3. ЦИВІЛЬНЕ ПРАВО І ЦИВІЛЬНИЙ ПРОЦЕС. СІМЕЙНЕ ПРАВО. ТРУДОВЕ ПРАВО. МІЖНАРОДНЕ ПРИВАТНЕ ПРАВО. ГОСПОДАРСЬКЕ ПРАВО. ГОСПОДАРСЬКО-ПРОЦЕСУАЛЬНЕ ПРАВО

DOI:10.35774/app2021.03.110
УДК: 347.44:347:78

Hanna Stakhyra,
PhD in Juridical Sciences,
Senior lecturer at the Department of
International Law and Migration Policy
West Ukrainian National University
ORCID: https://orcid.org 0000-0001-6978-4892

Lyudmila Savanets,
PhD in Juridical Sciences,
Docent, Docent at the Department of
International Law and Migration Policy
West Ukrainian National University
ORCID: https://orcid.org 0000-0002-0051-8905

ENSURING THE SECURITY OF PERSONAL DATA ON THE INTERNET: THE COMMERCIAL USE OF PERSONAL DATA BY DIGITAL CONTENT PROVIDERS

Проаналізовано правовий аспект використання соціальними онлайн платформами персональних даних користувачів. Проведено порівняльне дослідження концепції захисту персональних даних у національному та зарубіжному законодавстві. Розглянуто концепцію договору постачання цифрового контенту, відповідно до якої користувач в обмін на цифровий контент передає онлайн платформі свої персональні дані, що можуть бути використані у маркетингових та рекламних цілях. Проаналізовано положення про відповідальність соціальної онлайн платформи за збір та передачу даних про її користувачів іншим особам, в тому числі для реалізації політичних, маркетингових, соціальних, економічних, технологічних стратегій.

Ключові слова: *персональні дані, інтернет, монетизація, цифровий контент, безпека.*

Стахира Г. М., Саванец Л. М.

Обеспечение безопасности персональных данных в интернете: коммерческое использование персональных данных поставщиками цифрового контента

Проанализирован правовой аспект использования социальными онлайн платформами персональных данных пользователей. Проведено сравнительное исследование концепции персональных данных в национальном и зарубежном законодательстве. Рассмотрена концепция договора поставки цифрового контента, в соответствии с которой пользователь в обмен на цифровой контент передает он-лайн платформе свои персональные данные, которые могут быть использованы в маркетинговых и рекламных целях. Проанализированы положения об ответственности социальной онлайн платформы за сбор и передачу данных о пользователей другим лицам, в том числе для реализации политических, маркетинговых, социальных, экономических, технологических стратегий.

Ключевые слова: *персональные данные, интернет, монетизация, цифровой контент, безопасность.*

Stakhyra H., Savanets L.

Ensuring the security of personal data on the internet: the commercial use of personal data by digital content providers

The article analyzes the legal aspect of the use of personal data by users of social online platforms. A comparative study of the concept of personal data protection in national and foreign legislation.

Development of the Ukraine economy lead to creation new information society, digitization goods and services, rising level of person rights protection. With the framework of Association Agreement of the Ukraine and European Union it should harmonized legislation, and build wide common digital single market. Significant progress in the development of information technology, their widespread introduction, associated with the increase in volumes and areas of information use has led to the possibility of collecting, storing and processing information about the individual who is the subject of private law relations. In turn, due to the widespread use of automated systems and related technologies, information about any person may become one way or another open and lead to a violation of its lawful interests, material or non-pecuniary damage. But technology progress gives an opportunity to use personal data as a counter performance for getting goods and services in digital form. The emergence of such legal relations needs development and adoption some legislative regulation, which create maximum level of consumer rights protection.

The concept of a contract for the supply of digital content is considered, according to which the user in exchange for digital content transmits to the online platform their personal data that can be used for marketing and advertising purposes. The provisions on the responsibility of the social online platform for the collection and transmission of data about its users to other persons, including for the implementation of political, marketing, social, economic, technological strategies, are analyzed.

