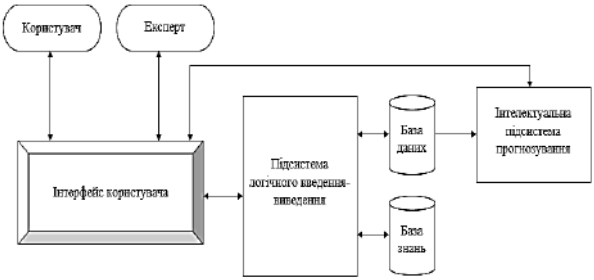

Рис. 1. Структура інформаційної інтелектуальної системи

Література:

1. Бреус Н.М. Інформаційна технологія моделювання морозива: дис. канд. техн. наук: 05.13.06. Київ, 2019. 153 с.

2. Криворучко О.В., Цюцюра С.В. Основи експертних систем: навчальний посібник. Київ: КНТЕУ, 2006. 140 с.

3. ISO/IEC/IEEE 24765:2017. Systems and software engineering – Vocabulary.

4. ISO/IEC 2382:2015. Information technology – Vocabulary – Part 1: Fundamental terms.

DOI https://doi.org/10.30525/978-9934-588-79-2-1.10

BIG DATA AND PROTECTION OF INFORMATION FROM LEAKAGE

Kokhan V. P.
Ph. D, Senior Researcher
Scientific & Research Institute of Providing Legal Framework
for the Innovative Development
of National Academy of Law Sciences of Ukraine
Kharkiv, Ukraine

Big Data is structured, unstructured and semi-structured data of huge volumes and diversity, as well as methods of processing them, which allow distributed analysis of information.

In the world of technology, it is common to define Big Data by describing its distinguishing features. Usually three, four or even five properties of

Big Data are distinguished. The defining characteristics of Big Data are volume (in the value of the physical volume), velocity (in the value of growth rate and the need for high-speed processing and obtaining results), and variety (in the value of the possibility of simultaneous processing of different types of structured and partially structured data). There are also two more characteristics of Big Data – veracity (in the value of the economic effect that the technology provides to users) and value (in the value of the quality of collected data may differ significantly) [1].

Sources of Big Data are referred to [2]:

– Internet – social networks, blogs, media, forums, sites, Internet of Things.

– Corporate data – transactional business information, archives, databases.

– Device readings – sensors, instruments readings, as well as meteorological data, cellular data, etc.

As indicated, Big Data is usually considered not only as data itself, but also as existing technologies for processing large volumes of data from various sources. Technologies such as parsing (the process of collecting information from pages of sites), web crawling (scanning information from a page), web scraping (extracting all kinds of information from a site: texts, images, contact details, prices, etc., which are essentially combined with parsing and crawling) are actively used to collect data from websites.

These data collection technologies are widely used in the digital environment, but are not established by the Ukrainian legislation, as well as the concept and legal regime of «Big Data». In case of controversial situations the well-known rule «Freedom of one person ends where the freedom of another begins» is applied. However, this rule has many reservations and the state information law is subject to application.

In Ukraine, the process of information collection is subject to the rules established for the handling of information, in particular the Law of Ukraine «On Information» [3], the Law of Ukraine «On Access to Public Information» [4], the Law of Ukraine «On Personal Data Protection» [5].

The Law of Ukraine «On Information» divides information into two criteria: by content and by access regime. Moreover, the access regime is determined, inter alia, by its content.

Any information is public, except for information classified as restricted access. Accordingly, it is possible to use any information that is not restricted in access. In turn, the information with restricted access is divided into confidential, secret and official information. The Law of Ukraine

«On Access to Public Information» defines each type of restricted information.

For the time being Big Data has become a valuable economic resource. The collection and processing of Big Data is related to the violation of the confidentiality of company commercial information or personal data of individuals. Therefore, the question of dividing the legal regime of the use of Big Data and confidential data of a person and a company becomes relevant.

Confidential information is information, access to which is restricted by an individual or legal entity, except for the subjects of power of authority, and which can be distributed in accordance with their order according to their desire under the conditions stipulated by them (The Law of Ukraine «On access to Public information»).

