ISSN 2078-4503. Вісник Львівського університету. Серія юридична. 2025. Випуск 81. С. 204–214
Visnyk of the Lviv University. Series Law. 2025. Issue 81. P. 204–214

342.9:340.5:341.1

LEGAL NATURE OF SOCIAL NETWORKING SERVICES AS DATA CONTROLLERS UNDER THE LEGISLATION OF THE EU AND UKRAINE

Rostyslav Prystai

Ivan Franko National University of Lviv,
I, Universytetska Str., Lviv, Ukraine, 79000
e-mail: rostyslav.prystai@lnu.edu.ua
ORCID ID: 0000-0002-8980-1650

The lack of effectiveness of the existing mechanism and practice of personal data protection of social services users in Ukraine necessitates the study of the possibility of applying the legal standards of the European Union in order to increase the level of protection of the rights of data subjects in the digital environment, in particular, in the field of electronic communications. Implementation, development of high-quality sectoral legislation or creation of effective national recommendations is possible only if there is a consistent and objective study of the specifics of the activities of the services provided by public electronic communications services, including online social networking services.

The article examines the peculiarities of the legal status of social networking services as data controllers under the laws of the European Union and Ukraine. The author examines the peculiarities of social networks as web services which form digital profiles of users, collect and process significant amounts of personal information, including biometric data, which may pose risks to the privacy and security of users. The author analyzes the concept of "Data controller" in accordance with Regulation (EU) 2016/679 (the "GDPR"), taking into account the practice of interpreting this term in the relevant recommendations of the European Data Protection Board. The author reveals the peculiarities of the legal status of social networks as sole or joint controllers, and identifies the main legal grounds for data processing, in particular, consent, legitimate interest and performance of a contract. The article also examines the peculiarities of the territorial application of the GDPR to users located outside the EU, in particular in Ukraine.

Keywords: social networks, personal data, data controllers, data processing, territorial scope.

DOI: http://dx.doi.org/10.30970/vla.2024.81.204

Introduction. The processing of personal data by social networking services has its own specific features, which consist in the formation of user profiles and the accumulation of a significant amount of information about individual users, the creation of conditions for relatively easy collection of data on communications between social network users and their interactions with the platforms, the use of new technologies, the processing of sensitive data for security purposes, and other peculiarities. Such processing takes place within the activities of web services based on the principles of Web 2.0. Participants of social networks create publicly accessible or semi-public profiles within a limited system, which represent their digital identities. These services enable users to create, publish, and distribute various types of content, including text, images, and videos, allowing other users to interact with that content [1]. The mentioned factors are associated with potential risks to the rights and freedoms of individuals, which may arise as a result of inadequate information security, improper or unlawful processing of personal data, as well as non-compliance with personal data protection legislation by social networking services.

Problem statement. The statistics on the use of social networks in the territory of the EU and Ukraine are approximately the same. In Ukraine, however, messengers such as WhatsApp, Telegram, and Viber are more widespread. Users in both regions share similar preferences for applications that allow the sharing of video and audio content – such as Instagram, TikTok, and YouTube – as well as professional social networks (LinkedIn) and discussion or debate forums (Facebook, Reddit) [2], [3]. These services are used in both the private sphere (communication, advertising, commerce) and the public sphere, as social networks constitute a common form of mass media.

Along with the widespread use of social networks, there is also a significant number of violations of users' rights and freedoms related to the processing of their data by these services [4]. Such violations include non-compliance with the principles of privacy by default and by design, unlawful international data transfers, failure to ensure adequate technical safeguards for personal data protection, unlawful disclosure of personal data to state authorities, and breaches of the principles of data minimization and transparency, among others. In practice, users of social networks in Ukraine are unable to adequately protect their rights related to the processing of their information by these services. These platforms are registered and actively operate in the territories of the United States, the European Union, South America, and China. However, with regard to Ukrainian users, the data controllers are predominantly legal entities established within the EU. The factors that hinder such protection include the lack of effective practice by national supervisory and judicial authorities, as well as the absence of effective recommendations or alternative mechanisms that could help protect users' rights without the need to initiate formal administrative or judicial proceedings.

