Vilnius University Faculty of Law

Department of Private Law

Rostyslav Prystai,

II study year, I group,

International and European Law Programme Student

Master's Thesis

Protection of Privacy and Personal Data in Social Networks

Privatumo ir Asmeninių Duomenų apsauga Socialiniuose Tinkluose

Supervisor: assoc. prof. dr. Rimantas Simaitis

Reviewer: LL.M. Kadys Eimantas

Vilnius

2023

ABSTRACT AND KEY WORDS

The work examines existing mechanisms and state of privacy and personal data protection in social networks within the framework of the European Union and other legislative systems. The concept of privacy and personal data as an object of the protection in social networks is analyzed. Modern risks and violations of privacy and personal data in social networks as a ground for privacy mechanisms protection review are clarified. European Court of Human Rights practice and the practice of national Data Protection Authorities in the context of the protection of personal data and privacy in social networks is outlined. An overview of existing privacy-enhancing technologies (PETs) and their applicability to privacy protection in Social Networks as well as Privacy by design concept as a basis for privacy protection in Social Networks is carried out.

Keywords: Privacy and Personal Data protection, online social networks, legal mechanisms, privacy-enhancing technologies, privacy by design.

TABLE OF CONTENTS

INTRODUCTION

Since 2016, within the framework of the European Union as well as other regional and national legal systems (the United States, China, South Korea, Brazil and others), the array of legal regulation of Personal Data protection has been rapidly extending. In 2016, the EU-U.S. Privacy Shield was adopted to replace Safe Harbor Principles (later invalidated in 2020 and changed by Trans-Atlantic Data Privacy Framework in 2022), GDPR went into effect in the EU and the European Economic Area (EEA) on May 25, 2018, California Consumer Privacy Act (CCPA) was adopted in 2020, The National People's Congress of the People's Republic of China passed the Personal Information Protection Law (PIPL) in 2021, Lei Geral de Proteção de Dados (LGPD) – Brazil's first law to provide comprehensive framework regulating the use and processing of all personal data, fully went into effect on August 1, 2021.

The new legislation aims to protect personal data in various sectors, industries and environments, in particular, in online social networks (OSNs). However, taking into account the latest economic, political, social, and other factors (such as increased access to the Internet, social interaction activity, mobile infrastructure improvement, the COVID-19 pandemic, mass media influence, etc.), the number of users of social networks is also expanding. As of 2023, the total number of users of social networks is 4.76 billion users. Along with this, the number of violations in social networks that relate to person's Privacy and personal data is also increasing. In the first quarter of 2023, more than six million data records were exposed worldwide through data breaches. From the first quarter of 2020, the largest number of open data records was discovered in the fourth quarter of 2020, with almost 125 million data sets. 41% of all compromised records in 2021-2023 originated from social networks data leaks. Statistics shows that the presence of complex legal and technical mechanisms for the protection of personal data in social networks is not able to adequately reduce or prevent the number of such violations, because in addition to the development of methods and means of such violations, the very specificity of social networks remains unchanged - namely, the dissemination of information and personal data of users and between them. Thus, the question arises about the need and implementation of new legislative and technical means of protecting personal data and privacy in social networks, which in turn requires to study and analyze the object of the protection, current mechanisms of such protection and possible ways of their developing.

The aim of the research is to to study and analyze current legal mechanisms of privacy and personal data protection as well as appearing Privacy Enhancing Technologies in the legal context. To achieve the goal of the research, the following tasks (questions) must be solved:

- clarification of the legal nature of the object of legal protection, namely the concept of privacy and personal data through the prism of the specifics of social networks – what should the legislator protect in OSNs;
- analysis of risks and violations in the field of privacy and personal data protection in social networks, their legal and technical specifics;
- analysis of approaches to legal regulation of privacy and personal data protection within various legal systems;
- analysis of the regulatory and organizational mechanism for the protection of personal data and privacy in the EU on the supranational and national levels, EU approach is separately outlined;
- analysis of the regulatory and organizational mechanism for the protection of personal data and privacy in separate legal systems; US, Canada, China and others experience to compare sectoral and unification approach;
- analysis of legal mechanisms for the protection of personal data arising from social media platform policies, terms of service, and privacy agreements, their roles, how do they intersect and which additional guarantees they give to the user;
- analysis of ECHR and National Data Protection Authorities practice in the sphere of privacy and personal data protection in Social Networks - examples of internal and constructed privacy and personal data violations;
- overview of existing privacy-enhancing technologies (PETs) and the development of the privacy by design concept as a basis for privacy and personal data protection in Social Networks.

