RIGHT TO PRIVACY ON THE INTERNET IN THE SOCIAL MEDIA CONTEXT

Kristina Tverezovska
PhD Student of the Department of Constitutional Law of Ukraine,
Yaroslav Mudryi National Law University,
77 Pushkinska Str., Kharkiv, Ukraine, 61024
https://orcid.org/0009-0001-6167-1575
k.s.tverezovska@nlu.edu.ua

Abstract. This research study has been conducted with a deliberate synthesis of both theoretical and practical components. This approach is grounded in the observation that research studies often tend to adopt either a purely theoretical or an exclusively practical and applied orientation. The author’s objective was to systematize theoretical and analytical insights concerning the right to privacy on the Internet within the context of social media functionality. This was achieved through a comprehensive examination that combined theoretical underpinnings with an analysis of real-world court cases. Commencing this research endeavor, an exhaustive analysis of the definitions associated with the concept of “social media” was undertaken. The intricate relationship between “social media” and “social networks” was scrutinized and elucidated. Subsequently, the author delved into the multifaceted issue of privacy and its evolving nature in the backdrop of the digitization process. The author provided a historical panorama, tracing the inception of the concept of privacy, charting its developmental trajectory, and elucidating its normative establishment at both the international and national levels. In recognition of the non-absolute character of the right to privacy, this research delineated the permissible boundaries within which state intervention may be exercised in the exercise of this right. In light of the comprehensive analysis conducted, practical instances were identified and examined, vividly illustrating the extent to which the necessary privacy safeguards are adhered to in the digital domain. An exploration of the jurisprudence of the European Court of Human Rights about this matter facilitated the observation of the intricate interplay between the right to privacy and other rights, such as the right to access the Internet, the right to access information, and the right to the preservation of honor and dignity. This exploration accentuated both the significance and complexity of achieving a delicate equilibrium in upholding these rights by their respective claimants. In any scenario, it is underscored by the author that states, law enforcement agencies, judicial authorities, as well as individuals and legal entities, are obligated to exert concerted efforts toward aligning the online environment with the standards set forth by human rights conventions.

Keywords: human rights, right to privacy, social media, social network, Internet, personal data, privacy, information and communication technologies.
INTRODUCTION

The rapid evolution of information technologies and the proliferation of social media platforms have significantly impacted the development of social relationships within the globalized context. In recent years, the discourse surrounding information security, cyber conflicts, political disinformation, as well as privacy, and the protection of users’ rights in social networks, has garnered substantial attention. Analogous to significant relationships, public relations within the domain of constitutional and legal analysis of digital human rights within the framework of social media necessitate legal frameworks, both on an international and national scale. The pertinence of the chosen subject matter is underscored by the increasing focus of international organizations, including the United Nations, on conferring distinct legal status upon digital rights. However, within domestic discussions, the regulation of individual digital rights within constitutional law remains largely unaddressed. This raises questions concerning the impact of digitization on the formulation of digital human rights and under which circumstances state intervention in the realm of internet freedom should be executed through legal measures.

The legal governance of social media is influenced by a multitude of factors, primarily contingent on the presence or absence of democratic principles in public administration, legislative mechanisms governing interactions between social media users and providers, as well as the safeguarding of human rights, particularly freedom of speech and self-expression. The proliferation of digital technology and the broadening avenues of interpersonal communication have rendered information acquisition increasingly accessible, consequently giving rise to novel threats to individual privacy within society. Scientific and technological advancements constitute the principal catalyst for the augmentation of the catalog of human rights, contributing to the emergence of what is often referred to as fourth-generation rights, denoting the most contemporary human rights.

However, concerning the focus of this inquiry, the classification of the right to online privacy within the realm of fourth-generation human rights is not an unequivocal matter. This complexity arises from the fact that while the medium through which this right is exercised is the internet—a characteristic often associated with fourth-generation rights—the essence of this right pertains to an individual’s entitlement to the preservation of their private life, aligning it more closely with first-generation rights.