Therefore, it is appropriate to examine the legal status of social networking services as data controllers, as essential for ensuring the rights and freedoms of data subjects in the digital environment and to formulate relevant proposals aimed at their protection.

Analysis of recent research and publications. The role of social networks as personal data controllers is examined, in particular, by R. Wong ("Social networking: a conceptual analysis of the data controller") as well as by Lichelle Wolmarans and Alex Voorhoeve ("What makes the processing of data by social networking services permissible?").

Purpose of the article. The purpose of this article is to disclose the legal nature of social networking services as data controllers in accordance with the legislation of the European Union and Ukraine, as well as to identify effective mechanisms for ensuring the rights of data subjects within these legal relationships.

The object of the research is the web-services that provide communication and information exchange on the Internet.

The subject matter of the research is the legal nature of web-services providing communication and information exchange on the Internet as data controllers in accordance with the legislation of the European Union and Ukraine.

The concept and features of social networking services. In both scientific and legal doctrine, there is no single universally accepted definition of the term "social networks." This lack of definition is due to the complex and multifaceted nature of the phenomenon, which manifests itself in various forms depending on the context in which it is applied. Social networks may be interpreted as social structures formed by individuals or institutions; as digital platforms designed to establish and maintain social connections; as specific online services that provide relevant communication functionalities; or as a set of digital identities of registered users who interact with one another. The meaning of the term "social networks" is therefore contextual and depends on the purposes for which it is used in a particular field.

N. Ellison and D. Boyd, in their work "Social Network Sites: Definition, History, and Scholarship", define social networks as online services that allow users to: 1) create a public or semi-public profile within a platform; 2) establish a list of contacts with whom they share social connections; and 3) view their own network of connections as well as those of other users. At the same time, the types and names of connections may vary depending on the platform.

In turn, K. Musiał and P. Kazienko, in their article "Social Networks on the Internet", draw attention to the features that distinguish online social networks from traditional, offline structures based on interpersonal interaction in the real environment. These include significant physical distances between participants; the often loose correspondence between a user's online identity and their real-life social persona; multimodal communication that enables simultaneous interaction with multiple individuals through various channels, including both online and offline formats (such as VoIP[1] and text messaging); the ease of pausing or terminating communication; and the accessibility of collecting and analyzing data on user activity [5]. However, the reliability of such data often raises concerns, as users frequently conceal or distort personal information due to privacy-related apprehensions.

From a technical perspective, K. Musiał and P. Kazienko consider social networks as a multi-system structure encompassing a set of virtual Internet identifiers associated with a single physical social entity. In this context, a social network appears as a collection of digital representations of registered users, interconnected based on data regarding shared activities, communications, or established direct connections within Internet-based systems. Accordingly, the following may be regarded as characteristics of social networks as communication service providers:

– Are web-based services.

– Enable individuals to create a public or semi-public profile within a restricted system.

– Compile a list of other users with whom they share connections.

– Allow users to view and navigate the list of their own connections as well as the connections established by other users within the system.

– Provide the ability to create, publish, and distribute various types of content, including text, images, and videos, thereby allowing other users to interact with such content.

Not all of the characteristics listed above are determinative for identifying an online social network. While such networks operate as web-based services, not every network provides the ability to compile lists of other users or to view their profiles. Social networks generally, though not necessarily, have the status of a legal entity (for example, a corporation or a limited liability company), which enables them to conduct commercial activities, enter into contracts, and operate as platforms for offering various services – such as content sharing, communication, or advertising. In this context, users can act both as creators and consumers of content and services. At the same time, organizational or legal form is not a mandatory condition for classifying a service as a social network. In our view, the key features are the presence of a web interface, the ability to establish interpersonal connections, and the formation of stable patterns or structures of such interactions. In the absence of these characteristics, the service is more accurately described as a communication tool rather than a social network as a distinct phenomenon.

[1] Voice over Internet Protocol (VoIP) is a technology that enables voice calls to be made using a broadband Internet connection instead of a conventional (or analog) telephone line. Some VoIP services may allow calls only between users of the same service, while others provide the capability to call anyone who has a telephone number – including local, long-distance, mobile, and international numbers.

