DOI: http://dx.doi.org/10.34069/AI/2020.27.03.42

Certain aspects of personal data protection in the social network: european experience and legislative regulation in Ukraine

ОКРЕМІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНІЙ МЕРЕЖІ: ЄВРОПЕЙСЬКИЙ ДОСВІД ТА ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ В УКРАЇНІ

Received: January 15, 2020 Accepted: February 28, 2020

Written by:
Iryna Davydova[137]
https://orcid.org/0000-0001-5622-671X
Olena Bernaz-Lukavetska[138]
https://orcid.org/0000-0002-2133-1672
Semen Reznichenko[139]

Abstract

The purpose of this study is to examine some aspects of personal data protection in the social network, a comparative analysis of the protection of personal data in the social network under Ukrainian and European legislation, namely the General Data Protection Regulation of the European Union. The methods used in this work are: dialectical, comparative-legal, formal-logical, analysis and dogmatic interpretation. Each of these methods was used in the study to understand and qualitatively explain to the audience categories the individual aspects of personal data protection on the social network. This article reveals the notion of: personal data in the social network, the features of their collection, storage and protection in accordance with European legislation and the development of proposals aimed at improving these processes in Ukraine. The research also addresses the following issues: Features of managing consent to the processing of personal data that have already been obtained; who can act as an "operator" under EU law and what actions he can take; who can act as "controller" and what functions it performs. The article concludes that there is an urgent need to streamline Ukrainian domestic legislation in line with EU law, which should result in a new law on personal data protection that complies with GDPR norms. As a result, a new law on personal data protection may soon emerge in Ukraine, replacing the outdated Law of Ukraine "On Personal Data Protection" of

Анотація

Метою даного дослідження є розгляд окремих аспектів захисту персональних даних у соціальній мережі, порівняльний аналіз захисту персональних даних у соціальній мережі за українським та європейським законодавством, а саме Загальним регламентом про захист даних Європейського Союзу. Методи, що використовувались у даній роботі: діалектичний, порівняльно-правовий, формально-логічний, аналізу та догматичного тлумачення. Кожен з цих методів застосовувався у дослідженні для усвідомлення та якісного пояснення категорій аудиторії окремих аспектів захисту персональних даних у соціальній мережі. Дана стаття розкриває поняття персональних даних в соціальній мережі, особливості їх збирання, зберігання та захисту відповідно до європейського законодавства та розробленні пропозицій, спрямованих на удосконалення даних процесів в Україні. Дослідженням також розкриті питання: особливості управління вже отриманими згодами на обробку персональних даних; хто може виступати «оператором» відповідно законодавства ЄС і які дії він може здійснювати; хто може виступати «контролером» і які функції він виконує. У статті зроблені висновки щодо нагальної необхідності впорядковувати вітчизняного внутрішнього законодавства у відповідності

[137] Doctor of Jurisprudence, Professor of Civil Law Department of National University "Odessa Law Academy"
[138] Candidate in Jurisprudence (Ph.D.) of Civil Law Department of National University "Odessa Law Academy"
[139] Ph. D. in Law, Professor, Odessa State University of Internal Affairs; Ukraine

01.06.2010, which is a “mirror” of the repealed Directive 95/46/EC of the European Parliament and of the Council.

Keywords: confidential information, information, personal data breach, personal data, social networks.

із законодавством ЄС, наслідком чого має стати новий закон у сфері захисту персональних даних, який би відповідав нормам, закріпленим у GDPR. Через це зовсім скоро в Україні може з’явитись новий закон у сфері захисту персональних даних, що замінить морально застарілий Закон України “Про захист персональних даних” від 01.06.2010, який є “дзеркалом” скасованої Директиви Європейського Парламенту і Ради ЄС No 95/46/ЄС.

Ключові слова: конфіденційна інформація, інформація, відтік персональних даних, персональні дані, соціальні мережі.