Therefore, there exists a pressing need to formulate legal regulations governing the attribution of rights related to internet usage, encompassing the dissemination, retrieval, compilation, processing, and utilization of information. Social media has engendered an unprecedented global public domain that experiences substantial expansion with each passing day, transcending geographical boundaries. Such an expansive domain necessitates legal frameworks not only at the national level but also at the international level to effectively address the myriad challenges and complexities that accompany its existence.

MATERIALS AND METHODS

The study of the issue of privacy on the Internet is gaining more and more relevance over time, which prompts researchers and lawyers to new comparative-based research analytic metrics. American lawyers Samuel D. Warren and Louis D. Brandeis are usually considered the authors of the origin of the privacy concept. With the development of scientific and
technological processes, more and more scientists have explored the topic of privacy in the digital age, including Australian researcher Stephen Coleman, Dutch researchers Pieter Kleve and Richard De Mulder, etc. Among those Ukrainian researchers who analyzed the issues of privacy on the Internet and the protection of personal databases in the online area are Paziuk A. V., and Razmetaieva Yu. S., Hnatiuk S. L. etc. Several works by domestic researchers, Chupryna L., Tsekhan D. M., and foreign researchers, primarily Ryan Garcia, Thaddeus Hoffmeister, Jonathan Obar, Steven Wildman, Thornley Joseph, Handley A., Chapman A., etc., are devoted to the issue of social media study. Given the increased attention of society to the exercise of human rights on the Internet, the issue of privacy will continue to be explored driven by new challenges of today.

The methodological basis of this study is general and special methods of scientific knowledge, the application of which allowed to ensure the scientific reliability of the presented material and the argumentation of general conclusions. This research was based on the following scientific methods: system method, historical and legal method, case study, and research of current judicial practice, in particular the practice of the European Court of Human Rights.

RESULTS AND DISCUSSION

Social media is a term that lacks a precise, scientifically grounded definition. In 2010, scholars from the ESCP Business School provided a definition for social media, which continues to be widely cited in contemporary English-language academic literature. According to their formulation, social media (or social networking services) encompass a category of internet applications rooted in the ideological and technological principles of Web 2.0. These platforms enable the generation of user-generated content. While many individuals associate social media primarily with prominent platforms like Facebook, Twitter (currently rebranding as X), LinkedIn, and others, it is crucial to acknowledge that the scope of social media extends far beyond these well-known sites. Black’s Law Dictionary defines social media as any cellular phone or internet-based tools and applications employed for information sharing and dissemination. A more detailed characterization is proffered by Joseph Thornley, who describes social media as online communications wherein individuals fluidly transition between the roles of audience and author. Furthermore, certain scholars view social media as a continuously expanding and evolving assortment of online tools, platforms, and applications that facilitate interactive information sharing among users. It is worth noting that within the Ukrainian-speaking academic community, the terms “social media” and “social networks” are frequently conflated, and erroneously treated as synonyms. However, American expert D. M. Scott aptly distinguishes between the two, positing that “social media” constitutes the superset, while “social networking” represents a subset.

The utilization of software by both the US Department of Homeland Security (DHS) and Oregon State authorities for monitoring Black Lives Matter hashtags on popular social media platforms such as Facebook and Twitter has raised significant concerns. This level of state surveillance unquestionably poses a substantial challenge to individual freedoms, particularly the fundamental right to freedom of speech, and presents potential implications for the democratic fabric.
The Guide to Human Rights for Internet Users, along with the Explanatory Memorandum (Recommendation CM/Rec (2014)6 of the Committee of Ministers to Member States on the Guide on Human Rights for Internet Users), reaffirms the principle that citizens possess the inherent right to seek, receive, and disseminate information and ideas across various media platforms, transcending geographic boundaries. This enshrines the freedom for individuals to express themselves openly on the Internet and access information, viewpoints, and expressions of others. This encompasses a broad spectrum, including political discourse, religious beliefs, perspectives, and statements that may be perceived as favorable or innocuous, as well as those that could potentially elicit offense, shock, or disconcert. However, it is essential to acknowledge that certain limitations may be imposed on such expressions, particularly when they involve incitement to discrimination, hatred, or violence. These restrictions, when enacted, must adhere to principles of legality, purposefulness, and judicial oversight.