Online social networks, understood as web-based services that allow for the creation of social connections and stable interactions, include, for example, Facebook, Instagram, Twitter, LinkedIn, TikTok, YouTube, Snapchat, Reddit, and Pinterest. By contrast, platforms such as Wikipedia, Skype, iCloud, and other online media are not considered social networks.

The concept of a data controller. With the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data [6], and later Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data [7], the concept of a data controller was introduced. This refers to a participant in legal relations concerning the processing of personal data who, alone or jointly with others, determines the purposes and means of processing personal data. Under the aforementioned Regulation, as well as other specific legislative acts adopted within the EU framework (for example, Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector), the data controller is assigned specific duties and responsibilities to ensure an appropriate level of personal data protection. This includes the implementation of technical and organizational measures in the context of data processing [8], as well as other obligations. Some of these provisions, albeit somewhat modified, have been incorporated into the national legislation of Ukraine, specifically in the Law "On Personal Data Protection" of 2010 [9], adopted to implement Directive 95/46/EC.

An important role in determining the criteria under which a person qualifies as a data controller is played by the Guidelines 07/2020 on the concepts of controller and processor under the GDPR (hereinafter – the Guidelines) [10]. Considering the absence of analogous recommendations or criteria for defining the role of a controller in Ukrainian legislation, Guidelines 07/2020 may be applied by analogy, as their content and scope reflect the same concept contained in Directive 95/46/EC as of 2010.

The Guidelines identify five key elements that a data controller must meet and emphasize that the concept of "controller" is both functional and autonomous. The functional approach means that the legal status of a subject as a "controller" should, in principle, be determined by its actual activities in a given situation, rather than by a formal designation of the subject as a "controller" (for example, in the context of a user). The autonomy of the concept entails that the notion of a controller should be interpreted primarily in accordance with EU data protection law. The concept of a controller should not be limited by other, sometimes conflicting or overlapping, concepts in other areas of law, such as a creator or rights-holder in intellectual property law or in competition law.

Overall, the term "controller" should be interpreted broadly, giving priority to the most effective and comprehensive protection of data subjects to ensure the full application of data protection legislation, avoid legal gaps, and prevent potential circumvention of rules, while at the same time not diminishing the role of other participants (e.g., processors).

Social Networking services as data controllers in the EU and Ukraine. Within the territory of the European Union, Meta platforms lead in popularity, reflecting global trends. The most popular social network in Europe is Facebook, with over 454 million users in the region, followed by Instagram with approximately 303 million users. Networks such as TikTok, Reddit, and Snapchat are gaining traction; however, their growth rates have been slower than in previous years (2020–2023). Instagram remains the second most popular platform in Europe and is projected to reach 325.9 million users by 2028. In Ukraine, the number of social network users is expected to steadily increase between 2024 and 2029 by a total of 4.6 million users (+14.74%). After nine consecutive years of growth, the social

network user base is projected to reach 35.78 million, reaching a new peak in 2029. It should be noted that the number of social network users has consistently grown in recent years. The figures regarding social network users were obtained from survey data that were processed to estimate missing demographic indicators. The data presented are excerpts from the "Key Market Indicators" (KMI) provided by Statista [11], [12].

These social network services process users' personal data for various purposes and on different legal bases in accordance with the provisions of Article 6 of the General Data Protection Regulation (GDPR). This includes information provided for the purposes of service provision, marketing, legal compliance, security, statistical analysis, and others. Pursuant to Article 5(2) GDPR, data controllers must adhere to the accountability principle, which means that the controller is responsible for compliance with the principles set out in Article 5(1) GDPR and must be able to demonstrate such compliance. Observance of this principle is particularly important in the context of the activities of controllers, notably social network services, since the processing of users' data in this environment and at such a large scale creates risks to their rights and freedoms. In 2024, 36% of surveyed Internet users worldwide reported exercising their right to submit Data subject access requests (DSARs), compared to 24% in 2022. Additionally, individuals aged 25 to 34 took the most measures to protect their privacy.

The legal nature of these services is that, under both territorial and material criteria, they qualify as data controllers with respect to users in both the EU and Ukraine. Let us examine the specific features of their legal nature in greater detail.