Due to the specifics of the study, we can outline two main objects of the study: legal mechanisms of privacy and personal data protection in various legislative systems; privacy and personal data as an object of the protection in social networks. In order to adhere to the logical presentation of the material, the legal nature of privacy and personal data in the context of their protection in social networks will be firstly outlined.

The research methodology is built on the principles of systematicity, objectivity, using the main general logical methods of legal research: analysis, synthesis and analogy. The methodology is based on a systematic and comparative legal method, which is reflected in the study and comparison of mechanisms for protecting privacy and personal data in various legal systems in social networks, in our case in the European Union, the USA, Canada, etc. As a result of the study, it is planned to establish the qualitative state of the specified legal systems as a whole, as well as their legal institutions, which are the basis of the administrative mechanism for the protection of privacy and personal data in social networks. For more complete and comprehensive study of the object of legal protection in the specified legal relationship, it is also necessary to apply the method of analysis in combination with historical-legal, sociological and logical-legal research methods, which will allow to qualitatively interpret the concepts of privacy and personal in the context of social networks and outline the most critically important interests of subjects whose rights are subject to protection.

The scientific novelty of the expected results lies in the fact that the study can become one of the recent researches on the mechanisms for the protection of privacy and personal data specifically in social networks. The study is one of the only few studies, that separately outline the concept of privacy linked particularly to the technical peculiarities of OSNs. The novelty of the research also lies in the identification of differences between the relevant mechanisms within the EU and other legislative systems. Overview of user held data model in OSNs also is relevant in the context of it`s practical implementation besides the sphere of wearable devices.

The added value of the research. The results of the performed research can be used:

- in further studies of privacy and personal data protection mechanisms in the European Union and other legislative systems;
- in the process of improving the legislation in the field of personal data protection, improving the efficiency and quality of the process of implementing the new norms into Personal Data protection legislation specifically oriented on the context social networks security;
- in the educational process, during the preparation of educational materials on International and European Law.

Sources of the research. The main materials used in the research are the EU legislation in the field of personal data protection, the legislation of the United States in the field of personal data protection, the relevant legislation of Canada, Brazil, China and South Korea. The legislation of the EU member states, the judicial practice of the ECHR, international recommendations and acts of soft law, documents of non-governmental organizations regarding the protection of privacy and personal Data were also used. Research conducted within the framework of OECD, IAPP, social networks policies, terms of service, and privacy agreements was used in the study. Separately scientific literature weas analyzed, namely researches performed by: Jurcys P., Compagnucci M.C., Fenwick M., Dixon S.J., Cooley, T. A., Beriorrs S., Hatt D., Choi Young B., Velten C., Arif R., Moehring D., Koerner K., Lalonde B., Chahar, H., Keshavamurthy, B.N., Khalid U., Barhamgi M., Perera C., Khader M., Karam M., De Montjoye, Y.A.; Shmueli, E.; Wang, S.S.; Pentland, A.S., and other written or electronic resources.

Protection of Privacy and Personal Data in Social Networks

PART I. Definition of Privacy and Personal Data as an object of the protection Social Networks

1.1. Chapter I. The concept of Privacy in the context of Social Networks

Social networks today are used both in private and public spheres, and the social network market has about five billion users worldwide[1]. In the process of using social networks, personal data is published, forwarded, stored and used in a variety of ways. These activities are called "Data processing". Social networks, due to their specifics, have many functions and technical features that can affect a person's Privacy in different ways. The object of this study is the protection of privacy and personal data, which are highlighted as separate categories. Since privacy in social networks includes not only the personal data protection, but also other structural components, we consider it necessary to separately investigate its concept and features.