Introduction

Today, due to the rapid development of information technology and the use of social networks in everyday life, the Internet contains personal data of users that must be protected properly and used solely for the intended purpose and with the consent of the person to whom they belong. Breach of personal data can lead to significant moral and material damage and cause inevitable consequences for both the individual user and the society at large, which also explains the urgent need to protect personal data that goes to social networks.

Since the likelihood of personal data breach is very high, the European Union endeavors use legislation that simplifies the processing, storage and increases the security of personal data. In order to properly and effectively use their rights in Ukraine, it is necessary to study in more detail the international experience in this matter.

Theoretical framework

Given the informatization of society and the creation of a digital environment that envisions the interaction of all subjects, including civilians, we can talk about the formation of an informative, digital society of a new model (quality), in which social networks have become very popular. Social networks aimed at enabling users to share and search information, such as finding old and new friends, classmates, etc. Currently, social networks are perceived by most users as a means of entertainment, communication, and information sharing. Also, the importance of using social networks in the economy is constantly increasing: when organizing various 3D conferences, international presentations, scientific video chats and more.

Most popular nowadays are social networks such as Facebook, Twitter and Instagram, which are widely used for business, not just communication. There is no platform that allows you to make money directly from social networks, but there are a large number of agencies operating in Ukraine that provide services to companies seeking to promote their brand through social networks (Kyryliuk, Baadzhy, Kapustina & Galupova, 2019). SMM specialists (from SocialMediaMarketing), content optimizers, and others are getting high returns. Digital agencies are organizations that develop and promote Internet resources in the media space, including in the social network. Employees of such agencies create sites and organize their optimum work, promote them through digital media and in online communities (forums, thematic sites), etc. In the context of what has been said, it is important to ensure effective protection of personal data of users of the social network, which is one of the main tasks facing society.

For a more detailed study of these issues, the following questions should be answered:

1. What is personal data and how is it determined by Ukrainian and European legislation?
2. Who is a "controller" and what functions does it perform?
3. Who is the "operator" under EU law and what actions can it take?
4. What is meant by "profiling"?
5. What are the features of managing personal data whose permission to process has already been obtained?
6. What is the peculiarity of such rights of personal data subjects as the right to

erasure, the right to mobility, the right to consent to the processing of personal data?

7. How to manage personal data processing consent already obtained and prevent the leakage or theft of such data?

This article is aimed at the theoretical and practical study of personal data in the social network, the features of their collection, storage and protection in accordance with European legislation and the development of proposals aimed at improving these processes in Ukraine. The problem of personal data protection on the social network was particularly acute in early 2018. A large data breach took place at Facebook in 2016-2017. As a result of this event, the personal information of 50 million social network users was removed through a third-party user survey program.

It is believed to be the result of the unlawful activity of a private Cambridge Analytica company that analyzes social networking data to develop an effective election campaign strategy (political consulting). The aforementioned company collected personal data of Facebook users for manipulation of public opinion. Cambridge Analytica has created an algorithm based on personal information that it receives to send targeted mailing. (Kovalchuk, 2018)

As a result, it is argued that Cambridge Analytica's activities significantly influenced the outcome of the 2017 USA presidential election and the outcome of the 2016 referendum in the United Kingdom on leaving the European Union. (David, 2018)

An example of a major breach of personal data is the situation with Marriott International, where hackers gained access to the Starwood Hotels (owned by Marriott) reservation database, which contains customer data from 2014 to 2018. In total, the personal data of 500 million guests using Starwood Hotels was hacked, 327 million of which include passport numbers, dates of birth, e-mail addresses, mailing addresses, dates of check-in and check-out, and in some cases even bank card details. In particular, payment information was encrypted using AES-128, but according to Marriott, the "decryption components" were also stolen. (Oganesyan, 2018a)

Therefore, protection of personal data on the social network is necessary not only for the individual user but also for the society as a whole, since the consequences of the leakage of personal data can have significant both moral and material damage and cause irreversible consequences.

