Philosophy, Economics and Law Review

Vol. 5. No. 1. 2025
Received: 18.11.2024
Revised: 29.03.2025
Accepted: 27.05.2025

Journal homepage: https://phelr.com.ua/en

UDC 343.98:004.738

DOI: 10.63341/2786-491X-2025-1-99

Legal regulation of the use of social media for marketing purposes: Aspects of human rights and constitutional guarantees

Bohdan Krytskyi*

Postgraduate Student
Scientific Institute of Public Law
03035, 2a H. Kirpa Str., Kyiv, Ukraine
https://orcid.org/0009-0007-1816-7588

Abstract. This study aimed to develop recommendations for enhancing the protection of user rights in the digital environment by implementing transparent mechanisms for monitoring compliance with human rights and optimising regulatory acts. The study included a comprehensive analysis of the legal regulation of the use of social media for marketing purposes, the specifics of user data processing and their impact on privacy, personal autonomy and freedom of choice. The analysis found that existing mechanisms for protecting personal data on social networks are insufficient, and current regulatory acts do not fully ensure transparency in information processing. In particular, users are often unaware of the scope of the data being collected and processed by social platforms, indicating a problem of insufficient awareness and the complexity of obtaining consent for data processing. It was found that social networks use personalised content algorithms, which not only aim to optimise advertising but can also shape users' digital behaviour by restricting their access to alternative information. The study also showed that Ukraine's current legislation contains significant gaps in the area of digital privacy, particularly concerning the consent of users for personal data processing, the responsibility of platforms for confidentiality breaches, and the regulation of automated decision-making systems in marketing strategies. An analysis of international standards, notably the General Data Protection Regulation, revealed substantial differences between the European and Ukrainian models of personal data protection. Based on the identified shortcomings, the study formulated recommendations for improving personal data protection mechanisms, including strengthening the responsibility of technology companies for confidentiality breaches, including imposing significant fines for the unlawful collection and use of personal data

Keywords: confidential information; digitalisation; ethical standards; commercial strategies; information privacy; digital ethics

Introduction

In modern world, social media has become an integral part of everyday life, actively influencing various aspects of social, economic and political activities. However, along with the growing influence of social media, an important issue arises regarding the legal regulation of their use, in particular in the context of marketing activities. One of the main problems is the balance between the economic interests of businesses that use social media as an effective tool for promoting goods and services and human rights, in particular the right to privacy, protection of personal data and freedom of speech. The problems of legal regulation of the use of personal data in social media, as well as the issue of achieving constitutional guarantees of human rights in the context of digitalisation, are becoming more important in the context of globalisation and rapid technological development.

Social media has become an integral part of the modern digital environment, radically transforming communication methods, information consumption, and business operations. They have impacted not only social interactions but also economic processes,

Suggested Citation:
Krytskyi, B. (2025). Legal regulation of the use of social media for marketing purposes: Aspects of human rights and constitutional guarantees. *Philosophy, Economics and Law Review*, 5(1), 99-110. doi: 10.63341/2786-491X-2025-1-99.

*Corresponding author

opening new opportunities for brand development and customer engagement. M. Shmatok (2024) notes that these platforms play a key role in shaping consumer preferences by offering businesses effective mechanisms for targeted advertising and personalised marketing. Since 2014, the Ukrainian market has shown significant growth, reflected in the increasing number of companies using social media as a marketing tool to enhance brand recognition and boost sales volumes. According to a study conducted by the East-West Digital News (EWDN) portal in 2021, about 90% of Ukrainian businesses use social media for marketing purposes, with 35% considering these platforms the most effective way to engage customers (Gyzhko & Montrin, 2023; Farmkhaus, 2023). At the same time, the active use of digital platforms creates new challenges for legal regulation. The protection of personal data in the context of online sales and marketing is an extremely complex issue, as it combines both legal and technical aspects. For example, R.Yu. Kravets (2021) pointed out that the practice of targeted advertising, which is based on the collection of data without users' explicit consent, has sparked debates among lawyers and public figures.

Despite the existence of pan-European standards for personal data protection, the practice of compliance remains a challenge even for the largest technology corporations. In several cases, companies have violated established rules, causing significant public outcry and intensifying discussions about the effectiveness of current regulatory mechanisms. This is particularly evident in high-profile scandals involving data leaks and the unauthorised use of personal information. Among the most well-known of these are the Facebook and data leaks from major technology companies. One of the most resonant scandals in the field of digital marketing was the data leak from Facebook in 2018. The British analytics firm Cambridge Analytica (2018) unlawfully gained access to the data of over 87 million users, using it to create targeted political campaigns, notably during the 2016 US elections and the Brexit referendum. This was made possible due to weak personal data protection mechanisms on Facebook: the company allowed app developers to collect data not only from their users but also from their friends on the social network. The scandal caused significant global outrage and led to the tightening of legislative requirements concerning personal data processing. Facebook founder Mark Zuckerberg was forced to testify before the US Congress, and the company was fined USD 5 billion by the Federal Trade Commission (FTC). As a result, Facebook changed its privacy policy, restricted third-party app access to data, and implemented new control mechanisms.

In addition to Facebook, several other technology companies have also been involved in scandals related to data breaches. One of the largest incidents was the Yahoo data leak in 2013-2014, when hackers gained access to 3 billion accounts, marking the largest breach in digital security. This not only led to significant financial losses for the company due to multi-billion-dollar fines but also severely undermined users' trust in online service confidentiality (Svitlyk, 2023). A similar incident occurred with LinkedIn in 2021, when information about 700 million users was made publicly available. This raised concerns about data security in professional social networks and demonstrated the vulnerability even of platforms aimed at business audiences (Tidy, 2021).

The aim of the study was to analyse the legal regulation of the use of social media in marketing, considering human rights and constitutional guarantees. The task of the work was to develop proposals for enhancing the protection of user rights in the digital environment, formulating recommendations for improving mechanisms for monitoring compliance with human rights in the online space, and exploring the possibilities of harmonising Ukrainian legislation with international standards, such as the General Data Protection Regulation.