Trade secrets may be the information of technical, organizational, commercial, production and other nature, except for those, which in accordance with the legislation can not be attributed to commercial secrets (article 505 of the Civil Code of Ukraine [6]).

Thus, the use of Big Data technologies may lead to the disclosure of trade secrets and the leakage of information that the company deems valuable. It will certainly affect negatively the company's reputation and revenues in the market.

The e-society, e-government, e-democracy and digital services are currently undergoing extensive development. The use of digital services, both private and public, requires the registration of a user on a web resource and the transmission of a number of personal data. In this context, the protection of transferred personal data is an urgent issue.

The protection of personal data should ensure an appropriate and secure environment for the processing and using of information received, prevent third parties from accessing information, and prevent information from leakage.

Cases in which user data enters the digital environment may include [7]:

– linking a person to a separate computer equipment: purchase of computer equipment with the execution of documents, conclusion of a contract with an Internet provider, video recording by the buyer's seller during the purchase of equipment, video surveillance and video recording of the user at an Internet cafe;

– registration on the site through a variety of software applications – entering your name, e-mail, phone number, place of residence (for example, if you order the delivery of goods);

– geolocation inclusion;

– visiting the website, the information is stored and displayed in your browser history;

– displaying data in logs of visits/connections made by hosting providers, etc.;

– the mere use of a computer, phone or other device, being online;

– participation in surveys created with the help of special programs, which, for example, analyze the user's profile on a social network and form the result based on the user's answers;

– adding «friends», geolocation, event participation notes or photo tagging;

– posting photo, video or audio files on pages of websites that are open or closed for sharing;

– messages in messengers, publications, «posts», tweets on social networking sites;

– making search queries about yourself and others;

– making online payments for goods and services;

– saving data in autofill format; remember me tagging, etc.

This list of cases is not exhaustive and includes only the main situations in which information and data about the user could be stored and processed by others.

Parsing, crawling, web scraping, which are used to collect Big Data on the Internet, are in the so-called grey zone from a legal point of view. There is no explicit prohibition on the use of these data collection technologies in Ukrainian legislation, however, as we can see, the result is of their using is a violation of citizens' right to protection of personal data from unauthorized access. A large part of Big Data, one way or another, refers to the collection of information about specific individuals and private or public companies, so the question arises about the need to protect personal data of individuals, and trade secret of companies.

Therefore, now in Ukraine it is still relevant to solve the issue of development of domestic regulations, which should establish the definition of the term «Big Data», the sphere of legal regulation of Big Data, protection of users, define types of penalties for illegal use of Big Data. In addition, the legal regimes for the use of Big Data and confidential data of a person or company should be separated.

The popularization and accessibility of the Internet to a wide range of users, the activities of large corporations in the collection and processing of personal data have force our government to respond to modern challenges

and develop rules under which such processing should be carried out, what rights owners of this information should be provided.

In any case, the protection of personal data remains a challenge for national regulators who need to find a fair balance between the useful collection, processing of Big Data and interests of the individual whose information is being processed and used.

References:

1. Zikopoulos, P., Parasuraman K, Deutsch T., Giles J., Corrigan D. Harness the power of big data the IBM big data platform. McGraw Hill Professional, New York, NY. 2012. 281p. URL: ftp://public.dhe.ibm.com/software/pdf/at/SWP10/Harness_the_Power_of_Big_Data.pdf (accessed 20.06.2020).

2. What is Big Data? URL: https://www.uplab.ru/blog/big-data-technologies/ (accessed 20.06.2020).

3. Law of Ukraine «On Information» № 2657-XII, 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (accessed 20.06.2020).

4. Law of Ukraine «On Access to Public Information» № 2939-VI, 2011. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (accessed 20.06.2020).

5. Law of Ukraine «On Protection of Personal Data» № 2297-VI, 2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (accessed 20.06.2020).

6. Civil Code of Ukraine. 2003. URL: https://zakon.rada.gov.ua/laws/show/435-15 (accessed 20.06.2020).

7. Legal review of cookies or how websites collect information about users. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/pravovyy-poglyad-na-cookies-abo-yak-veb-sayty-zbyrayut-informatsiyu-pro-korystuvachiv-/ (accessed 20.06.2020).