Methodology

General scientific and special methods of scientific cognition were used to prepare the article. They have been selected with regard to the purpose and objectives of the study, its object and subject. The methodological basis of the study was the dialectical method of cognition, which allowed to identify and investigate in their development the features of personal data protection in the social network. The formal-logical method was used to study the legal rules governing the collection, storage and protection of personal data on social networks. The issues explored in the article were addressed through the analysis of laws and the scientific literature. The comparative method was used to compare European and national approaches to regulate the features of collecting, storing and protecting personal data on a social network. The method of logical analysis and dogmatic interpretation of legal norms was used in formulating the conclusions and proposals contained in the article.

Results and discussion

The right to the protection of a person's personal data is a necessary element of human life in the information society. It is a fundamental human right, because in the event of its violation, the person's safety, honor, dignity, etc. are at stake. This right is also derived from the right to prevent interference with privacy and the right to prohibit the collection, storage, use and dissemination of confidential information about a person enshrined in Article 32 of the Constitution of Ukraine.

According to EU law, the protection of individuals when processing personal data is a fundamental right. In particular, Article 8 (1) of the Charter of Fundamental Rights of the European Union states that everyone has the right to the protection of his or her personal data.

In Ukraine, the main legal act that regulates the relations that arise in connection with the protection of personal data on the social network is the Law of Ukraine "On Protection of Personal Data" of 01.06.2010 This law regulates the legal relations concerning the protection and processing of personal data, aimed at the protection of fundamental rights and freedoms of the individual and citizen, including the right to

non-interference with privacy, in connection with the processing of personal data.

However, on 25.05.2018 the General Data Protection Regulation of the European Union (GDPR Rules) came into force, which began to regulate personal data protection relations not only in the EU but also partly in Ukraine. This is made possible by the extraterritoriality principle set out in Article 3 of the GDPR. Namely, GDPR rules apply in the following cases:

1. The controller or the operator of personal data are located within the territory of the European Union, regardless to the place where personal data is processing.

2. The controller or the operator of personal data is located outside the territory of the EU and the holders of personal data (data subjects) are located within the territory of the EU:

a) in the case of free / paid delivery of goods or services to such persons within the EU or
b) when monitoring the behavior of personal data holders within the EU.

3. The controller or the operator of personal data is located outside the EU but in a place where the law of a Member State is applicable under public international law.

So, GDPR Rules covers fully / partially automated processing of personal data of EU citizens in the EU and beyond by natural / legal person, government bodies and other institutions and organizations. In particular, GDPR will be applied to: any, including non-profit, activities related to the processing of personal data; free provision of services to EU citizens; registering on the relevant EU citizen's server and providing them with their personal data; receiving visitors from the EU and collecting cookies by a regular website (although cookies are stored on a user's computer). In addition, in accordance with the Association Agreement on 27 June 2014, Ukraine must harmonize its domestic legislation in accordance with the GDPR Rules.

All of the above makes it possible for Ukrainian natural and legal person, under certain circumstances, to be subject to the GDPR Rules. For example, an IT company that has developed a social network, if there is a user located in the EU, is obliged to process his or her personal data in accordance with the GDPR Rules. This document will also apply to an individual who is located in Ukraine but uses a social network maintained by an EU-based IT company.

The main ideas of GDPR are protection of personal data, restriction of movement of personal data within the EU. The main goals of the GDPR are: to provide individuals with tools to control their personal data, to implement modern standards of personal data protection, to develop an EU digital space for personal data protection, to ensure strict compliance with rules by all parties (including the competent authorities of EU Member States) and legal support for the international transfer of personal data. Which is in line with the urgent need to ensure information security in today's society (Getman, Danilyan, Dzeban, Kalinovsky & Hetman, 2020).