Materials and Methods

The study was based on an interdisciplinary approach that combines legal, social, and technical aspects of analysing the use of personal data in social media for marketing purposes. This approach allows for a comprehensive evaluation of the effectiveness of existing legal norms, the impact of personalised marketing on users' rights, and potential threats associated with the use of large volumes of data. Special attention is given to analysing cases that illustrate violations of user rights in social media. Specifically, the Google scandal regarding illegal tracking of users' locations without their consent is examined, as well as the TikTok case, where the company was accused of collecting personal data of children without parental consent (Mori, 2021; Google to pay…, 2022).

The analysis of regulatory documents involved studying international and national legislation regulating the use of personal data. Specifically, documents such as the General Data Protection Regulation (GDPR), the European Convention on Human Rights (1950), the Law of Ukraine No. 2297-VI (2010), and the Law of Ukraine No. 675-VIII (2015) were examined. Special emphasis is placed on analysing provisions that define the rights and duties of social networks regarding the processing of personal data, as well as mechanisms for control by state regulators. A comparative analysis of legislative regulation of personal data in social media was carried out for the EU, the USA, and Ukraine. The EU is governed by Regulation of the European Parliament and of the Council No. 2016/679 (2016), the primary legislative act in the USA is the California Consumer Privacy Act (2018), and in Ukraine, it is governed by the Law of Ukraine No. 2297-VI (2010). The analysis considered the specific approaches to user confidentiality, legal control mechanisms, and corporate responsibility for violations.

A sociological approach was used to study the impact of personalised marketing strategies on user behaviour and rights. Statistical analysis was employed to illustrate the scale of personal data use in social media. Notably, the Pew Research Center (n.d.) study on excessive data collection by companies on customers, and research on the growth of the social media market and personalised advertising (Kubay *et al.*, 2016) were examined.

Results

The foundation of personal data protection systems lies in the European Convention on Human Rights (1950), particularly Article 8, which stipulates those public authorities shall not interfere with citizens' private life except when such interference is legally justified, necessary for a democratic society, and carried out for the purpose of ensuring national security, public order, or protecting the rights and freedoms of others. Regulatory control over personal data protection is based on international human rights treaties that view this as an integral part of the right to privacy. The Directive of the European Parliament and of the Council No. 95/46/EC (1995) became the cornerstone for national regulatory acts, including the Law of Ukraine No. 2297-VI (2010).

National legislation in Ukraine also provides for the regulatory protection of personal data. This is enshrined in Article 32 of the Constitution of Ukraine (1996), which prohibits the collection, storage, and use of confidential information without the person's consent, except in cases provided by law. The Law of Ukraine No. 2297-VI (2010) contains provisions regarding the protection of information, which are clarified by secondary legislation, such as the Typical Procedure for the Processing of Personal Data and other regulatory documents that establish the rules and conditions for processing personal information. The growing popularity of social networks and personalised advertising creates new challenges regarding confidentiality. Targeted advertising, based on the analysis of user behaviour, allows companies to create detailed consumer profiles using parameters such as preferences, geolocation, financial status, and even emotional state (Baruh & Popescu, 2017).

On the one hand, personalised advertising improves the user experience, but on the other, it may restrict freedom of choice and privacy. For example, social media algorithms can manipulate consumer preferences, creating imposed needs and stimulating the purchase of goods or services that users did not plan to buy (Chirak, 2023). Moreover, data collection models often lack sufficient transparency. Many users do not read or understand privacy policies, depriving them of the opportunity to make an informed decision regarding the use of their personal data (Solove, 2007).

Personal data refers to any information that allows identification among other individuals (Tymoshenko, 2023). According to the Law of Ukraine No. 2297-VI (2010), personal data is understood as information or a set of information about a natural person who is identified or can be specifically identified. Personal data is classified into general and sensitive categories. In Ukraine, sensitive data includes information about racial or ethnic origin, political, religious, or philosophical beliefs, membership in political parties or trade unions, criminal records, as well as data related to health, sexual life, biometric or genetic data. The practice of using personal data, especially sensitive data, for advertising purposes often leads to violations of legislation (How personal data…, 2021). The use of personal data for marketing purposes significantly impacts users' personal autonomy and privacy. On the one hand, personalised advertising creates a more relevant experience for consumers, but on the other, it breaches the boundaries of private life and limits freedom of choice.

The collection and analysis of user data allow companies to create detailed profiles that include information about preferences, habits, financial status, location, and sometimes even emotional state. These data are used to predict behaviour and influence consumer decision-making. For example, targeted advertising can create a sense of urgency for users to purchase products or services they had not intended to buy, thus restricting their personal autonomy. Many platforms gain access to data through hidden mechanisms, such as background activity tracking or reading metadata, without users' direct consent. The loss of privacy becomes one of the greatest concerns in this context. The collected data is often not only used for marketing purposes but may also be shared with third parties without users' knowledge. This creates a risk of misuse, such as data leaks or unauthorised use (Baruh & Popescu, 2017).

The "notice and choice" model, which dominates privacy regulation, requires individuals to be responsible for managing their private data. On the one hand, users can opt out of services that do not provide adequate privacy protection. On the other hand, according to marketing experts, if consumers overcome their concerns about potential data misuse and carefully assess available protection options, they can fully engage in the mutually beneficial exchange of personal information. This model is widely supported by government policies and industry standards, such as the "privacy by design" approach implemented in the USA and EU. It is expected that after being informed, consumers will take responsibility for their decisions regarding privacy and the consequences of those decisions (Solove, 2007).

However, studies showed that people are very concerned about the use of their data but often lack the knowledge or tools to effectively protect their privacy. Many users do not read or understand privacy policies and cannot predict how their data will be used in the future. This problem arises not only from personal shortcomings but also from structural barriers created by

the modern big data environment. The digital economy focuses on integrating people into its ecosystem rather than genuinely raising awareness about privacy risks (Solove, 2007). Moreover, the individually orientated "notice and choice" model may not only fail to protect privacy but also negatively affect overall public privacy standards. When decisions about privacy are left entirely to individuals, collective privacy values may decline. The reliance either on opting out of the digital economy as a form of resistance or on market tools for managing privacy does not address systemic problems. A collective understanding of privacy, considering its broader social aspects and strengthening protection for everyone, is necessary (Westin, 2003).