The five functional elements that define the content of data controller concept include: a) the existence of a natural or legal person, a public authority, an institution, or another body b) that determines, c) alone or jointly with others, d) the purposes and e) means of f) personal data processing.

Social network services mostly operate in the form of limited liability companies (LLCs) or corporations (Inc.). This includes companies such as Meta (Corp.), Telegram (LLC), and Reddit (B.V. – the Dutch equivalent of an LLC). Both LLCs and corporations provide protection to their participants in the form of limited liability. However, in the case of corporations, there is a slightly higher risk that a court may hold participants personally liable for business debts. This typically occurs when owners commingle personal and business finances, fail to adhere to proper corporate formalities, or engage in fraudulent activities. Under the EU data protection legislation (Regulation 2016/679), the legal form of these entities is irrelevant for determining their role as data controllers, since both types fall within the category of legal persons.

The second key element of the data controller concept concerns the controller's influence over data processing through the exercise of decision-making authority. A controller is considered a subject that determines certain fundamental aspects of personal data processing. Such controller status may be explicitly established by law or inferred from an analysis of the actual circumstances of a specific situation. For example, according to Meta's Privacy Policy [13], it is explicitly stated that when using Meta products, the company determines the conditions and utilizes personal data for personalized user interaction, analytics, user communications, and conducting research. As a general rule, a functional, factual criterion is applied to determine the controller in a given situation, regardless of what the company's policy declares. However, in this case, the company itself declares that it makes decisions regarding the purposes of processing as well as the methods of such processing. This can additionally be verified through an external audit initiated by the company, a public organization, an analysis of the application's operation, or at the initiative of a national supervisory authority. Here, the key element in defining a

controller pertains to the object of the controller's influence, namely the "purposes and means" of personal data processing. This is an essential part of the controller concept: it defines what a subject must determine to be considered a controller – specifically, the intended outcome that guides or directs planned actions and how that outcome is achieved or a particular purpose of the processing is realized.

Social networking services as joint data controllers. It should be noted that an organization can be considered a controller even if it does not make all decisions regarding the purposes and means of processing. This means that several different organizations may act as controllers for the same processing, and each is subject to the applicable provisions of data protection law.

This applies, for example, when a company uploads its client lists (e.g., email addresses) to Meta in order to create a "custom audience" for advertising purposes. In such cases, Meta Platforms Ireland Limited and the other company are considered joint controllers under Article 26 of the General Data Protection Regulation in the context of joint processing as defined by the terms applicable to the relevant products.

The scope of joint processing may include the collection of personal data as defined by the terms of the applicable products and its transfer to Meta Ireland. However, any further processing of data by Meta Ireland does not constitute part of the joint processing. In any case, the purposes and means determined by the controller must relate to the processing of personal data.

Pursuant to Article 4(2) GDPR, the processing of personal data is defined as "any operation or set of operations performed on personal data or on sets of personal data". Accordingly, the concept of a controller can be associated with either a single processing operation or a set of operationi. In practice, this means that the control exercised by a subject may extend to the entire processing within a given process, but it may also be limited to a specific stage. In the activities of social networks such as Facebook, Instagram, or TikTok, the controller concept can apply to either the full scope of data processing or to particular stages. For example, when a company runs targeted advertising via Facebook Ads, it jointly determines the purposes and means of processing together with Meta, making both parties joint controllers. At the same time, Meta itself may act as the sole controller with respect to processing user behavior data in the news feed for content personalization. Similarly, in TikTok, an advertiser who uploads its own client lists to create Custom Audiences assumes partial controller functions only for a specific stage of processing.

Thus, the role of a controller may encompass the entire chain of personal data processing or be limited to a particular operation, depending on the degree of influence over the purposes and means of processing.