Let us analyze the definitions of the basic concepts enshrined in the GDPR Rules and Ukrainian legislation. Personal data (Art. 4 GDPR) means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data (Article 2 of the Law of Ukraine “On Protection of Personal Data”) is information or a set of information about an individual who is identified or can be specifically identified. This definition corresponds to the definition of "personal data" given in Directive 95/46 / EC 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, which the GDPR Regulations have abolished. Therefore, the definition of personal data set out in the Ukrainian legislation should be changed in accordance with the GDPR Rules.

According to the GDPR Rules, the controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. In

Ukrainian law, the definitions of "controller" and "operator" of personal data are almost identical to the definition of "owner of personal data" and "manager of personal data".

Here is an example of how the GDPR Rules apply to a Ukrainian legal person. Suppose that in Ukraine developed an imaginary social network called "LSN", which gained popularity not only in Ukraine but also in Europe, as a consequence, people who are in the EU, began to actively register in this social network. In this case, the GDPR Rules apply directly to the LSN social network. LSN will be the controller of personal data and Amazon Web Services, Inc. (AWS) will be the personal data operator as it provides hosting services for processing and storing personal data of social network users on AWS servers.

GDPR rules also include the term "profiling", which means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Following the profiling process, personal data is transformed into secondary information, which enables automated decision-making based on primary information. An example would be advertising on the social network Facebook, which almost every one of us has repeatedly encountered, which depends on gender, age, location, etc.

According to Art. 22 GDPR Rules the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The GDPR Rules in Chapter III set out a significant list of the rights of personal data subjects: right of access by the data subject; right to rectification; right to erasure ('right to be forgotten'); right to data portability; right to object; automated individual decision-making, including profiling, etc.

Particular attention should be paid to the erasure right, the right data portability, and the right to consent to the processing of personal data. Right to data portability is the right by which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

The right to erasure of personal data enables the data subject to be "forgotten", ie to require erasure of all personal data. In this case the controller must delete this data without any undue delay. However, this is quite complicated from a technical point of view because even after the removal of personal data, some of it is still stored on magnetic media. Therefore, to ensure full compliance with the GDPR Rules, controllers may encrypt such social media user data and then delete only the encryption key. This method converts data into a completely and forever unreadable array of information. (Nuzhnyy, 2018)

The exercise of the right to consent to the processing of personal data is clearly regulated by the rules of the GDPR Rules: the data subject (user of the social network) must give a clear and explicit consent to the processing of the personal data. Therefore, the generally accepted practice of granting consent by clicking on the "plus sign" or "checkmark" will not comply with the GDPR Rules. This explains how most social networks get their users' consent through a pop-up window with a summary of personal information processing and a consent to such action.

GDPR rules require a volume of privacy policy notice that must be simple, clear and understandable. In practice, it became popular to use two documents: Privacy Policy - the general privacy policy of the social network, and Privacy Notice - a separate part of Privacy Policy, which communicates the scope and purpose of processing personal data. (Tarasyuk, 2018)

To verify a project for GDPR compliance, it is necessary to: 1) determine what personal data is collected for the project, where and how it is stored, processed and used; whether all the data is really needed; if the set of data does not allow the identification of a particular person, then it is not personal data; 2) control the use of personal data, in particular: how, when, by whom and why they are processed; 3) to develop mechanisms for protection of personal data, in particular: to check the reliability against hacking, to allow the limited (necessary) circle of persons to work with personal data, to create a policy of access to the processing of personal data; 4) appoint a staff

member who would understand the legislation and work with users' complaints and EU supervisors; 5) maintain the reporting required by the GDPR Rules.

In addition to obtaining consent, it is also important to manage the consent already obtained.