Thus, the use of user data for marketing purposes presents significant challenges to personal autonomy and privacy protection. To minimise the negative impact, stricter data processing regulation mechanisms need to be implemented, privacy policy transparency should be enhanced, and user awareness about their rights should be increased. An important international document in this field is the GDPR, adopted in the EU in 2016. This regulation establishes high standards for data protection that apply not only to EU member states but also to individuals and legal entities from other countries in certain cases. The GDPR defines key principles of personal data processing, such as legality, transparency, relevance, security, and data retention limitations.

It also strengthens individuals' rights, including the right to access their data, the right to delete information, and the right to informed consent. Although Ukraine is not an EU member, the provisions of the GDPR can affect entities under Ukrainian jurisdiction in cases of cross-border processing of personal data. This further highlights the importance of aligning national legislation with international standards for data protection (Ovcharenko, 2018). The EU, through the GDPR, has implemented one of the strictest and most comprehensive personal data protection systems in the world. The GDPR not only sets high standards for the processing and storage of personal information but also applies to all organisations that handle the data of EU citizens, regardless of their geographic location. This ensures the extraterritorial application of the regulation, forcing companies from other countries to adapt their processes to meet European requirements (Lehka, 2021).

Importantly, the GDPR introduces stringent requirements for transparency, informed consent, and the protection of users' rights, such as the right to access, the right to correct data, and the right to "be forgotten". This approach guarantees not only the security of personal data but also enhances companies' accountability for any violations, imposing significant fines for non-compliance. A landmark case in this regard was that of Mario Costeja González, who demanded that Google remove information about his settled debts, which remained accessible online and harmed his reputation. Costeja initially approached the newspaper "La Vanguardia", which refused to comply with his request. He then submitted a complaint to Google, which also did not comply. As a result, the Spanish Agency for the Protection of Data (AEPD) ordered Google to remove the links, but the company appealed to the Spanish court. The case was referred to the Court of the EU, which confirmed the right to remove outdated data from search results (Sukhorolsky, 2016). The GDPR came into effect the very next day, and the first complaints about its violations were filed the very next day. They concerned companies like Facebook, Instagram, WhatsApp, Google, and Android and related to the absence of users' voluntary consent for the processing of their data.

One well-known example is the scandal involving Google tracking users' locations. The company received numerous complaints in this case because its services collected geolocation data even after the tracking feature was turned off. This sparked public outrage and attracted the attention of regulators to issues of data collection transparency and users' rights to control their data (Google to pay…, 2022). Another example is the issue of storing children's data on TikTok. This platform was criticised for failing to comply with legislation regarding the protection of children's data. Regulators found that the company did not sufficiently inform parents and children about the collection of their data, which led to fines and demands for the platform to change its approach to processing minors' information (Mori, 2021).

In September 2018, the Portuguese regulator CNPD imposed a fine of EUR 400,000 on a local clinic for allowing employees to access patients' personal data using improperly created accounts. In March 2019, a company in Poland was fined EUR 220,000 for processing data on over 7 million people from public registers without properly informing those citizens (Lehka, 2021). Ukraine also took action. In 2020, the National Coordination Centre for Cybersecurity (NCCS) under the National Security and Defence Council (NSDC) of Ukraine recorded a personal data breach from one of the leading medical institutions in Dnipro. Personal data of employees and clients, including names, birthdates, addresses, phone numbers, emails, diagnoses, test results, and lists of people infected with COVID-19, were exposed. The incident was caused by errors in the configuration of information systems and databases that had internet access. This not only allowed unauthorised access to the data but also created risks of data modification, including changes to medical prescriptions, test results, and examination records (A leak of…, 2020).

"Big data" is associated with vast amounts of information generated by the informatisation of economic activities and everyday life. In the context of social media, it includes large volumes of structured data, which are often automatically filled through sensors, mobile devices, or platforms (Khrupovych & Borysova, 2021).

Statistics show a rapid growth of the social media market, accompanied by large-scale collection of personal information. Social networks like Facebook, Instagram, and TikTok generate enormous volumes of data about their users, including timestamps, geographical markers, interaction history, and personalised information (Fig. 1).

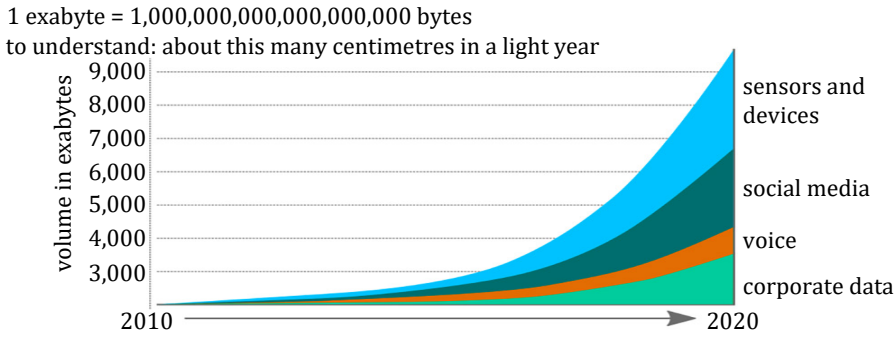

Figure 1. Dynamics of data volume growth by categories from 2010 to 2020
Source: K. Kubay *et al.* (2016)

The rapid increase in data volumes, especially in social networks, shows their key role not only in everyday life but also in business activity. Structured information generated in social media platforms becomes the basis for effectively using these platforms for marketing purposes (Marynin, 2024). In modern competitive environment, using social media has become an essential part of successful business operations. Through these channels, businesses can not only maintain their market positions but also actively grow. Having social media accounts allows businesses to increase the number of potential customers, improve sales, and simplify customer interactions. This enables providing personalised services, meeting the needs of each customer, and responding more quickly to their requests (Maksymova *et al*., 2023).