Keywords: *personal data, internet, monetization, digital content, security.*

Formulation of the problem. The rapid development of scientific and technological progress, which are characterized by the introduction into the daily lives of users of computer and information technology, has led to an increase in the volume and use of information, including the collection, processing and storage of personal data. Extensive use of automated information systems contributes to the emergence of an open bank of information about a person, the accumulation and use of which may lead to a violation of it legitimate interests, the occurrence of material or moral damage.

At the same time, technological advances have made it possible to use personal data as a new form of retribution in order to acquire goods and services in digital form. This necessitates the development of effective regulation of the use of personal data, including in contracts for the supply digital content.

Analysis of resent research and publications. In the article author is taking into account the works of Klein A., Pormeister K., Nowacka I. and others.

The purpose of the article is to determine the concept of a contract for the supply of digital content, according to which the user, in exchange for digital content, transfers his personal data to the online platform, which can be used for marketing and advertising purposes.

Presentation of the main research material. It should be emphasized that the problem of personal data trade, and therefore, the actual inclusion of personal data in the category of objects of civil rights is extremely relevant for Ukrainians. Them also face two significant problems: first, personal data, including information about age, gender, interests, pages visited and services used, telephone number and even bank account number, become the subject of civil law contracts and therefore have a certain material value - the monetary equivalent of personal data. Secondly, the legislative regulation of personal data circulation is actually detached from the real state of

affairs, thus users of Internet resources are deprived of legislative protection of the state due to the lack of legal regulation of this issue.

According to the Unified State Register of Court Decisions, over the past 5 years, Ukrainian courts have issued 5,965 decisions on the protection of personal data of persons on the Internet. Analyzing the number of cases considered, we can conclude that there has been a significant increase in violations of the use of personal data on the Global network. Thus, if in 2016 the number of cases considered by national courts concerning the leakage and use of personal data on the Internet was 378 cases, in 2020 the number of filed and considered cases increased to 1641 [1].

It is worth noting that in 2016, most citizens went to court to protect their violated rights on the Internet as part of a criminal case (bank theft, illegal online casinos, fraud), while now there is a significant increase in the number of civil cases on personal data protection, which were transferred to the service provider on the basis of a contract for the supply of digital content with social media platforms, such as Facebook, Instagram. That is why it is so important analyze the legal grounds and limits of the use of personal data of Ukrainian users of social networks on the example of social platforms as Facebook, and determine how to prevent the violation of the use of personal data, and bring offenders to justice.

Transfer of personal data to social platforms is a new type of repayment agreement.

The transfer of personal data, as a form of remuneration under a contract for the supply digital content is a relatively new solution in EU law.

Newest Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services contains an obligation for the recipient of digital content to pay a certain price in favor of the supplier, or provide it own personal data, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose [2]. It is worth noting that the wording of the obligation of the recipient of digital content in the form of payment of a certain price is not limited to the transfer of funds. We agree with A. Klein that repayment in contractual obligations is characterized by the exchange between the parties of objects that have a certain property value [3, p. 103]. The property value of the object is evidenced by the desire of the subjects of contractual relations to receive it for a fee, thus establishing the market value for a particular good or service [4, p. 290].

The introduction of the latest technologies in economic relations has contributed to the emergence of new technical ways of concluding contracts for the supply of digital content. Consumers can choose the means of such supply among its many subspecies. The most popular are: delivery of digital content "on demand", at the personal request of the user, download it by clicking a special button on the supplier's website, receiving digital content via streaming and webcast online, by connecting IP- addresses to the TV data channel, subscriptions to e-books, e-magazines and e-newspapers, download mobile applications, and make online purchases in these applications, use cloud technologies and much more. Equally diverse is the method of payment for the provision of digital data, which varies from the transfer of funds to the fulfillment of obligations in kind (in particular, receiving e-mail and viewing online advertising materials, selection of contextual advertising, passing a questionnaire to develop marketing supplier strategy, etc., the provision of personal data) [5, p.39].

It should be noted, that the supply of digital content is based on accession agreements, which are usually concluded online. K. Pormeister notes that the transfer, accumulation and use of personal data occurs through the conclusion of contracts for the supply of digital content through automated online systems. In these cases, the agreement of the parties on all the essential terms of a separate agreement does not occur, and the agreement is concluded on the basis of automated processing of information submitted by the parties [5, p. 17]. An example of such automatically concluded agreements can be services that provide digital content on the basis of user registration. The recipient of digital content fills in a special form on the supplier's website, which usually indicates personal data, including e-mail address, and the completion of registration and receipt of digital content is impossible without consent to the processing and use of personal data, agreement without the possibility of making any changes or reservations.