For example, the Information Commissioner's Office (ICO), in its own guidance on managing the consent received when complying with the GDPR Rules, makes the following requirements:

1) the request for consent must be clear, concise, separate from other terms and easy to understand;
2) should include the name of the organization and any third-party controllers that will be based on consent; explain the purpose of the information collection and describe the actions that will be taken with it; recognize the right of the data subject to withdraw the consent;
3) consent must be given in an active form (without automatically filling in the questionnaire fields or by default);
4) it is necessary to provide a detailed choice of the terms of consent for different purposes of different types of processing;
5) confirmation of the fact of consent has to be kept (data on: the subject who gave the consent, the time of the submission, the method and what was communicated to the subject before giving such consent);
6) the withdrawal of the given consent should be carried out simply (in a simple form);
7) consents obtained must be kept under review and updated in the event of changes that may be part of business processes.

The Law of Ukraine “On Personal Data Protection” has both similar and distinct features with the GDPR Rules, in particular, under Ukrainian law: 1) personal data are processed openly, transparently and solely for the purpose of achieving specific and legitimate purposes, which must be confirmed by the clear consent of the data subject, or expressly provided by applicable law; 2) the purpose of the personal data processing process must be defined in internal documents that regulate the activity of the personal data holder and comply with the current legislation on personal data protection, and the general list and content of personal data must adequately and not excessively meet the purpose of their processing; 3) personal data should be provided in a sufficiently precise and accurate manner and should be regularly updated as necessary for the purpose of processing; 4) the processing of personal data is carried out with the involvement of the means and in a manner that is strictly in accordance with its purpose and purposes, and in case of incompatibility of the previous and the new purpose the data subject must give a new consent to the processing of his personal data in accordance with the new purpose.

Another principle of personal data protection enshrined in the GDPR Rules is "default", which means implementing technical and organizational measures to protect personal data by controllers and operators even before the data is accessed. Technical measures include: application of network protection against unauthorized access to the personal data base, use of data encryption methods and their anonymization, physical and online control of access to data, implementation of multi-stage authorization procedures for employees, etc .; to organizational: measures to determine the order of access of employees to personal data, determine the order of accounting of personal data transactions, the conclusion of NDA and DPA contracts with employees and counterparties, etc. (Dreis, 2015)

GDPR rules also ensure that data is kept confidential. The obligations to protect personal data obtained during the operation of the social network are governed by several articles of the GDPR Rules. To prevent the subject's personal data from leaking to controllers and operators, it is necessary to: protect the data of social network users by default; enter into confidentiality disclosure agreements (NDA) with their contractors and employees; apply cryptographic algorithms for personal data encryption or pseudonymisation; implement security measures for assessing the risks of personal data leakage; take measures when storing data for further processing.

GDPR encryption is stated as a major requirement for data security. This is explained by the fact that organizations need to conduct a risk assessment and, based on that assessment, take measures that would reduce (mitigate) those risks. Given that no organization can fully identify or anticipate all the risks to its data, and no security approach is reliable, organizations must encrypt their data so that they can comply

with GDPR rules and have robust protection in the event of a real threat to personal data. (Nuzhnyy)

In addition, special attention should be paid to the Privacy Policy, which should be given to the individual as a user of the social network, as mentioned above. This document should specify: a list of personal data; purpose of their processing; a list of social network users' rights to their data; the procedure for responding to complaints of users regarding the violation of the terms of use of their personal data.

Analysis of Art. 83 GDPR Rules testify to the seriousness and responsibility of the EU legislator in the obligation to protect personal data, which is expressed in the imposition of severe sanctions for violations of the provisions of this document:

in the event of a breach of the obligations under the GDPR Privacy Policy, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher;
in case of violation of the terms of consent, data subject rights, rules for transfer of personal data to the recipient in a third country or to an international organization, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The case of applying sanctions in practice (though even before the entry into force of these Rules) is the imposition of a fine on the European Uber of $ 1.2 million by the authorities of the United Kingdom and the Netherlands for the breach of personal data of 7 million drivers and 57 million passengers, which happened in 2016. By comparison, USA Uber has agreed to pay $ 148 million for pre-trial settlement. (Oganesyan, 2018b)

In order to protect themselves from such sanctions, persons who fall under the notion of controller or operator of personal data should conduct a general audit of personal data, which should include the definition of: the form and extent of the collection of personal data; a clear list of personal data to which the person has access and which is stored on their own and / or third-party media or information stores; the list of persons to whom personal data may be transferred (which of the person's counterparties may have access to them); the scope, scope and specific uses of the personal data of the person.