Legal bases and scope of personal data processing by social networking services. Among the six lawful bases for processing personal data, within five of the most popular social network services (Facebook, Reddit [14], TikTok [15], Discord [16], YouTube (Google) [17]), the most prevalent are legitimate interests of the companies, processing necessary for the performance of a contract, and user consent. Legitimate interest as a legal basis is actively used for collecting information to personalize and improve products, protect the security of users and services, conduct research, and implement innovations (Meta). One common form of data processing is the display of advertisements, which, according to the privacy policies of Facebook and Reddit, is also carried out on the basis of legitimate interest. Consent, as a legal basis for processing, is characteristic of activities such as sending push notifications to a user's mobile device, use of the service by underage users, and conducting surveys. Processing based on contractual necessity is performed for the handling of audio and images provided by users, responding to user inquiries and complaints, communication

with users, verification of proper service functioning (e.g., bug fixes), and other related activities. It should be noted that the legal nature of the contract between the user and the service is that it constitutes an adhesion contract in the form of a public offer, concluded by implied actions, namely by accessing the platform (e.g., Facebook) or using another product where the service acts as the provider and the user as the consumer of digital services. The contract may be paid or free of charge and has a hybrid nature, combining elements of a contract for information services and a license agreement (on the terms of a non-exclusive license for content provided by the user). As Meta notes, when a user shares, publishes, or uploads content that is subject to intellectual property rights, the user grants the company a non-exclusive, royalty-free, worldwide license, with the right to sublicense, to host, use, distribute, modify, reproduce, copy, publicly perform or display, and translate the content – which may include personal data.

Furthermore, the processing of personal data of social network users does not occur under a separate "data processing agreement," as is sometimes mistakenly assumed, but rather within the framework of the main contract for the provision of digital services (since the processing of personal data is not an independent subject of obligation in the controller–data subject relationship). This contract, concluded in the form of a public offer through implied actions, provides for the use of personal data as a necessary element for the functionality of the service. The legal basis for such processing is either the necessity of contract performance (e.g., to provide access to an account or to process requests), consent (particularly in cases that involve elevated risks to the rights and freedoms of the data subject, such as personalized advertising or the use of trackers), or legitimate interest (notably for security, analytics, and service improvement).

At the same time, the term "data processing agreement" is correctly applied to relationships between, a controller and a processor, where another entity is engaged to process data on behalf of the service in accordance with Article 28 of Regulation 2016/679.

Relations between social networking services as data controllers and data subjects outside the EU. Issues that may potentially arise for data subjects regarding the exercise of their rights when using social networks outside the jurisdiction of EU Member States include, in particular, the applicability of Regulation 2016/679 to such users (for example, when the service collects behavioral data or uses targeting); determining who qualifies as the controller in the relevant relationship – whether it is the European entity or the company's U.S. affiliate (e.g., Meta Ireland or Meta Platforms Inc.) – and whether this distinction has practical significance. Another relevant issue concerns the advisability of establishing and registering representative offices of the respective companies that process data locally in countries that are service-users.

The territorial scope of Regulation 2016/679 automatically extends to the activities of social networking services if one of the following two criteria is met: the presence of the controller's establishment within the European Union, or the targeting of activities to the EU market, including the offering of goods or services, or the monitoring of individuals' behavior within the EU. However, pursuant to Article 3 of the Regulation, the Regulation applies to all processing only if there is real and effective activity carried out through stable organizational structures, regardless of their legal form (branch, subsidiary, representative office, etc.). In the absence of such an establishment, if goods or services are merely offered or behavior is monitored within the EU, the Regulation applies only to data subjects within the EU.

Accordingly, for data subjects in Ukraine, the Regulation will be applicable if a social network (or other online service) conducts actual commercial activities in the EU through a stable establishment (e.g., a branch or subsidiary) and such activity involves the processing of personal data. In this scenario, all processing, regardless of the geographic

location of the data subjects (including those in Ukraine), falls within the scope of the GDPR (Article 3(1)).

However, for example, Meta's Terms of Service regarding users in Ukraine provide for a contract with Meta Platforms, Inc. – quote: "*These Products are provided to you by Meta Platforms, Inc. Accordingly, these Terms constitute an agreement between you and Meta Platforms, Inc. If you do not agree to these Terms, do not access Facebook or use other products and services covered by these Terms*". In this case, the data controller is Meta Platforms, Inc. (California) for users located outside the European Economic Area (EEA). Conversely, the data controller is Meta Platforms Ireland Limited (Ireland) for users within the EEA. This means that the GDPR does not fully apply to the respective processing (only to users within the EEA), and users from Ukraine cannot exercise their rights under the Regulation (such as data subject requests under the GDPR or complaints to the Irish Data Protection Commission) alongside their national legislation (only under the California Consumer Protection Act of 2018 (CCPA)). Meta determines the location of a user using several technical methods, including IP address, account settings, SIM card, mobile network, interface language, and GPS data if the user has provided the relevant consent. The IP address is the primary geolocation tool, as it allows an approximate determination of the connection country.