In 1996, the US Congress passed the Telecommunications Act, primarily aimed at preventing minors from accessing obscene online content. To achieve this objective, Section 230 of the Communications Decency Act was introduced. The pivotal aspect of Section 230 consists of a succinct 26-word provision: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” The genesis of Section 230 stems from legal actions taken against early Internet companies, predating the advent of social media. In one notable case, Prodigy Services found itself liable for content published on its website due to its content moderation efforts. In contrast, another case absolved CompuServe of liability as it pursued a policy of non-interference and was regarded as a distributor rather than a publisher of content.

It is noteworthy that the recent actions leading to the suspension of former President Trump’s social media accounts were made possible through the invocation of Section 230 of the Telecommunications Act, as modified by government intervention. This development underscores the complex interplay between legislative frameworks and digital rights within the evolving landscape of online communication. It can be concluded that due to the unsettled legislative mechanisms of social media activities at the international and national levels, situations of unprecedented interference in personal life and violation of the rights of Internet users arise. Digital oligarchy is a threat to states and democracies, therefore the regulation of digital giants among social media shall be carried out by consensus of the authorities, people, and justice.

Right to privacy on the Internet. In 2017, the French social media expert Frédéric Cavazza identified 6 large social media groups:

1. to make publications (blog platforms, wikis, sharing platforms, etc.);
2. to share videos, documents, data, photos, hobbies and music;
3. messengers (mobile, visual, and classic);
4. discussion platforms, commenting (feedback) and FAQ systems;
5. professional messengers and collaborative platforms;
6. professional social networks, dating services, and meeting services.

The daily use of various social media platforms underscores the pressing concern of online privacy, demanding heightened attention from society at large. The delineation
of the right to online privacy assumes significance due to its amalgamation of several fundamental rights and liberties, encompassing freedom of thought and expression, the unrestricted articulation of personal beliefs and perspectives, and the freedom to assemble and disseminate information. These rights find their roots in foundational documents such as the Universal Declaration of Human Rights, particularly Article 19, which unequivocally declares that “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” While the Universal Declaration was adopted in 1948, well in advance of the emergence of contemporary social networks, the recognition of the freedom to access and disseminate information, as enshrined within it, assumes pivotal importance within the context of modern globalization processes.

The main basis for understanding the right to privacy was formed in 1890 by American lawyers Samuel D. Warren II and Louis Brandeis in their law review article «The Right to Privacy», where they analyze the development of the concept of privacy, its origin from looking at a person from a different angle – from the side of his/her spiritual nature, feelings, and intellect. The authors reveal the meaning of the concept of the «right to privacy» as «the right to be left alone» and also emphasize that the spheres of private and family life are sacred. The modern understanding of the right to privacy in the online environment includes, in particular, the following components: protection of personal data (health data, location data, data related to bank accounts), personal photos, conversations, and correspondence, i.e., all those elements of human life that a person does not want to make known to the general public, but through the use Internet resources, he/she is forced to provide access to this information in some cases even to an unspecified circle of persons. The provision of such data exists outside the Internet, but with its help, access to information becomes easier and the speed of distribution is faster, thereby creating greater threats to the privacy of each of us.

In the resolution of the UN General Assembly «The Right to Privacy in the Digital Age» of 18 December 2013, deep concern was expressed about situations where the practice of using electronic surveillance and interception was discovered in countries around the world, which indicates the vulnerability of digital information and communications technology (ICT). Examples of overt and/or covert digital surveillance have increased in jurisdictions around the world, with government mass surveillance becoming a dangerous habit rather than an exception.