A key element of a successful marketing strategy is a clear understanding of one's target audience. The portrait of the target audience helps identify the key characteristics of potential clients, allowing for optimised marketing campaigns, reducing unsuccessful contacts, and enhancing advertising effectiveness. A detailed portrait of the target client helps to understand the needs, motivations, and problems of buyers that the business can solve with its products or services. This allows businesses to create unique offers that precisely meet customers' expectations, thereby increasing sales and profits. Understanding the target audience also helps determine through which channels clients learn about the product and which devices they use. This information can be used to strengthen existing promotion channels or launch new ones (Khadzhiradieva *et al.*, 2024).

To create a portrait of the target audience, businesses analyse various characteristics, including geographic, demographic, social, and behavioural features (Jansen *et al*., 2024). Particular attention is paid to clients' interests and their current needs, helping to demonstrate an understanding of consumer problems and offer solutions. Various methods are used to gather such data, including personal communication, online surveys, social media data analysis, and the use of analytics tools such as Google Analytics. These tools help track client behaviour, their location, the devices they use, and other details (Levinson, 2010).

Using social media for marketing purposes often raises questions about consumer freedom of choice and may shape imposed preferences. Due to content personalisation algorithms, users are shown products and services that match their previous search queries or online behaviour. This can limit access to alternative information, narrowing the choice to only those goods or services that the system deems relevant (Arrigo *et al.*, 2021). As a result, consumers are influenced by advertising strategies that can manipulate their needs and decisions, reducing them to pre-determined business goals. This approach not only affects consumer behaviour but also creates dependency on the algorithms that dictate what to buy or be interested in (Chirak, 2023).

The informational influence of social networks can reach significant scales and even impact society through information wars. In this context, influence is defined as the process aimed at changing the behaviour, thoughts, or decisions of an individual or group under the influence of another. It can be directed when the goal is to achieve a specific outcome or indirect, occurring unintentionally through external circumstances. Directed influence aims to change beliefs or behaviour; for example, convincing someone to take certain actions or make specific decisions. Indirect influence occurs without a clear goal as a result of random circumstances or actions. Social networks, due to their communication capabilities, have become a powerful tool of influence, connecting people and helping them achieve common goals. They provide links between individuals and groups exchanging information, influencing decisions, and coordinating actions (Chirak, 2023).

Protecting personal data on social networks at the individual level is a critical aspect of online security,

as evidenced by numerous empirical studies. For instance, the results of the national survey "Online Security" show that fraudulent activities related to personal data are widespread in Ukraine. According to the study, 30% of respondents have fallen victim to various forms of online fraud. This indicates that many social media users in Ukraine are insufficiently aware of proper security measures, leaving them vulnerable to various types of fraudulent activities, such as phishing, malware distribution, identity theft, and financial fraud (Kravchuk, 2024a).

One of the main elements of individual protection is privacy settings on social media (Kroll & Stieglitz, 2021). Popular platforms like Facebook, Instagram, and Twitter allow users to control access to their personal data and adjust relevant settings. For example, users can limit the number of people who have access to their personal data, photos, and posts. It is also important to be cautious when sharing personal data on social media. Users should avoid publishing excessive information such as credit card numbers, passport details, or home addresses that could be exploited by malicious actors. Instead, it is recommended to provide only the minimum personal data necessary for normal social media use (Kravchuk, 2024b; Humenyuk, 2024).

It is also important to consider how Ukrainian legislation aligns with the EU GDPR, the California Consumer Privacy Act (2018), and the regulations of EU countries. The GDPR, adopted in the EU, sets high standards for personal data protection. Key principles include legality, transparency, and fairness in processing, data minimisation, and ensuring the rights of data subjects. For example, the GDPR guarantees users' rights to access, correct, delete ("right to be forgotten"), and transfer their data. The regulation also has extraterritorial application: it applies to all companies processing data of EU citizens, regardless of their geographic location. The California Consumer Privacy Act (2018), effective in California (USA), is focused on protecting consumer rights in the digital environment. Its key provisions include the right for consumers to know what data is being collected about them, request its deletion, or prohibit its sale. Although the California Consumer Privacy Act does not have extraterritorial application like the GDPR, its provisions still influence the business practices of many companies operating in the US (Dyakovsky, 2023).

At the same time, Ukraine's legislation in the field of personal data protection is based on the Law of Ukraine No. 2297-VI (2010). While this law incorporates some GDPR provisions, it has certain limitations. For instance, data subjects' rights, such as the "right to be forgotten" or the right to data portability, are underdeveloped. Additionally, fines for violations are much lower than those in the GDPR, which does not always motivate companies to comply with confidentiality standards. Ukrainian legislation also lacks extraterritorial application, making it difficult to protect citizens' data in the international context (Dyakovsky, 2023).

With the development of the digital economy, personal data has become an important resource for business, particularly in marketing. Through the analysis of behavioural patterns, preferences, and personal characteristics, companies can form personalised advertising offers, optimise customer acquisition strategies, and enhance sales efficiency. However, this approach raises significant ethical questions, particularly regarding data collection transparency, informed consent from consumers, the line between legal targeting and manipulation, and companies' responsibility for data security. One of the key ethical dilemmas is the issue of obtaining user consent for processing their personal data (Nicholls *et al.*, 2016). Many companies use complex and unclear privacy policies that make it difficult for consumers to understand the extent of data being collected and how it will be used. This creates a situation where users formally agree to data processing without fully understanding all the consequences.

Moreover, consent is often obtained through mechanisms of "covert data collection", where information is gathered in the background without active interaction with the user (Zhang & Rodgers, 2023). For instance, mobile apps may track geolocation or access contacts without explicit notification (Ylitalo, 2024). Such practices contradict the principle of "transparency and control", which requires that users have a real opportunity to manage their personal information (Krat, 2020). Marketing strategies based on personalised advertising allow companies to significantly improve the quality of the user experience. For example, instead of random ads, users receive offers that match their interests (Tucker, 2014). However, this approach can have a reverse effect – the formation of a so-called filter bubble, where the user is limited to only the content the system deems relevant. This narrows access to alternative information, reducing the possibilities for independent choice (Dahlgren, 2021).