Meta Platforms Inc. may fall within the scope of the GDPR under Article 3 (2) (b) – monitoring the behavior of individuals located in the EU. Regardless of where the agreement was concluded, if Meta Inc. monitors the behavior of a user situated in the EU (for example, via cookies, tracking, profiling, or targeted advertising), the GDPR applies. If no such monitoring occurs, Article 3 (2) (b) is not applicable. If the individual is located in Ukraine, the GDPR formally does not apply – in this case, Meta Inc.'s internal policies (such as the CCPA) and local legislation (e.g., Ukraine's Law on Personal Data Protection) govern the processing.

To summarize, if a user from Ukraine is physically located in the EU and enters into an agreement with Meta Inc. (USA), the GDPR may apply, since under Article 3 (2) (b), the behavior of a person located in the EU is being monitored.

If the user is located in Ukraine and uses the services of Meta Inc. (USA), the GDPR does not apply, as neither the processing nor the monitoring is related to the territory of the EU. If the user is located in the EU and enters into an agreement with Meta Ireland, the GDPR applies pursuant to Article 3(1), as the processing is carried out within the activities of an establishment located in the EU. Even if the user is located in Ukraine, processing by Meta Ireland is also subject to the GDPR under the Article 3 (1), since the mere fact that the individual is outside the EU does not exclude the application of the GDPR if the processing is carried out by a European company.

It is important to note that, in practice, in the absence of cooperation between supervisory authorities of EU Member States and third (non-EEA) countries, process duplication is possible. The GDPR does not prohibit the simultaneous filing of complaints with supervisory authorities in different jurisdictions, as each authority will consider the matter within the scope of its own jurisdictional powers.

Thus, the application of the Regulation's provisions allows the protection of data subjects' rights in cases of gaps in national legislation. However, there is a theoretical possibility that a single violation could result in two separate sanctions: one under local law and another under the GDPR, which is a negative consequence of the lack of cooperation mechanisms.

Conclusions. 1. The concept of "social networks" is dynamic, and its definition varies depending on the context of application. In both scientific and legal doctrine, there is no

unified approach to its interpretation, which is due to the diversity of social network functions as well as differences between online and offline forms of social interaction. The main characteristics of online social networks include the presence of a web interface, the ability to create a digital identity, the establishment of social connections, and the maintenance of stable communication patterns. Despite technical and organizational heterogeneity, these features allow social networks to be distinguished from other internet services and classified as a separate socio-technological phenomenon. Ukrainian legislation does not provide such a definition, which prevents a full delineation of the sphere where risks to users' rights and freedoms – particularly privacy – may arise.

2. Defining the role of the data controller is fundamental for the effective legal regulation of personal data protection. The approach applied in Regulation 2016/679 and detailed in Guidelines 07/2020 is based on the functional and autonomous nature of this concept, which allows for an accurate reflection of a subject's actual influence on data processing regardless of its formal status. Despite the absence of a similar doctrinal approach in Ukrainian legislation, the provisions of these Guidelines can be applied by analogy, given the harmonization-based origin of the national Law on Personal Data Protection.

3. Social networks that dominate the European and Ukrainian markets act as data controllers under the EU and U.S. law, particularly Regulation 2016/679 and CCPA. In the context of data processing, their legal nature is determined less by organizational or legal form and more by their actual influence over the purposes and means of data processing, which aligns with the functional approach to defining a controller. A controller may, in particular, be a subject that determines only part of the purposes or means of processing, which allows for the possibility of joint control under Article 26 of the Regulation. In such cases, each party bears separate responsibility for compliance with data protection law within its sphere of influence.