By concluding a contract for the supply of digital content online by registering on the platform, the user provides the provider with a list of their personal data, which is often subject to transfer to others. After all, the user has the right only to join the standard terms of the contract, which are often frankly unfair and violate the rights of users to personal data, without the possibility of negotiating the terms of the contract by the user.

It is worth paying attention to one of the most popular social networks today – Facebook. According to the communication agency Plusone, the total amount of Ukrainian Facebook users in 2020 is 14 million [6]. And

this social media collects personal data of each of them. Yes, Facebook software has the ability to collect, store and analyze user data, however, it has other ways to gather information about user behavior.

Among other means, accumulate information about the user's preferences Facebook uses tracking cookies. If a user is logged into Facebook and simultaneously browses other websites, Facebook can track the sites they are visiting. Tracking cookies are a specialized type of cookie that can be shared by more than one website or service. They are commonly used for legitimate marketing and advertising purposes, but because they contain a history of the user's actions on multiple sites, they may be exploited or misused to track the user's behavior [7]. Collecting information about user's behavior allow Facebook sell it and send users personalized contextual advertising. Thus, concluding a seemingly gratuitous contract for the supply of digital content, the user actually transfers his personal data, and the social network sells it to third persons for profit, which actually violates the legislation in the field of personal data protection.

In addition, this social platform forces users to agree with openly dangerous conditions – to allow use facial recognition. The technology of automatic identification of a user's personality by his image in a photograph has a wide commercial application. This technology is interesting because it can be carried out without contact with the object. The danger of using this technology is that anyone on the street, taking a photo of a person on your phone and uploading it to social networks can get information about it: age, gender, place of work, place of study and even phone number and home address (if the service uses geolocation).

Facebook uses software, which allow collect and analyze likes on particular post, then platform sell this information about persons preferences for in order to select effective advertising.

The above allows us to conclude, that the transfer of personal data on the basis of registration in the social network and further activities on the platform to the provider – it is a form of repayment in the contract for the supply of digital content, and personal data can be monetized.

The data that need legal protection.

It is necessary to to explore which data can be considered as «personal» in the understanding of the legislator and require exclusive legal protection against distribution and sale on the Internet.

According newest Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and their free circulation, and repealing Directive 95/46/EU personal data determines as 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 [8].

It is worth paying attention on provisions of Directive 2002/58/EU of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the field of electronic commerce of 12.07.2002 [9], according to which personal data also includes:

• confidential data that contains the content of messages sent during e-mail;

• data needed to establish and maintain a connection: information about traffic, providers, connection time and its total duration;

• information about the location of electronic devices from which users connected to the Internet at a specific time. This information also applies to tracking the whereabouts of a person through the technology of the Global Positioning System used by modern mobile devices.

Regarding the legislation of Ukraine in the field of provision, processing and protection of personal data, it should be noted that it is in its infancy. Consolidation of legislation provides significant value to this process. Thus, in accordance with the provisions of Art. 200 of the Civil Code of Ukraine, information is any information and / or data that can be stored on physical media or displayed in electronic form, and the procedure for using information and protecting the right to it is established by the Law of Ukraine «On Information» № 2657-XII. This legal act defines information about an individual (personal data) as information or a set of data about an individual who is identified or can be specifically identified. A similar definition is found in special legislation aimed at protecting personal data - The Law of Ukraine «On Personal Data Protection» № 2297-VI dated 01.06.2010.

It necessary to note, that national legislation does not establish a single list of personal data. In particular, the Law of Ukraine «On Information» to the list of personal data includes data on the nationality of the individual, education, marital status, religious beliefs, health status, as well as his address, date and place of birth. The Law of Ukraine «On Advocacy» dated 05.07.2012 № 5076-VI to the personal data of a person includes a list of issues with

which a person applies to a lawyer for advice, its content, a list of data obtained by a lawyer in the performance of his professional duties.