The essence of privacy is reflected in various concepts, but the most common are the understandings of privacy as the inviolability of a person's private life, non-interference in the personal sphere, control over personal data, selective disclosure of information, autonomy in the private sphere, defined limitation of communication, the ability to share information with a self-selected circle of sub objects, right to be let alone[2] and desire to freely choose the circumstances and the degree to which individuals will expose their attitudes and behaviors to others. There are many terms used to denote this concept, including "privacy", "confidentiality", "secret of personal life", "inviolability of private life", "private sphere". There is no unity in the presentation of the content of privacy in the international and national legal acts, although the Right to Privacy is established and guaranteed as one of the fundamental human rights. In particular, variations of this right with a focus on non-interference, protection and withdrawals are found in the Universal Declaration of Human Rights[3], the International Covenant on Civil and Political Rights[4],

[1] DIXON S.J.. Social media – Statistics & Facts. Published August 31, 2003, from https://www.statista.com/topics/1164/social-networks/

[2] COOLEY, T. A Treatise on the Law of Torts or the Wrongs which arise independent of contract. Chicago: Callaghan, 1888.

[3] Universal Declaration of Human Rights. Adopted and proclaimed by UN General Assembly Resolution 217 A (III) of 10 December 1948 Text: UN Document A/810, p. 71 (1948). See Art.12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[4] International Convenant on Civil and Political Rights (1967). [1976] UNTSer 141;999 UNTS 171.

European Convention on Human Rights[5], the US Constitution[6], General Data Protection Regulation[7] and other documents.

The abovementioned normative acts reveal the general notion of privacy. But the privacy in social networks has it`s own specifics. Thus, in order to define privacy in social networks we should understand, who are the stakeholders when talking about such a privacy – both in the context of security and a breach, which users` rights (interests) are to be protected and how do social networks interact with Data in genereal.

Stakeholders. The main stakeholders in the relationship of privacy protection in social networks are: users of social networks, developers or service providers of social networks and the state. It is worth noting that such an interest can be manifested both in complete protection of privacy and in the opposite. Social networks are a convenient platform for a fraud, phishing, blackmail, etc. In addition, some particular states themselves may be interested in the possibility of having access to the personal data of its citizens and other users, for example, during the investigation of crimes in the order of secret investigation actions or for its own personal purpose (intelligence, defense, economic, etc.[8]).

Data in social networks – types and interaction. Social networks can include different types of platforms. Typical types of social networks are: social networks of a general profile (creating a profile, exchanging messages, publishing content), these include Facebook, Twitter, Whatsapp, Telegram, LinkedIn; photo and video communities (visual social networks - uploading and viewing images, likes and comments), for example, Instagram, Tik Tok or YouTube; Professional social networks (communication with colleagues, job search, information exchange), LinkedIn, Xing, Forums (discussion of specific topics), Reddit, Quora[9][10]. The division into these groups is extremely conditional,

[5] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 3 November 2023]. See Art.8 of the European Convention on Human Rights.

[6] The United States Constitution (1787), 1th, 3th, 4th, 5th, 9th Amendment, from https://constitution.congress.gov/constitution/amendment-4/.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[8] BULAVKO A.. Technical Review of End-to-End Encryption in Mobile Social Networks. Published 2018/01/05, from https://arturasbulavko.com/documents/E2EE_In_MSN.pdf.

[9] Affiliate Marketing, Social Networks Definition: What are They and Why are They Important?. Published 13 April, 2023, from https://www.linkedin.com/pulse/social-networks-definition-what-why-important-affiliate-marketing.

[10] WONG L.. 9 Types of Social Media and How Each Can Benefit Your Business. Published September 2, 2021, from https://blog.hootsuite.com/types-of-social-media/.

since there are now many other networks that can actually have the characteristics of several groups, or their own individual ones.

Despite the same or similar categories of data with which these networks deal with, their peculiarity lies precisely in the functionality and technical component of each network. Social networks can process personal data in different ways, filter received information, interact with users. For example, general social networks have advanced functionality that includes the ability to add friends, exchange messages, create groups and events. Privacy can be managed by setting profile visibility, allowing friend requests and restricting access to posts. At the same time, visual networks focus on content such as photos and videos. Users can manage the privacy of their posts by setting limits on their visibility or choosing the audience with whom they want to share their content, collect and process data on views, interactions and preferences of users to personalize recommended content.

Taking into account abovementioned pecularities of interaction between social networks and personal data used, there are three main types of privacy, which are an object of the protection in social networks: territorial, communications and information privacy.