In light of the relentless progress of scientific and technological advancements, the legal framework surrounding the right to privacy has undergone significant development, encompassing both its broader implications and its specific relevance to online privacy. It is imperative to recognize that the latter should be integral to the overarching right to respect for private and family life, a principle deeply entrenched in international instruments such as Article 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms, as well as Article 12 of the Universal Declaration of Human Rights. The safeguarding of personal data, a crucial aspect of privacy, is subject to distinct legal provisions.

In this regard, Article 8 of the Charter of Fundamental Rights of the European Union stands as a notable safeguard, explicitly enshrining the right to the protection of personal data. This provision emphasizes the equitable processing of personal data for explicitly
defined purposes, contingent upon the consent of the individual concerned or other legitimate legal grounds. Furthermore, it confers upon every individual the entitlement to access data and the prerogative to request rectifications when necessary. The specialized legal instruments governing the exercise of these rights encompass the Convention on the Protection of Individuals concerning Automated Processing of Personal Data, established on 28 January 1981, and Regulation (EU) 2016/679 of the European Parliament and of the Council, promulgated on 27 April 2016. These instruments delineate fundamental principles and regulations governing the processing of personal data, reinforcing the paramount importance of privacy in the digital age.

At the national level, the right to online privacy is underpinned by the provisions enshrined in Article 31 of the Constitution of Ukraine. This constitutional article guarantees the confidentiality of various forms of communication, including correspondence, telephone conversations, telegraphic exchanges, and others. In parallel, Article 32 of the same constitution underscores the inviolability of personal and family life, save for circumstances prescribed by the Constitution of Ukraine. It explicitly proscribes the collection, storage, use, and dissemination of confidential information about individuals without their explicit consent. Additionally, Article 32 establishes the individual’s right to access and review information concerning themselves, coupled with the right to challenge inaccuracies and seek compensation for any harm incurred due to the collection, storage, use, or dissemination of such information. To further fortify these protective provisions, Article 3 of the Civil Code of Ukraine explicitly prohibits unwarranted intrusions into an individual’s personal life. Finally, the Law of Ukraine titled “On the Protection of Personal Data” establishes a comprehensive framework of requirements governing the collection, processing, storage, utilization, and distribution of personal data. This legislation meticulously outlines the rights of data subjects and prescribes procedures for accessing personal data, thereby reinforcing the fundamental significance of privacy rights in the digital era.

Personal information on the Internet spreads faster, it is easier to access it, and this information can be stored for an unlimited amount of time. This phenomenon is connected with the emergence of a new era of Web 3.0 and the development of artificial intelligence technologies. Even a simple exchange of letters online has its feature, which consists of the use of intermediaries between users who have access to the transmitted information. This access is not direct, but the risk of leakage of confidential information remains. Also, the content of the issue we are researching includes the concept of privacy of information activity, which consists of the fact that Internet users, when visiting websites, leave traces with their data, including information about the Internet address of the user’s computer; data about software, time visits to the web page, based on which a general idea is formed. The general idea about the user is based on a set of characteristics that cover his or her preferences, desires, habits, interests, motivations for using the Internet, etc. As the Court of Justice of the European Union rightly observed, communication metadata «in general may allow very precise conclusions to be drawn concerning the private life of the persons whose data have been retained». Recognition of this evolution has prompted initiatives to reform existing policies and practices to provide stronger privacy protections. Algorithms are configured in such a way that the Internet knows everything and offers users only what corresponds to the general perception of them through the eyes of the World Wide Web. It
is behind such methods of collecting information on the Internet that the right to privacy stands, which today is being eroded due to insufficient protective mechanisms both from the technological side and from the side of statutory regulation.