During the development of information systems and ambiguity in deciding supplies specific information in the list of personal data, national legislators should define a list of data that needs protection. In this context, it necessary to analyze the definition of personal data set out in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 [10]. The Convention defines personal data as any information relating to a specific person or a person that can be identified. This gives grounds to assume the thesis of the existence of a wide range of information that can be defined as personal data, other data about the person that allow it to be identified.

An analysis of national legislation suggests that there are no clear restrictions on the use of personal data of digital content users by its suppliers. At first glance, the need to obtain the consent of the personal data subject, which is a prerequisite for their use, should be a key factor in formulating the right of a person to decide on the collection, accumulation, processing, storage and dissemination of personal data, including for profit.

However, in the legislation of Ukraine, consent to the processing and use of personal data in the digital sphere is defined as marking the granting of permission to process personal data during registration in the information and telecommunications system of the e-commerce entity [10].We believe that this approach to the protection of personal data from their further use by the supplier for advertising and marketing purposes is ineffective, because in order to obtain a certain digital content, the marking is necessary.

Litigation is related to the sale of personal data.

The lack of a provision in national law on the ability of personal data to be circulated and have a certain property value, as well as protection against the collection, processing and transfer of personal data by social platforms, has led to widespread violations of social media users rights and high-profile lawsuits.

Loud publicity about the sale of personal data by the platform Facebook received the case Smith v. Facebook. The plaintiffs appealed to the court to bring the platform to justice for the collection and processing of their medical data. Users alleged that the company tracked their visits to healthcare websites, in violation of the websites' explicit privacy policies. Court decided that Facebook was not bound by the promises made not to disclose users' data to Facebook because Facebook has a provision, buried deep in its own policy, that allows Facebook to secretly collect such data [11].

Another loud case connecting with Facebook selling personals data called Cambridge Analytica scandal. Cambridge Analytica had purchased Facebook data on tens of millions of Americans without their knowledge for the aim to predict how they will vote on the next American president election. This company create profiles of that people, analyzed their likes, the visited pages, commentaries. In addition, the company selected relevant content for users to persuade them to vote for Donald Trump. Facebook was hit with a $5 billion fine from the Federal Trade Commission as part of a settlement over claims the company mishandled user data [12].

So, if only the rules, which was made by the platform allow it to collect and sell data about a person – it is strongly violation of the user's privacy, and such provision should be prohibited by state law.

Liability for the transfer of personal data.

It should be noted that today it does not exist a single unified legal act that determines which data cannot be collected and used by social platforms, and what liability is provided for the use of such data.

Ukrainian legislation in the field of personal data protection should develop in the light of the decisions taken by the International Organization for Economic Cooperation and Development on the basic principles of protection of privacy and individual freedoms and General Data Protection Regulation of EU. The state should take into account the purpose of personal data processing, the composition of personal data, ensuring a balance between the level of threat and access to personal data, ensuring the protection of personal data from illegal processing and illegal access to them.

It should be emphasized, that personal data as a legal institution in need of protection appeared in Ukrainian legislation in 2011, with the entry into force the Law of Ukraine "On protection of personal data".

In the same year, the State Service of Ukraine for Personal Data Protection appears, and entities that use personal data are obliged to register their databases in the service. The technical support of the service did not withstand the mass registration of databases – and therefore, in fact, such databases, despite the obligations of the law, were not registered. And since January 2014, all the powers of the service have been transferred to the Department for Personal Data Protection of the Secretariat of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine.

It should be noted that this body is designed to protect personal data of citizens, including from illegal collection and sale by social platforms on the Internet, and to bring offenders to civil, administrative, criminal liability.

According to the Resolution of the Supreme Court of Ukraine of 27.09.2017 in the case № 6-1435tss17 in disputes concerning compensation for non-pecuniary damage, in particular in cases of disclosure of personal data and interference with privacy, there is a presumption of non-pecuniary damage by the defendant and the defendant's obligation to refute presumption [14].

In turn, in accordance with Art. 188-39 of the Code of Ukraine on Administrative Offenses provides for administrative liability in the form of various fines ranging from UAH 1,700. up to UAH 17,000.