Territorial privacy places limits on intrusions to specific physical or virtual environments, not limited to personal ones. They can include environments outside the home, such as places of employment, or even public spaces. In addition to territorial intrusions, such as in a home or other private space, this aspect of privacy can involve closed-circuit cameras and other video monitoring, ID checks, geolocation tracking and other surveillance techniques, which may be also techncically applied in OSNs.

Communications privacy is concerned with all methods of communication, such as the telephone, social networks, email and the postal system[11]. It is focused on keeping communications private, whether a verbal confession to a priest or a handwritten letter to a friend. In the context of social networks it means the the impossibility for somebody to enter or read users chats.

Information privacy is primarily concerned with rules that govern collecting and handling personal data, which is the focus of most modern privacy laws. While information privacy is technology-neutral, rules in certain laws may apply to different technologies. Some data protection laws focus on challenges protecting and managing specific sectors of the economy, such as medicine or finance. Other laws set a baseline of data protection for

[11] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. From https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

all personal data and provide special protections for certain categories of sensitive data – for example data used in social networks – given and retaining within registration, metadata and any other aggregated data.

Looking ahead, after revealing the examples and specifics of violations of privacy in social networks, we can also highlight at least several elements of the right to privacy in social networks, taking into account the specifics. These interests are derivative from the following parts but are essential to be used now when difining Privacy in social networks.

- the protection of personal data and information shared by individuals on social networks;
- the right to control and manage the visibility and accessibility of their personal information on social media platforms;
- appropriate technical and organizational measures to ensure the security and confidentiality of users' personal data;
- the right to give informed consent regarding the collection, processing, and disclosure of their personal information on social networks;
- comprehensive privacy policies, outlining the types of personal data collected and the purposes for which they are processed;
- the right to access their personal data held by social networks and the right to rectify any inaccuracies or errors;
- the right to take appropriate measures to prevent access to harmful content
- the right to file complaints and seek remedies if their privacy rights are violated by social networks;
- the right to be free from harassment, cyberbullying, and online abuse on social networks, with platforms taking proactive measures to prevent and address such issues etc.

Thus, privacy in social networks as an object for the protection should be characterized as a *state of inviolability of a person's private life in social networks, where both a person's interests arising from the concept of the right to privacy and social networks benefits can be freely satisfied*. When creating conditions under which there is no possibility to protect your private life, social networks will continue to exist, however, privacy can then be forgotten. If the provision of social network services is regulated too much, privacy will be fully protected, but the advantages that social networks are capable of bringing would be leveled. Therefore, there must be a proper balance that allows both to receive the benefits of the networks themselves, while at the same time ensuring the conditions under which the right to privacy cannot be violated, or to take some and effective means to eliminate the violation.

However, Pamela J. Wisniewski and Xinru Page in the article “Privacy Theories and Frameworks” outline different models of Privacy. In particular, it is stated, that the increasingly blurry distinction between public and private spheres further complicates privacy management, with platforms only now beginning to consider solutions to make privacy and disclosure easier to manage[12]. It will only become more important to understand users’ mental models of privacy, which shape individual and group behavior around privacy in unexpected and often underappreciated ways. User mental models that understand privacy as control[13], privacy as contextual integrity[14], privacy as an emotional variable, privacy as a commodity[15], or privacy as a universal right are just a few possible ways of evaluating privacy needs and explaining concerns and behaviors. Drawing on these privacy conceptualizations can guide researchers, designers, and policymakers even as technologies continually change and social norms evolve. The proposed definition of Privacy in social networks includes mentioned user mental models with the only exception of understanding it as a commodity, as we are talking about Privacy in social networks from the user directed approach.

[12] P. J. Wisniewski and X. Page, Privacy Theory and Methods. Published June 29, 2021. From https://doi.org/10.1007/978- 3- 030- 82786- 1.

[13] Coursaris, Constantinos, Wietske Van Osch, Jieun Sung, and Younghwa Yun. 2013. Disentan- gling Twitter’s adoption and use (dis)continuance: A theoretical and empirical amalgamation of uses and gratifications and diffusion of innovations. *AIS Transactions on Human-Computer Interaction* 5 (1): 57–83.

[14] Burke, Moira, and Robert E. Kraut. 2016. The relationship between Facebook use and well-being depends on communication type and tie strength. *Journal of Computer-Mediated Communication* 21 (4): 265–281.

[15] Burke, Moira, Robert Kraut, and Cameron Marlow. 2011. Social capital on Facebook: Differentiating uses and users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 571–580.