Another important ethical issue is the use of personal data to influence consumer decisions. A vivid example is "emotional artificial intelligence" technologies, which analyse users' mood through facial expressions, voice tone, or behaviour patterns. Protecting collected personal data is another significant ethical challenge. Many companies store vast amounts of sensitive information but do not always ensure its proper security. Frequent data leaks, hacker attacks, and unauthorised sales of information to third parties indicate flaws in the protection of user privacy. Adhering to ethical principles not only helps companies avoid reputational risks but also becomes an important strategic factor for long-term success. Investments in ethical marketing should be considered not as a cost but as an investment in brand sustainability and competitiveness in the future. Only those companies that ensure

a high ethical culture in their activities can maintain consumer trust, uphold their reputation, and remain market leaders (Rayko *et al.*, 2024).

To minimise ethical risks in digital marketing, it is essential to adhere to the principles of responsible use of personal information. Companies should ensure transparency by clearly informing users about the collection and use of their data. An important aspect is voluntary and informed consent, which implies that users have the right to decide what data they are willing to provide and receive clear conditions for its processing. To protect privacy, the amount of collected information should be limited to the minimum necessary level, and proper security measures should be guaranteed to prevent unauthorised access and data leaks (Rayko *et al.*, 2024). When comparing the approaches of different EU countries, one can see how national laws adapt to the requirements of the GDPR. For example, Germany has introduced strict rules for processing medical data, France has strengthened child protection in the digital environment, and Italy has created detailed regulations for processing financial information. Ukrainian legislation currently lacks such detail, making it less effective in specific areas (Bryntsev, 2021).

Under the GDPR provisions, significant administrative fines are imposed for violations of personal data processing rules. For less serious violations, the fine can be up to EUR 10 million or 2% of the company's total annual turnover from the previous financial year, whichever is higher. In cases of more serious violations, fines can reach EUR 20 million or 4% of the company's total annual turnover from the previous year, depending on which sum is higher. Meanwhile, Ukrainian legislation provides for significantly lower fines for similar violations. For example, late reporting or providing false data to the Ombudsman of the Verkhovna Rada of Ukraine results in administrative liability. The fine typically amounts to around UAH 5,100, which is much lower than the European sanctions. Similar liability is also imposed for non-compliance with the Ombudsman's lawful requests (Dyakovsky, 2023).

It is also important to note the structural differences between the GDPR and the California Consumer Privacy Act (2018). While the GDPR has a global nature and focuses on protecting the rights of data subjects, the California Consumer Privacy Act is more focused on regulating relationships between consumers and companies, particularly on the ability to prohibit the sale of data. To ensure Ukrainian legislation meets modern challenges, several changes need to be made. First, align the norms with the GDPR by expanding the rights of data subjects and introducing extraterritorial applicability. Second, strengthen companies' liability for violations, including increasing the size of fines. Third, develop specific rules for sectors such as healthcare and finance, similar to the practices of EU countries (Bryntsev, 2021).

Research results showed that the issue of protecting personal data in social networks remains one of the most pressing problems in the digital environment. The use of personal information for marketing purposes creates significant legal and ethical challenges, particularly regarding confidentiality, user consent, and data processing transparency. Analysing international and national legal norms highlights the need for stronger control over the use of personal data in commercial practices. Thus, harmonising Ukrainian legislation with international standards such as the GDPR and California Consumer Privacy Act (2018) is an essential step to ensure effective protection of citizens' personal data. This will not only strengthen legal protection but also align Ukraine with modern international standards in the field of privacy.

Discussion

The results of the study confirmed that the issue of protecting personal data in social networks is highly relevant in the modern digital environment. Significant legal and ethical challenges have been identified regarding the use of personal information for marketing purposes. The main aspects are confidentiality, user consent, and data processing transparency. These problems are confirmed by numerous international studies, which emphasise the need to strengthen control over commercial practices that involve the use of personal data (Havur *et al*., 2020).

Research into international legal norms indicates that the issue of privacy is not unique to Ukraine. The GDPR, adopted by the EU in 2016, sets high data protection standards that apply to all organisations handling information about EU citizens. D.J. Solove (2007) notes that the "notice and choice" system is inadequate to ensure transparency in the use of personal data, as users often do not fully realise the extent of the information being collected. This aligns with the results of this study, which showed that most users do not read or understand the privacy policies of social networks. Studies by L. Baruh & M. Popescu (2017) demonstrated that personalised advertising can not only improve users' experiences but also limit their personal autonomy by creating an artificial need for products or services they initially did not plan to purchase. These findings correlate with the research of P.M. Dahlgren (2021), who revealed the concept of the "digital cocoon", which forms users' preferences, limiting their access to alternative information.

A significant contribution to the discussion of privacy issues was made by A.F. Westin (2003), who emphasised the need for a collective approach to ensuring the security of personal data. He argued that shifting responsibility solely to users does not resolve the issue of effectively protecting information. J. Levinson (2010) also supported this position, emphasising that businesses that implement ethical standards in using

personal data have competitive advantages and higher levels of trust from clients. The findings of this research indicated that the use of personal data for marketing purposes creates numerous risks. A low level of user awareness is a significant issue, as the Pew Research Centre (n.d.) showed that 72% of respondents believe companies collect excessive information about them, and 65% are concerned about potential data leaks. The lack of transparency in data collection is confirmed by a case with Google, where the company continued to collect location data from users even after the tracking feature was disabled, demonstrating the need for stronger regulatory oversight (Google to pay…, 2022). The manipulative impact of personalised advertising is another serious challenge, as research by D.V. Rayko *et al.* (2024) showed that using artificial intelligence (AI) to analyse users' emotional states can lead to "emotional marketing", which significantly influences consumer decision-making and may limit users' autonomy.