In accordance with the provisions of the provisions of Art. 255 of the Code of Ukraine on Administrative Offenses the Ombudsman has the right to draw up reports on administrative offenses, after which the materials of the administrative case are transferred to the court.

The most resonance case was Resolution of the Lychakiv district court of Lviv from 02.19.2018 in case № 463/255/18, in accordance to which the military commissar of the Lviv regional military enlistment office was bringing to administrative responsibility and imposing a fine of UAH 5,100 for posting on the official website of the military enlistment office lists of citizens who are subject to conscription and did not appear at the military commissariat [15].

Moreover, the Criminal Code of Ukraine provides liability for the fact of illegal collection, storage, use, destruction, dissemination of confidential information about a person or illegal change of such information, except as provided by other articles of Criminal Code a fine of five hundred to one thousand non-taxable minimum incomes or correctional labor for up to two years, or arrest for up to six months, or restriction of liberty for up to three years.

Instead, if the offense concerns non-compliance with the procedure for personal data protection established by the legislation on personal data protection, which led to illegal access to them or violation of the rights of the personal data subject, administrative liability in accordance with the provisions of the Code of Administrative Offenses.

Conclusions. In conclusion, it is worth noting that in fact personal data become a new object of civil rights, and it can be an object of contracts and have a property value. At the same time, the variety of data that can be interpreted as personal is constantly expanding. Today, in accordance with international regulations and court decisions, personal data determines not only the name of a person, his identification number, but also data that helps to identify him on the Internet – the location of a mobile device, IP-adress, browsing websites, likes, etc.

Large amount of Ukrainian social network users actually gives their data to the platform operator every day. Its protection as well as bringing the operator to justice, and preventing the inclusion of provisions that allow collecting and selling personal data of social network users to third parties in the standard terms of the platform operator are possible only if such provisions are enshrined in law.

Thus, the domestic legislator has a task to amend the Civil Code of Ukraine, expanding the list of objects of civil rights, the Law of Ukraine on Personal Data Protection - expanding the concept of personal data subject to protection, as well as provide administrative and criminal liability for illegal collection, sale and use of personal data by social platforms.

References

1. *Unified State Register of Court Decisions.* Retrieved from https://reyestr.court.gov.ua [in English].
2. *Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770 [in English].
3. Klein, A. (2005). *Elementy zobowiązaniowego stosunku prawnego.* Wrocław : Wydawnictwo Uniwersytetu Wrocławskiego [in Polish].
4. Nowacka, I. (2017). *Umowa o dostarczeniu tresci cyfrowych.* Kraków. [in Polish].
5. Pormeister, K. (2017). Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of '23andMe'. *Journal of European Consumer and Market Law, 1* [in English].
6. *Facebook and Instagram in Ukraine.* Retrieved from https://plusone.com.ua/research/Facebook%20та%20Instagram%20в%20Україні%20(січень%202020)_UA.pdf [in Ukrainian].
7. *Tracking cookies.* Retrieved from https://www.f-secure.com/sw-desc/tracking_cookie.shtml [in English].

8. *Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and their free circulation.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [in English].
9. *Directive 2002/58/EU of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the field of electronic commerce of 12.07.2002.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 [in English].
10. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.* Retrieved from https://zakon.rada.gov.ua/laws/show/994_326 [in Ukrainian].
11. *Winston Smith V. Facebook, INC., No. 17-16206 (9th Cir. 2018).* Retrieved from https://law.justia.com/cases/federal/appellate-courts/ca9/17-16206/17-16206-2018-12-06.html [in English].
12. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.* Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [in English].
13. Obukhovska, T.I. *State mechanisms for providing personal data protection in Ukraine.* Retrieved from http://academy.gov.ua/pages/dop/138/files/842f46c2-f889-4639-8f34-605930281696.pdf [in English].
14. *Resolution of the Supreme Court of Ukraine of 27.09.2017 in the case № 6-1435tss17.* Retrieved from https://oda.court.gov.ua/sud1590/pravovipoziciivsu/6-1435cs17 [in Ukrainian].
15. *Resolution of the Lychakiv district court of Lviv from 02/19/2018 in case №463/255/18.* Retrieved from https://verdictum.ligazakon.net/document/72335799 [in Ukrainian].

Стаття надійшла до редакції 16.09.2021.