1.2. Chapter II. The security of Personal Data in Social Networks as the Right to Privacy component

After the analyzis of privacy and the main elements of right to privacy in social networks, we can come to the conclusion that its main part is the protection of personal data. In order to clarify the categories of data used in social networks (object of the protection), it is necessary to outline the concept of personal data in general.

As in the situation with the notion of privacy, regulatory acts have different interpretations of the concept of personal data. The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and European Convention on Human Rights provide only a general definition of the right to privacy. The definition of personal data is formulated on the national or regional regulatory levels. Special legislation that defines the concept of personal data is the General Data Protection Regulation, California Consumer Privacy Act[16], Personal Information Protection and Electronic Documents Act[17], Data Protection Act 2018[18] and others.

Thus, Article 4 of the General Data Protection Regulation defines the concept of personal data, namely as “any information relating to an identified or identifiable natural person (‘data subject’)”. At the same time, the California Consumer Privacy Act (CCPA) uses the term “personal information”. According to CCPA 1798.140(o)(1-2), personal information is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Another regulatory act that contains its own definition of the concept of personal data is the Personal Information Protection and Electronic Documents Act (PIPEDA). The term "personal information" is also used here. According to the provisions of Part 1, 2(1), personal information means information about an identifiable individual. This includes any factual or subjective information, recorded or not, about an identifiable individual. Another example of a definition of personal data is the definition proposed by the Data Protection Act 2018. Here under personal data according to clause 3 should be uploaded any information relating to an identified or identifiable living person, in fact taking into account the provisions of the GDPR as it is directly used in the data protection itself to act. Finally, the very interesting definition of personal data is entioned

[16] California Consumer Privacy Act (CCPA) (2018), from https://oag.ca.gov/privacy/ccpa.

[17] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), from https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.

[18] Data Protection Act (2018), from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

in the OMB Circular №.A-130, where under the term Personally Identifiable Information (PII) we should understand information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual[19].

The above-mentioned normative acts contain approximately the same and rather broad interpretation of the concept of personal data. This is done in order to ensure proper regulatory coverage of the most diverse data that can be used in one or another area that falls under their protection. They have three main functions: to protect, control and manage the use of Personal Data. According to this, it can be concluded that any information about a natural person, which is used in/by social networks and with the help of which such a person can be identified, is protected by the relevant acts. In the context of social networks, as we noted above, this data may include: name, username, email address, phone number, date of birth, gender, profile picture, location data, educational information, employment history, interests and hobbies, relationship status, family connections, messages, chats, search history, IP address and device information, account activity information, payment information, app usage data, cookies and other data.

Regarding specific types of personal data that are used in social networks, we may outline the next categories:

1) Registration data (which was actively or passively provided during the registration process – let`s call this data "input data 1");

2) Input data: all the data that individuals are manually adding to social networks (photo, photo caption, chats, comments – "input data 2");

3) The metadata: for example, GPS data, which is attached to the photo, detils about the camera, resolution etc.;

4) Observed and observable data: data, which is neither created by OSN nor by the user (the number of likes, that photo received, photo background);

5) Derived data: preferences, behaviours patterns, some insights about the individual. All this data has it`s own specific legal regime of ownership depending on user agreement and Privacy Policies.

All categories of personal data mentioned above are the subject to protection. The activity of private and public entities aimed at their protection is called data protection. In

[19] CIRCULAR NO. A-130, Revised, (Transmittal Memorandum No. 4) (November 28, 2000), from https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130trans4.pdf.

the context of social networks this means technical and legal mechanisms[20] of protecting personal data aimed on ensuring privacy[21].

Right to Privacy and data protection are often used interchangeably, but they are slightly different concepts. Right to privacy is the right of an individual to be treated a certain way – to be let alone – as well as to have rights with respect to information. Data protection, in turn, includes how information is managed and protected (secured) as well as the privacy rights. Thus, data protection laws will often include additional management and organizational requirements, such as privacy officers, reporting and oversight that are not part of how privacy laws focusing strictly on the information are structured. Data protection laws and regulations addressing privacy and security-related issues are common in the EU and other jurisdictions.