4. The legal bases for processing personal data within the activities of social network services are primarily founded on legitimate interest, the necessity of contract performance, and user consent. The digital services agreement, concluded in the form of a public offer through implied actions, serves as the key mechanism under which user data is processed (*legal basis – necessity for performance of a contract, not consent; if data is not needed for contract performance and separate data processing consent is not provided – there is no 'agreement to data processing' and processing has no legal basis (is illegal)*), in particular to ensure the functionality of the service, provide access to content, or handle requests.

5. Regulation 2016/679 (GDPR) may have extraterritorial effect and apply to the processing of personal data of subjects located outside the EU if the relevant service has a stable establishment in the EU. If controller is located outside the EU (regardless offering services to the EU data subjects or monitoring user behavior within the EU), the Regulation applies only to data subjects within the EU. Accordingly, users in Ukraine, depending on the Terms of Service or user consent, may in certain cases exercise their rights as data subjects in accordance with, and following the procedures set forth by, the GDPR.

Список використаних джерел

1. Boyd, Danah & Ellison, Nicole. (2007). Social Network Sites: Definition, History, and ScholarshiP. J. Computer-Mediated Communication. No.13. P. 210–230. 10.1111/j.1083-6101.2007.00393.x.
2. StatCounter. Social Media Stats in Ukraine. URL: https://gs.statcounter.com/social-media-stats/all/ukraine (date of access: 21.05.2025).
3. Statista. Social network visit in Ukraine by platform. URL: https://www.statista.com/statistics/-1473398/social-network-visit-ukraine-by-platform/ (date of access: 21.05.2025).

4. Statista. Social media regulations in Europe. (2024, September 26). URL: https://www.statista.-com/topics/12810/social-media-regulations-in-europe/#topFacts (date of access: 21.05.2025).
5. Musial, Katarzyna & Kazienko, Przemysław. (2012). *Social networks on the Internet. World Wide Web.* 16. 10.1007/s11280-011-0155-z.
6. Directive – 95/46 – EN – Data Protection Directive – EUR-Lex. (n.d.). URL: https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng.
7. Regulation – 2016/679 – EN – gdpr – EUR-Lex. URL: (n.d.). https://eur-lex.europa.eu/eli/reg/-2016/679/oj/eng.
8. Directive – 2002/58 – EN – eprivacy directive – EUR-Lex. (n.d.). URL: https://eur-lex.europa.-eu/legal-content/EN/ALL/?uri=celex:32002L0058.
9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17ж.
10. Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board. (n.d.).
11. Social media usage in Western Europe. (2024, November 4). Statista. URL: https://www.-statista.com/topics/4106/social-media-usage-in-europe/#topicOverview.
12. Statista. (2025, March 3). *Social media users in Ukraine 2020–2029.* URL: https://www.-statista.com/forecasts/1145635/social-media-users-in-ukraine.
13. Meta Privacy Policy – How Meta collects and uses user data. URL: https://www.facebook.-com/privacy/policy, accessed: May 21, 2025.
14. Reddit – The heart of the internet. (n.d.). URL: https://www.reddit.com/policies/privacy-policy.
15. Privacy Policy | TikTok. (n.d.). URL: https://www.tiktok.com/legal/page/us/privacy-policy/en.
16. Privacy Policy | Discord. (n.d.). URL: https://discord.com/privacy.
17. Privacy Policy – Privacy & Terms – Google. (n.d.). Privacy & Terms – Google. URL: https://-policies.google.com/privacy.