Specific personal data is information about a person’s location, i.e. geolocation as we all know. Providing this information to Internet resources opens up opportunities for using online maps, ordering various types of services, etc., however, its improper use can harm the provider, including illegal surveillance. It is also necessary to emphasize that the distribution of information about certain events, about individuals, was transformed with the emergence of the Internet in the direction of wider coverage of this information by various representatives of society, its faster dissemination, and a reduction in the possibility of deletion since anyone has the opportunity to save information on their devices.

The illustration of these examples proves that the use of the Internet significantly narrows the private space, which can lead to a loss of control over personal data. However, it can be argued that the legal regulations for the protection of the personal data of Internet users are constantly developing and are aimed at providing opportunities to use the technical benefits of the network without the threat of information leakage.

An examination of both international and national legal instruments reveals that the right to privacy is not absolute; rather, it is subject to constraints under exceptional circumstances. The legitimate limitation of the right to privacy on the Internet is permissible in the following scenarios:

1. when such limitations are imposed under the law.
2. when they pursue a legitimate objective, which includes safeguarding national and public security, promoting economic well-being, preventing upheaval or criminal activities, protecting public health or morals, or preserving the rights and freedoms of others.

When these limitations are proportionate to the stated objective, meaning that the ends must justify the means employed. Furthermore, it is essential to ensure that the right to privacy aligns harmoniously with the right to freedom of expression, as enshrined in Article 10 of the Convention on the Protection of Human Rights and Fundamental Freedoms, Article 19 of the Universal Declaration of Human Rights, and Article 19 of the International Covenant on Civil and Political Rights. This balance underscores the intricate interplay between these two fundamental rights within the context of legal frameworks. For the full exercise of this right in the digital age, anonymity is of considerable importance in the case when a person does not want to reveal his/her identity when making certain statements. However, unfortunately, quite often the possibility of anonymity leads to the violation of other rights of persons in respect of whom such statements are made, e.g., infringement of the people’s honor and dignity. The case of Delfi AS v. Estonia, in which the European Court of Human Rights (hereinafter referred to as the ECtHR) stated: «Despite the importance of the right to anonymity on the Internet, an appropriate balance must be struck between this right and other rights and interests ... Internet users have no interest in revealing their identity ... sometimes the unrestricted dissemination of information on the Internet has extremely negative consequences.» The circumstances of this case demonstrate that anonymity can often result in impunity for individuals who use hate speech and direct calls for violence. Thus, the idea of privacy on the Internet in no way aims to create an atmosphere of permissiveness and lack of responsibility for one’s statements.
The legality of disclosing personal information about a person on the Internet without his/her consent must be determined using certain criteria:

1. importance of information for society;
2. publicity of the person about whom the information was disseminated;
3. method of obtaining information and its reliability;
4. previous conduct of the person about whom the information was disseminated;
5. probable;
6. consequences of information dissemination for the person.

These criteria should be applied in their entirety. Thus, applying them to the case of Fuchsmann v. Germany, the ECtHR found that it would not be a violation of the right to privacy to publish on the website and in the print version of The New York Times an article about criminal offenses with which German businessman Fuchsmann may have been connected, as the Court prioritized the public’s right to know information that may be important about such a public figure. Moreover, the consequences of the inability of society to find out this information in an objective sense would be worse than the disclosure of this data to the individual.

In the contemporary landscape characterized by the utilization of advanced digital information and communication technologies, the rights to the inviolability of private life (as articulated in Article 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms) and freedom of expression (enshrined in Article 10 of the same Convention) are particularly susceptible to infringements. Violations of these rights, stemming from the operations of social media platforms, have emerged as a prominent focal point within the jurisprudence of the European Court of Human Rights (ECtHR). The role played by the ECtHR in shaping the legal framework concerning the fourth generation of human rights is of paramount significance. The doctrine of the “fourth instance” enables the differentiation of the ECtHR’s legal positions as independent and non-binding norms, wielding substantial influence in forging a unified jurisprudential practice.