For example, article 5[22] of the General Data Protection Regulation (GDPR) sets out key principles which lie at the heart of the general data protection regime. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation:

1) Lawfulness, fairness, and transparency: Any processing of personal data in social networks should be lawful and fair. It should be transparent to the users that personal data concerning them is collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. For this, clear and accurate Privacy policy and user agreement shold be provided;

2) Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data – which means that it should be collected due to the main functions and purposes of the particular social network;

3) Data Minimisation: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes of social network. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means;

[20] Cambridge Dictionary, from https://dictionary.cambridge.org/dictionary/english/data-protection.

[21] See Chaper I.I.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

4) Accuracy: Controllers must ensure that personal data is accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Failing to comply with such provisions may also violate minimization principle, as if data is no valuable anymore, it cannot be stored on the OSN server without any legitimate reason;

5) Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. For example, this issue is strongly connected to dating apps (social networks), which may store the data up to one year after deleting an account (which does not have any legal ground);

6) Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7) Accountability: the controller is responsible for, and must be able to demonstrate his compliance with all of the Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance.

The inviolability of these categories of data (registration data, input data, the metadata, observed and observable data, derived data), as well as the processing of this data only on the basis and within the limits provided by law (Lawfulness, fairness, and transparency, purpose limitation, data minimisation etc.), is a key right of all users of social networks. This involves, in particular, internal and external audit.

If the concept of privacy is general and acts rather as inviolability of private life (a state and a result at the same time), then the protection of personal data acts as a tool to achieve the state of data security (but not only), which serves as a basis for building privacy (Personal Data protection – Information and Data security – Privacy).

PART II. Privacy and Personal Data concerns in Social Networks

2.1. Chapter I. Analysis of Privacy and Personal Data risks and vulnerabilities in Social Networks

Privacy and personal data security, in particular in the field of social networks, is characterized by the reduction of risks of personal data violation, as well as the elimination of technical or legal weaknesses in the context of mechanisms for the protection of personal data in social networks. Conducting research on the nature of personal risks, and weaknesses in the realm of personal data protection within social networks is crucial for defining the scope of protection and establishing the clear objectives that legislators, developers, and social network users should strive to achieve.

Risks that may affect privacy and are related to a person's personal data in social networks should be understood as potential dangers and violations of privacy that may occur when using social networks. It should be noted that the concept of "risks" or violations in the field of privacy in social networks is connected to the concept of information security (confidentiality, integrity and inviolability[23]).

The relationship between data protection and information security is often complicated, but the two functions are mutually supportive. Information security typically resides within the information technology (IT) department and, as such, uses defined measures and controls, such as in a project plan or security plan. Information security is a discipline focused on protecting information assets within an organization, personal or otherwise – in our case in social networks. Some of the most significant risks to privacy and a strong data protection are related to information security. In the context of social networks these include identity theft, social engineering[24], improper access controls and weak authentication. It is important to note that this is only a part of the privacy risks that may arise in social networks. The specificity of the mentioned risks is determined by the types of privacy violations that can be committed by different subjects, related to different objects, and with different degrees of public danger.

[23] HATT D., CHOI YOUNG B., Role of Security in Social Networking, February 2016, International Journal of Advanced Computer Science and Applications 7(2), DOI:10.14569/IJACSA.2016.070202
from https://www.researchgate.net/publication/297591795_Role_of_Security_in_Social_Networking

[24] VELTEN C., ARIF R., MOEHRING D., Managing Disclosure through Social Media: How Snapchat is Shaking Boundaries of Privacy Perceptions, Vol. 6, No.1(2017): The Journal of Social Media in Society, from https://thejsms.org/index.php/JSMS/article/view/214

Identity theft. Insiders and other parties commonly use stolen personal data for identity theft. As the name suggests, identity theft involves using another person's personal data to assume or manufacture an identity. Third parties can use identity theft to illicitly obtain financial or other benefits, evade the authorities, steal government benefits or further perpetrate fraud in another person's name[25].

Social engineering. Social engineering is a common threat that victimizes trusting persons to access their personal data. It uses common communication techniques, such as email, chats, and manipulating the victim into unintentionally sharing information or executing actions without their direct and conscious will. One of the most common methods is phishing, unfair commercial practices, political markering etc.