Furthermore, the results confirmed the critical role of social networks in shaping the digital public space. J.M. Balkin (2021) argued that social network regulation should focus on creating reliable intermediary institutions that ensure the sustainable development of the digital environment and uphold the principles of free speech, political democracy, and cultural diversity. Regulation approaches to social networks differ significantly depending on the national context. K.A. Andresen (2011) emphasised the need to implement policies to reduce business and legal risks, such as the loss of trade secrets, violations of intellectual property rights, and failure to meet confidentiality obligations. R.E. Ennan (2024) examined the issue in the context of digital law, emphasising the need for its digitalisation and adaptation of traditional legal mechanisms to the digital economy. This aligns with the results of this study, which showed the importance of harmonising the legal regulation of digital rights and digital information circulation. D.V. Rayko *et al.* (2024) highlighted the risks of personalised advertising and its potential impact on users' autonomy through AI usage.

When comparing Ukrainian legislation with international standards, it is worth noting several key aspects: the GDPR imposes significantly stricter sanctions for violations of personal data processing than the Law of Ukraine No. 2297-VI (2010). In Ukraine, fines for privacy violations are much lower than in the EU, which reduces the responsibility of companies for failing to meet data security standards (Dyakovsky, 2023). To improve personal data protection in Ukraine, it is necessary to improve the legal framework according to international standards, strengthen companies' liability for personal data processing, and implement educational initiatives to raise users' digital literacy. Thus, harmonising Ukrainian legislation with GDPR norms will help enhance personal data protection and ensure greater transparency in the digital environment. Research findings from H. Felzmann *et al.* (2019), C. Santos *et al*. (2021), and D. Almeida *et al.* (2022) confirmed that privacy and transparency in social networks are highly relevant. The use of personal data for marketing purposes creates significant challenges, as users often do not understand how their data is used.

One possible solution is the implementation of data usage control architectures, which include semantic information management, automated compliance with pivacy policies, and digital signatures for data authenticity verification (Felzmann *et al.*, 2019). These technologies can enhance the transparency of information processing on social networks and minimise the risks of data breaches or unauthorised use. Research by C. Santos *et al.* (2021) emphasised that consent management platforms (CMPs) used in social networks may violate the principles of transparency and user control over their data. They often act not as neutral intermediaries but as full-fledged personal data controllers, responsible for additional processing, sorting trackers, and automatically embedding third-party advertisers. This means that Ukrainian legislation needs to strengthen regulatory mechanisms to control such platforms to ensure user rights protection.

Another critical challenge is the development of facial recognition technology (FRT) in social networks. D. Almeida *et al.* (2022) noted that uncontrolled implementation of FRT could lead to privacy violations, biometric data collection without consent, and even human rights abuses. The introduction of regulatory standards should include not only the GDPR but also an impact assessment on human rights (HRIA), which will help avoid the opaque use of biometric technologies. Additionally, it is necessary to reconsider automated advertising algorithms that could manipulate users' choices. H. Felzmann *et al.* (2019) highlighted that transparency in the use of AI should not only comply with legal norms but also consider users' real perceptions of how their data is collected and analysed. Implementing such measures will minimise the risks of data breaches, ensure transparency in information processing, and increase user trust in the digital environment.

Conclusions

Data protection is an essential aspect of safeguarding human rights in the digital age. A comparison of Ukrainian national legislation with international standards, such as the GDPR and the California Consumer Privacy Act, reveals significant gaps that need to be addressed. Aligning these norms will allow Ukrainian legislation to adapt to contemporary international challenges in the field of privacy. In summary, it can be said that Ukraine is in the process of forming national awareness, which requires improving the legal regulation of information relations according to modern challenges. One of the key tasks of the state in this regard is to determine strategic priorities for legal regulation

and create proper guarantees to ensure citizens' rights in the information sphere.

To achieve this goal, it is necessary to bring national legislation in line with European norms and international standards, as well as develop a unified legislative act regulating the processes of collecting, processing, protecting, and transferring personal data similar to the GDPR. An important aspect is also the harmonisation of the terminology with international normative documents, the implementation of mandatory certification to ensure information security, the development of modern cryptographic and encryption technologies, as well as strengthening liability for violations of personal data protection norms. Moreover, a significant role in enhancing personal data protection is played by citizens' awareness of their rights and how to protect their privacy. To this end, it is necessary to expand educational initiatives that promote increased digital literacy among the population, as well as introduce mandatory training programmes for companies working with personal data.

It is also worth considering the creation of an independent state authority or agency to oversee the processing of personal data, which would monitor companies' activities in this field, provide recommendations for improving legislation, and respond to citizens' complaints in cases of rights violations. Such a practice is already effectively implemented in many European countries, ensuring better protection of users' personal information. Further scientific research should be directed towards a deeper study of international experience to improve the Ukrainian personal data protection system and enhance its alignment with contemporary challenges. In the future, it is worth researching the effectiveness of different approaches to regulating privacy and personalised advertising in various countries, as well as evaluating the impact of new technologies such as artificial intelligence and blockchain on personal data protection.

Acknowledgements
None.

Funding
None.

Conflict of Interest
None.