Contemporary scholars contend that international and national judicial practices serve as the primary catalyst for the constitutionalization of digital rights in the realm of social media usage. National courts are tasked with adapting traditional constitutional principles to the context of social media, thereby resolving legislative conflicts between the constitutional dimension of the state and online platforms. Edoardo Celeste’s work titled “Digital Punishment: Social Media Exclusion and the Constitutionalizing Role of National Courts” delves into the examination of this issue. In this discourse, our analysis will focus on the ECtHR’s protection of the right to online privacy, primarily through the lens of violations of the right to access information, freedom of information, and anonymity.

A pivotal case exemplifying the ECtHR’s stance on this matter is Ahmet Yıldırım v. Turkey. In this case, the ECtHR concluded that blocking access to the Internet could “directly contradict the actual wording of part 1 of Article 10 of the Convention, according to which the rights outlined in this Article are ensured ‘regardless of frontiers’.” The essence of the case revolved around the applicant’s assertion that the state’s decision to block access to his Internet site constituted an unjustifiable interference with his rights guaranteed by Articles 6, 7, 10, and 13 of the Convention and Article 2 of Protocol No. 1. The Committee of Ministers’ declaration on human rights and the rule of law in the information society’s preamble acknowledges
that “limited access or lack of access to [information and communication technologies (ICT)]
can deprive individuals of the opportunity to fully realize fundamental rights.” The first
chapter of this declaration, titled “Human rights in the information society,” emphatically
underscores, “Freedom of expression, information, and communication should be respected
in a digital as well as in a non-digital environment.” This ECtHR decision establishes the
fundamental principle that “the right to access the Internet is, in theory, protected by
constitutional guarantees that exist in the field of freedom of speech and freedom to receive
opinions and information.” The French Constitutional Council has unequivocally affirmed
that contemporary freedom of speech encompasses the right to access the Internet.

Another significant case, Cengiz and Others v. Turkey holds particular importance in the
jurisprudential context of our inquiry. In this case, the ECtHR asserts that user-generated
communication on the Internet provides an unprecedented platform for the exercise of
freedom of expression. Furthermore, the case of Szabó and Vissy v. Hungary, centered on
Hungarian legislation about covert anti-terrorist surveillance, raises concerns regarding
the potential surveillance of individuals under the pretext of safeguarding public security.
The ECtHR underscored that the fight against contemporary manifestations of terrorism
naturally leads states to employ advanced information-gathering technologies, including
the mass monitoring of communication channels.

In summation, the relentless advancement of information and communication technologies
undeniably exposes us to increased violations of the right to privacy in the digital dimension.

CONCLUSIONS

The advent of Internet technologies has extended the purview of the right to privacy,
encompassing the online sphere. Nonetheless, the fundamental principles governing the
exercise of this right remain unaltered:

a) Entities entrusted with personal data must adhere to regulations governing its collection,
processing, storage, utilization, and dissemination.

b) Individuals should be shielded from unwarranted intrusion into their private online
activities, including correspondence, internet calls, search history, geolocation data, and
more. Exceptions to this rule may only occur when lawful intrusion is deemed necessary
within a democratic society to safeguard national and public security, economic prosperity,
crime prevention, public health, moral values, or the protection of the rights and freedoms
of others.

c) The utilization of anonymity by users may be restricted in cases where it promotes
hostility or encourages violent actions.

d) Striking a judicious balance between the right to online privacy and the individual’s
right to access socially pertinent information is imperative.

Hence, the matter of the right to online privacy is intricate and dynamic, contingent upon
the evolving societal landscape. Ongoing investigations into the right to online privacy aim
to refine legal frameworks in this domain and mitigate potential threats to individual privacy
arising from World Wide Web utilization.
REFERENCES


Scott, J. D. (2017). *Social Media and government surveillance: The case for better privacy protections for our newest public space.* Retrieved from https://digitalcommons.law.umd.edu/jbtl/vol12/iss2/2


