure of restricting the inviolability of personal data.

References

1. The European Convention on Human Rights amended in accordance with the Protocol No. 14 (CETS no. 194) from the date of entering into force on June 1, 2010 [Internet resource] / European Court of Human Rights. – Access mode : http://www.echr.coe.int/Documents/Convention_UKR.pdf.

2. The Law of Ukraine “On Personal Data Protection” dated from June 1, 2010. No. 2297-VI // Bulletin of Verkhovna Rada of Ukraine. – No. 34. – P. 1188. – Art. 481.

3. Criminal Procedural Code of Ukraine dated from April 13, 2012 No. 4651-VI [Internet resource] / Verkhovna Rada of Ukraine : Legislation. – Access mode: http://zakon5.rada.gov.ua/laws/show/4651-17.