References
[1] A leak of personal data of patients was revealed in one of the largest private clinics in Dnipro. (2020). Retrieved from https://interfax.com.ua/news/general/692349.html.
[2] Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377-387. doi: 10.1007/s43681-021-00077-w.
[3] Andresen, K.A. (2011). Marketing through social networks: Business considerations-from brand to privacy. *William Mitchell Law Review*, 38(1), article number 10.
[4] Arrigo, E., Liberati, C., & Mariani, P. (2021). Social media data and users' preferences: A statistical analysis to support marketing communication. *Big Data Research*, 24, article number 100189. doi: 10.1016/j.bdr.2021.100189.
[5] Balkin, J.M. (2021). How to regulate (and not regulate) social media. *Journal of Free Speech Law,* 1(1), 71-96.
[6] Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, 19(4), 579-596. doi: 10.1177/1461444815614001.
[7] Bryntsev, O. (2021). Actual problems of personal data protection in Ukraine. In S.V. Glibko & K.V. Efremova (Eds.), *Collection of scientific works Research Institute of Legal Support for Innovative Development of the National Academy of Legal Sciences of Ukraine* (pp. 43-48). Kharkiv: Research Institute of Legal Support for Innovative Development of the National Academy of Legal Sciences of Ukraine.
[8] California Consumer Privacy Act. (2018, June). Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.
[9] Cambridge Analytica. (2018). *Facebook data-harvest firm to shut*. Retrieved from https://www.bbc.com/news/business-43983958.
[10] Chirak, I.M. (2023). *The economics of social media.* Ternopil: Western Ukrainian National University.
[11] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/254%D0%BA/96-%D0%B2%D1%80#Text.
[12] Dahlgren, P.M. (2021). A critical review of filter bubbles and a comparison with selective exposure. *Nordicom Review*, 42(1), 15-33. doi: 10.2478/nor-2021-0002.
[13] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng.
[14] Directive of the European Parliament and of the Council No. 97/66/EC "Concerning the processing of personal data and the protection of privacy in the telecommunications sector". (1997, December). Retrieved from https://eur-lex.europa.eu/eli/dir/1997/66/oj/eng.

[15] Dyakovsky, O. (2023). Comparative characteristics of personal data protection under national and european legislation. *Juridical Scientific and Electronic Journal,* 8, 278-280. doi: 10.32782/2524-0374/2023-8/64.
[16] Ennan, R.E. (2024). Digitalization of law and formation of digital law. *Uzhhorod National University Herald Series Law*, 1(83), 200-205. doi: 10.24144/2307-3322.2024.83.1.29.
[17] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.
[18] Farmkhaus, P. (2023). Social networks as a tool for state communication with citizens: Analysis of problems and paths for optimization. *Scientific Notes of Taurida V I Vernadsky University Series Public Administration*, 6, 169-174. doi: 10.32782/tnu-2663-6468/2023.6/27.
[19] Felzmann, H., Villaronga, E.F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, 6(1). doi: 10.1177/2053951719860542.
[20] Google to pay $391.5 million for secretly tracking users' location history. (2022). Retrieved from https://interfax.com.ua/news/telecom/872134.html.
[21] Gyzhko, M., & Montrin, I. (2023). Theoretical foundations of marketing in social networks. In A.A. Mazaraki (Ed.), *Brand management: Marketing technologies: Abstracts of the 5th international scientific and practical conference* (pp. 300-301). Kyiv: State Trade and Economic University.
[22] Havur, G., Sande, M.V., & Kirrane, S. (2020). Greater control and transparency in personal data processing. In S. Furnell, P. Mori, E. Weippl & O. Camp (Eds.), *Proceedings of the 6th international conference on information systems security and privacy* (pp. 655-662). Valletta: SciTePress. doi: 10.5220/0009143206550662.
[23] How personal data became a bargaining chip for political forces in elections. (2021). Retrieved from https://cedem.org.ua/analytics/personalni-dani-vybory/.
[24] Humenyuk, V. (2024). *Legal regulation of facial recognition technologies in the EU, the USA and Ukraine: Private and public law aspects*. Kyiv: National University "Kyiv-Mohyla Academy".
[25] Jansen, B.J., Aldous, K.K., Salminen, J., Almerekhi, H., & Jung, S.G. (2024). *Understanding audiences, customers, and users via analytics: An introduction to the employment of web, social, and other types of digital people data.* Cham: Springer. doi: 10.1007/978-3-031-41933-1.
[26] Khadzhiradieva, S., Bezverkhniuk, T., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social and Legal Studios*, 7(3), 245-256. doi: 10.32518/sals3.2024.245.
[27] Khrupovych, S.E., & Borysova, T.M. (2021). Using artificial intelligence in marketing analysis of unstructured data. *Marketing and Digital Technologies*, 5(1), 17-26. doi: 10.15276/mdt.5.1.2021.2.
[28] Krat, O.O. (2020). *Organization of marketing activities in social networks*. Poltava: Poltava University of Economics and Trade.
[29] Kravchuk, V.O. (2024a). Administrative-legal protection tasks of personal data in social networks. *Precarpathian Legal Bulletin*, 2(55), 65-68. doi: 10.32782/pyuv.v2.2024.14.
[30] Kravchuk, V.O. (2024b). Personal data protection in social networks in the EU, the USA and China. In I.V. Zhukova & E.O. Romanenko (Eds.), *Modern aspects of science modernization: Status, problems, development trends: Materials of the XXXV international scientific and practical conference*(pp. 90-96). Istanbul: Public Scientific Organization "All-Ukrainian Assembly of Doctors of Science in Public Administration".
[31] Kravets, R.Yu. (2021). *Use of personal data in advertising and sales*. Retrieved from http://protocol.ua/ua/vikoristannya_personalnih_danih_v_reklami_ta_prodagah/#google_vignette.
[32] Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behaviour and Information Technology*, 40(1), 1-19. doi: 10.1080/0144929x.2019.1584644.
[33] Kubay, K., Gazin, A., Horbal, A., Shulga, E., & Shapovalenko, E. (2016). *Open data open guide*. Retrieved from https://socialdata.org.ua/manual/.
[34] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.
[35] Law of Ukraine No. 675-VIII "On Electronic Commerce (E-Commerce)". (2015, September). Retrieved from https://zakon.rada.gov.ua/laws/show/en/675-19#Text.
[36] Lehka, O.V. (2021). Current issues of personal data protection: Domestic and international experience. *Legal Position*, 2(31), 74-79. doi: 10.32836/2521-6473.2021-2.15.
[37] Levinson, J. (2010). *Guerrilla marketing for nonprofits*. Irvine: Entrepreneur Press.
[38] Maksymova, J., Rudyk, O., & Zaletska, I. (2023). Use of social media for effective activities of modern enterprises. *Economy and Society*, 47. doi: 10.32782/2524-0072/2023-47-75.