Access and authentification issues. Data protection and information security professionals often closely collaborate on selecting proper access controls. An organization's access control environment needs to align with internal policies, legal and contractual considerations, and risk appetite policies. Often, such policies or the very practice of social network services are of poor quality and can cause harm to the user or create the possibility of causing such harm, which consists of the consequences indicated in this and other sections. The creation of such conditions should be interpreted as a separate type of risk and violation of a person's personal data. *These threats can be divided into three categories: security incident[26], privacy incident[27] and data breach.*

A security incident is the loss of information security that compromises the confidentiality, integrity or availability of data. A privacy incident is a violation of privacy policy or law that could result in privacy harms, such as lack of or inaccurate privacy notice, improper consent or uses of data beyond the purposes for which it was collected. A data breach is the improper disclosure and unauthorized access or acquisition of personal data. Depending on legal requirements, an organization may need to notify proper authorities and, often, the affected data subjects.

In the comprehensive review of security threats and solutions for the online social networks industry, conducted by Naeem A. Nawaz, Kashif Ishaq, Uzma Farooq, Amna Khalil, Saim Rasheed, Adnan Abid and Fadhilah Rosdi, five categories of specifically Data

[25] BERRIORS S., Social Media and Privacy, Modern Socio-Technical Perspectives on Privacy, 2022, from https://www.academia.edu/76360943/Social_Media_and_Privacy

[26] RISKOPTICS, 9 Common Types of Security Incidents and How to Handle Them. From https://reciprocity.com/blog/common-types-of-security-incidents-and-how-to-handle-them/

[27] SOVEREN, What is a privacy incident? Mar 2, 2022, from https://soveren.io/blog/what-is-privacy-incident

breach threats are distinguished: classical threats, modern threats, insider threats, multimedia threats, and targeting children[28].

Classic threats are understood to be those that have been a problem for users since the very beginning of the Internet and with the help of which criminals collect and use a person's personal information. These include malware, phishing attacks, spam, cross-site scripting (XSS) and many other threats that are the main problems of social network users.

Regarding modern threats related to personal data in social networks. They are conditionally new threats that obtain confidential user information. This includes clickjacking, de-anonymization attacks, sybil attack or fake profile, identity clone attacks, inference attacks, information leakage, location leakage, etc.

Insider threats. This category of threats in social networks should be understood as those cases when the identity of the attacker is known to the network user. It can be any close person of the user or a person who works in the organization and may know the login, password or other data necessary for authorization and access to information.

Multimedia threats in OSN. This category of threats has emerged due to the development of opportunities to exchange or display multimedia content in high resolution. Such content may include location information through geotagging, facial recognition and home address, etc. Related multimedia threats include: multimedia disclosure, shared ownership, steganography, metadata, static links, data center outsourcing and transparency, video conferencing, tagging of shared multimedia, and unauthorized data disclosure.

The final category identified by the review above is threats targeting children. Authors include harmful or offensive content, scams and fake friends entering the chat. Here it is worth noting that the mentioned examples are typical not only for children's, but are the most common in this audience.

Regarding vulnerabilities that can potentially have a negative effect on the protection of personal data in social networks. They should be understood as the weaknesses of the existing system of personal data protection and privacy in social networks, as well as the very specificity of social networks as a phenomenon. They can be conditionally divided into two general categories: technical and legal.

The technical weaknesses or the specific features of the protection of personal data in social networks include: the accumulation of a large amount of information about a

[28] Naeem A. Nawaz, Kashif Ishaq, Uzma Farooq, Amna Khalil, Saim Rasheed, Adnan Abid, and Fadhilah Rosdi, A comprehensive review of security threats and solutions for the online social networks industry, 16 January 2023, from https://peerj.com/articles/cs-1143.pdf

person in one place; insecure Application Programming Interfaces, weak passwords, insufficient encryption, etc. This also includes downgraded server versions and hypertext transfer protocol (HTTP), open FTP servers (File Transfer Protocol)[29]. Legal ones include inadequate or unclear privacy policies, collecting more personal data than necessary, international data transfers, etc. typical legal omissions that are not directly a violation of the law, but create opportunities for violating personal data or a person's privacy in social networks.