Also, in order to reduce the risk of GDPR fines, some companies intend to unify the processing of personal data and delegate these functions to third-party processors. In particular, Google, Microsoft, Twitter and Facebook have already announced a joint Data Transfer Project (DTP) initiative, which is developing a set of specifications, data models, protocols and open frameworks to organize the transfer of data between providers of various online services. That is, in the future, you will be able to switch from one social network to another or from one mail hosting to another, with all user-generated content also automatically moved, including photos, messages, contacts, calendars, etc. (Ajax, 2018)

Conclusion

From the above we can conclude that as of today the protection of personal data on the social network has reached a new qualitative level. After several high profile cases of personal data breach on the social network, the world community has realized that effective protection of personal data is an urgent need today. As a result, in 2016, the European Union adopted the GDPR Rules, which, through their extraterritoriality, can regulate personal data protection relationships even in Ukraine. According to the Association Agreement of June 27, 2010, Ukraine has to regulate internal legislation in accordance with the EU legislation, because of this a new law on personal data protection may soon emerge in Ukraine, replacing the outdated Law of Ukraine “On Personal Data Protection” of 01/06/2010, which is a “mirror” of the repealed Directive 95/46 / EC of the European Parliament and the Council. That is why the study of GDPR rules is well-founded and expedient when covering the features of protection of personal data on the social network.

References

Ajax (2018). OpenNET. Google, Microsoft, Twitter, and Facebook Launch Data Portability Project. Retrieved from: https://www.opennet.ru/opennews/art.shtml?num=48998
David D. Kirkpatrick (2018). The New York Times. Using Digital Firm, Brexit Campaigners Skirted Spending Laws, Ex-Employee Says. Retrieved from: https://www.nytimes.com/2018/03/24/

Dreis Y. O. (09.2015). Personal data protection measures in information (automated) systems. Perspective directions of information protection: materials of the first all-Ukrainian scientific-practical conference. ONAC, Odesa, P. 29-31.

Getman A., Danilyan O., Dzeban A., Kalinovsky Y. & Hetman Y. (2020). Information security in modern society: Sociocultural aspects. Amazonia Investiga, 25(9), P. 6-14.

Kovalchuk O. & Gaida T.Y. & Genet S.Y. (2018). Big Data Technologies in Innovative Marketing. Ukrainian Journal of Applied Economics, Volume 3 (1), P. 36-52.

Kyryliuk A., Baadzhy N., Honhalo R., Kapustina N. & Galupova L. (2019). Protection of copyright on the Internet. Amazonia Investiga, 24(8), P. 464 – 470

Nuzhnyy V. (2018). Channel for IT. New EU requirements for personal data protection from May 2018. Retrieved from: http://channel4it.com/publications/ Nov-vimogi-S-do-zahistu-personalnih -danih-z-travnya-2018-roku-30154.html.

Oganesyan A. (2018a). DeviceLock DLP. The UK and the Netherlands fined Uber $ 1.2 million for the leak of personal data. Retrieved from: https://habr.com/ru/company/devicelockdlp /blog/431256/

Oganesyan, A. (2018b). DeviceLock DLP. Marriott leaked personal data of 500 million customers. Retrieved from: https://habr.com/ru/company/devicelockdlp/blo g/431682/

Tarasyuk A.V. (2018). Information and law. Influence of general data protection regulation on controllers and processors of personal data-residents of Ukraine. Retrieved from: http://ippi.org.ua/tarasyuk-av-vpliv-zagalnogo-regulyuvannya-zakhistu-danikh-na-kontroleriv-ta-protsesoriv-personalnikh