[39] Marynin, D.L. (2024). Big data collection and processing methods used in modern systems. *Scientific Notes of Taurida National V.I. Vernadsky University Series Technical Sciences,* 35(74(2)), 369-375. doi: 10.32782/2663-5941/2024.2/51.
[40] Mori, Y. (2021). *TikTok accused of illegally collecting personal data of underage users*. Retrieved from https://suspilne.media/culture/124635-tiktok-zvinuvaucut-u-nezakonnomu-zbori-osobistih-danih-nepovnolitnih-koristuvaciv/.
[41] Nicholls, S.G., Langan, S.M., & Benchimol, E.I. (2016). Reporting and transparency in big data: The nexus of ethics and methodology. In B.D. Mittelstadt & L. Floridi (Eds.), *The ethics of biomedical big data* (pp. 339-365). Cham: Springer. doi: 10.1007/978-3-319-33525-4_15.
[42] Ovcharenko, Ya.O. (2018). General data protection regulation aand possibility to apply it in Ukraine. *Legal Scientific Electronic Journal,* 3, 236-239.
[43] Pew Research Center. (n.d.). Retrieved from https://www.pewresearch.org/.
[44] Rayko, D.V., Masalab, O.V., & Alekseev, O.S. (2024). Ethical aspects of digital marketing and their impact on consumers and society. In E.I. Sokol (Ed.), *Information technologies: Science, engineering, technology, education, health: Abstracts of the 32nd international scientific and practical conference*. Kharkiv: National Technical University "Kharkiv Polytechnic Institute".
[45] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[46] Santos, C., Nouwens, M., Toth, M., Bielova, N., & Roca, V. (2021). Consent management platforms under the GDPR: Processors and/or controllers? In N. Gruschka, L.F.C. Antunes, K. Rannenberg & P. Drogkaris (Eds.), *9th Annual privacy forum: Proceedings: Privacy technologies and policy* (pp. 47-69). Cham: Springer. doi: 10.1007/978-3-030-76663-4_3.
[47] Shmatok, M. (2024). The role of social media in creating and naging the brand image of a small business. *Scientific View: Economics and Management*, 1(85), 91-97 doi: 10.32782/2521-666X/2024-85-14.
[48] Solove, D.J. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet*. New Haven, London: Yale University Press.
[49] Sukhorolsky, P. (2016). The right to be forgotten in the legal system of the European Union: Realities, problems and prospects. In *The science of international law at the turn of the century. Trends in development and transformation: A special edition of scientific articles* (pp. 90-101). Lviv: Ivan Franko National University of Lviv.
[50] Svitlyk, Y. (2023). *The most famous hacker attacks that hit the whole world*. Retrieved from https://root-nation.com/en/articles-en/tech-en/en-most-famous-hacker-attacks/.
[51] Tidy, J. (2021). *How your personal data is being scraped from social media*. Retrieved from https://www.bbc.com/news/business-57841239.
[52] Tucker, C.E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546-562. doi: 10.1509/jmr.10.0355.
[53] Tymoshenko, O. (2023). Protection of personal data in civil legal relations: National legal provision through the prism of the practice of the European Court of Human Rights. *Analytical and Comparative Jurisprudence*, 4, 165-172. doi: 10.24144/2788-6018.2023.04.27.
[54] Westin, A.F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453. doi: 10.1111/1540-4560.00072.
[55] Ylitalo, J. (2024). *Smart phones and data collection: Autonomous agency in everyday experience*. Espoo: Aalto University.
[56] Zhang, W., & Rodgers, S. (2023). Linking ethnicity targeting with artificial intelligence and data collection: Perceptions and behavioral responses of black consumers. *Journal of Current Issues & Research in Advertising,* 44(3), 37-391. doi: 10.1080/10641734.2023.2212022.

Правове регулювання використання соціальних медіа в маркетингових цілях: аспекти прав людини та конституційні гарантії

Богдан Крицький
Аспірант
Науково-дослідний інститут публічного права
03035, вул. Г. Кірпи, 2а, м. Київ, Україна
https://orcid.org/0009-0007-1816-7588

Анотація. Метою роботи було вироблення рекомендацій для підвищення захисту прав користувачів у цифровому середовищі шляхом впровадження прозорих механізмів контролю за дотриманням прав людини та оптимізації нормативних актів. Дослідження охопило комплексний аналіз правового регулювання використання соціальних медіа в маркетингових цілях, особливості обробки персональних даних користувачів та їхній вплив на приватність, особисту автономію і свободу вибору. За результатами аналізу встановлено, що існуючі механізми захисту персональних даних у соціальних мережах є недостатніми, а чинні нормативні акти не повною мірою забезпечують прозорість обробки інформації. Зокрема, користувачі часто не усвідомлюють обсягу даних, які збираються та обробляються соціальними платформами, що свідчить про проблему недостатньої інформованості та складність процесу отримання згоди на обробку даних. Виявлено, що соціальні мережі використовують алгоритми персоналізованого контенту, які не лише спрямовані на оптимізацію реклами, а й можуть формувати цифрову поведінку користувачів, обмежуючи їхній доступ до альтернативної інформації. Дослідження також показало, що поточне законодавство України містить значні прогалини у сфері цифрової приватності, зокрема в аспектах отримання згоди користувачів на обробку персональних даних, відповідальності платформ за порушення конфіденційності та регулювання використання автоматизованих систем ухвалення рішень у маркетингових стратегіях. Аналіз міжнародних стандартів, зокрема Загальний регламент про захист даних, показав суттєві відмінності між європейською та українською моделями захисту персональних даних. З огляду на виявлені недоліки, у роботі сформульовано рекомендації щодо удосконалення механізмів захисту персональних даних, зокрема посилення відповідальності технологічних компаній за порушення конфіденційності, включно з введенням суттєвих штрафів за незаконне збирання та використання персональних даних

Ключові слова: конфіденційна інформація; цифровізація; етичні стандарти; комерційні стратегії; інформаційна приватність; цифрова етика