References

1. Boyd, Danah & Ellison, Nicole. (2007). Social Network Sites: Definition, History, and ScholarshiP. J. Computer-Mediated Communication, *13*, 210–230. 10.1111/j.1083-6101.2007.00393.x.
2. StatCounter. Social Media Stats in Ukraine. Retrieved from https://gs.statcounter.com/social-media-stats/all/ukraine (date of access: 21.05.2025).
3. Statista. Social network visit in Ukraine by platform. Retrieved from https://www.statista.-com/statistics/1473398/social-network-visit-ukraine-by-platform/ (date of access: 21.05.2025).
4. Statista. Social media regulations in Europe. (2024, September 26). Retrieved from https://-www.statista.com/topics/12810/social-media-regulations-in-europe/#topFacts (date of access: 21.05.2025).
5. Musial, Katarzyna & Kazienko, Przemysław. (2012). *Social networks on the Internet. World Wide Web.* 16. 10.1007/s11280-011-0155-z.
6. Directive – 95/46 – EN – Data Protection Directive – EUR-Lex. (n.d.). Retrieved from https://-eur-lex.europa.eu/eli/dir/1995/46/oj/eng.
7. Regulation – 2016/679 – EN – gdpr – EUR-Lex. Retrieved from (n.d.). https://eur-lex.europa.-eu/eli/reg/2016/679/oj/eng.
8. Directive – 2002/58 – EN – eprivacy directive – EUR-Lex. (n.d.). URL: https://eur-lex.-europa.eu/legal-content/EN/ALL/?uri=celex:32002L0058.
9. On personal data protection : The Law of Ukraine No. 2297-VI (01.06.2010). Retrieved from https://zakon.rada.gov.ua/laws The heart of the internet. (n.d.). URL: https://show/2297-17ж.
10. Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board. (n.d.).
11. Social media usage in Western Europe. (2024, November 4). Statista. Retrieved from https://-www.statista.com/topics/4106/social-media-usage-in-europe/#topicOverview.

12. Statista. (2025, March 3). Social media users in Ukraine 2020–2029. Retrieved from https://-www.statista.com/forecasts/1145635/social-media-users-in-ukraine.
13. Meta Privacy Policy – How Meta collects and uses user data. Retrieved from https://-www.facebook.com/privacy/policy (accessed: May 21, 2025).
14. Reddit. Retrieved from //www.reddit.com/policies/privacy-policy.
15. Privacy Policy | TikTok. (n.d.). Retrieved from https://www.tiktok.com/legal/page/us/privacy-policy/en.
16. Privacy Policy | Discord. (n.d.). Retrieved from https://discord.com/privacy.
17. Privacy Policy – Privacy & Terms – Google. (n.d.). Privacy & Terms – Google. Retrieved from https://policies.google.com/privacy.

ПРАВОВА ПРИРОДА СЕРВІСІВ СОЦІАЛЬНИХ МЕРЕЖ ЯК КОНТРОЛЕРІВ ПЕРСОНАЛЬНИХ ДАНИХ ЗГІДНО ЗІ ЗАКОНОДАВСТВОМ ЄС ТА УКРАЇНИ

Ростислав Пристай

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, Україна,79000
e-mail: rostyslav.prystai@lnu.edu.ua
ORCID ID: 0000-0002-8980-1650

Стан ефективності наявного механізму та практики захисту персональних даних користувачів соціальних мереж на території України зумовлює необхідність дослідження можливості застосування правових стандартів Європейського Союзу з метою підвищення рівня захищеності прав суб'єктів даних у цифровому середовищі, зокрема, у сфері електронних комунікацій. Імплементація, розробка якісного секторального законодавства або ж створення ефективних національних рекомендацій є можливою лише за наявності послідовного та об'єктивного дослідження особливостей діяльності зазначених сервісів, які надають постачальники загальнодоступних послуг електронних комунікацій, серед них – сервісів соціальних онлайнмереж.

Досліджено особливості правового статусу сервісів соціальних мереж як контролерів персональних даних згідно зі законодавством Європейського Союзу та України. Розглянуто особливості функціонування соціальних мереж як вебсервісів, що формують цифрові профілі користувачів, збирають та обробляють значні обсяги персональної інформації, включаючи біометричні дані, що може створювати ризики для приватності та безпеки користувачів. Проаналізовано поняття «контролер» згідно з Регламентом (ЄС) 2016/679 (GDPR) з урахуванням практики тлумачення цього терміна у відповідних рекомендаціях Європейської ради з питань захисту даних. Розкрито особливості правового статусу соціальних мереж як одноосібних або спільних контролерів, визначено основні правові підстави обробки даних, зокрема згода, легітимний інтерес та виконання договору. Також досліджено особливості територіального застосування GDPR щодо користувачів, які знаходяться поза межами ЄС, зокрема на території України.

Ключові слова: соціальні мережі, персональні дані, контролери даних, обробка персональних даних, територіальна сфера дії.

Стаття: надійшла до редакції 09.09.2025
прийнята до друку 21.10.2025