[29] Tabassum Tamboli, Aditya Shende, Archana Varade. Impacts of Vulnerabilities on Security and Confidentiality in Online Social Networks along with Preventive Measures. Special Issue - 2020 International Journal of Engineering Research & Technology (IJERT). From https://www.ijert.org/research/impacts-of-vulnerabilities-on-security-and-confidentiality-in-online-social-networks-along-with-preventive-measures-IJERTCONV8IS05038.pdf

2.2. Chapter II. Overview of Privacy incidents and Personal Data breaches in Social Networks

The basis for researching the mechanisms for protecting privacy and personal data in social networks is the identification of types and examples of privacy incidents and violations. In the previous section, we examined what are the typical types and classifications of threats in the field of personal data protection and privacy in social networks. This section is devoted to specific examples of relevant cases that put the question of necessity of the revision of the existing system and approaches to data protection in social networks.

The first example which will be further provided is an example of both security and privacy incident. It should also be treated as data breach in the context of Stop Hacks and Improve Electronic Data Security Act (SHIELD Act[30]).

On May 7, 2020, Zoom Video Communications, Inc. (Zoom) became the first company to experience one of the new enforcement tools available to the New York Attorney General's Office (NYAG) under the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)[31]. Zoom received media scrutiny, a Federal Trade Commission (FTC) inquiry, a New York Attorney General (NYAG) investigation and faced a series of class action lawsuits over its security practices. The main concern was the company's alleged failure to use strong encryption (despite representing otherwise) and the security of stored meeting recordings[32].

The Federal Trade Commission argued that: 1) Zoom did not use end-to-end encryption, even though Zoom said it did; 2) Zoom did not immediately encrypt recordings made to the cloud, even though Zoom said it did, and 3) Zoom installed software that let users bypass browser safeguards intended to protect against malware[33]. As previously

[30] SHIELD Act, July 25, 2019, from https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

[31] DULLEA A., BEEBE M., Zoom's Popularity Leads to New York Investigating Its Security Flaws, May 18, 2020, Byte Back – Husch Blackwell`s Data Privacy and Cybersecurity Legal Resource, from https://www.bytebacklaw.com/2020/05/zooms-popularity-leads-to-new-york-investigating-its-security-flaws/

[32] Letter Agreement between Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020), https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf; Complaint at 3-7, *In the Matter of Zoom Video Communications, Inc.*, Docket No. C-4731 (Federal Trade Commission) and *In Re: Zoom Video Communications, Inc. Privacy Litigation.*, Case No. 5:20-CV-02155-LHK (D. Cal. Oct. 21, 2021) (order granting preliminary approval of class action settlement)

[33] Letter Agreement between Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020), https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf; Complaint at 3-7, In the Matter of Zoom Video Communications, Inc., Docket No. C-4731 (Federal Trade Commission) and In Re: Zoom Video Communications, Inc. Privacy Litigation., Case No. 5:20-CV-02155-LHK (D. Cal. Oct. 21, 2021) (order granting preliminary approval of class action settlement)

mentioned above, such actions could be interpreted as security - , and – privacy incidents, because information and data availability as well as confidentiality was not enough secured.

In the class complaint, Zoom users argued that Zoom disclosed passively collected device information to "Facebook and possibly other third parties" without sufficient disclosures to data subjects in violation of unfair and deceptive trade practice laws[34]. The complaint also alleged that Zoom did not do enough to stop "Zoom-bombing," in which an unauthorized individual accesses a Zoom meeting.

Finally, in its settlement with the FTC, Zoom agreed to improve its information security program, including annually assessing its risk factors, having a "vulnerability management program," and using safeguards like multi-factor authentication[35]. Zoom made similar promises to the NYAG. In the class action, Zoom agreed to: pay $85 million to users, modify its setting to alert hosts when new people join meetings, and train its own employees about data security[36].

The next case shows a power impact, that some personal data may have in the context of Big Data and unfair information practices. In 2018, the Office of the Privacy Commissioner of Canada (OPC) commenced an investigation into Facebook following revelations about Facebook's disclosure of certain users' personal data to a third-party application (the "TYDL App"). The data was later used by third parties, including Cambridge Analytica, for targeted political messaging.

Following its investigation, the OPC found that Facebook:

1) failed to obtain valid and meaningful consent from users installing the app for their information to be processed and disclosed to third parties, and did not make reasonable efforts to ensure that the third-party app was obtaining meaningful consent from users;

2) failed to obtain meaningful consent from friends of users installing the app, even though the friends would have had no knowledge that their information had been disclosed to the third-party app or additional third parties;

3) had inadequate safeguards to protect user information and ineffective monitoring to ensure compliance; and

[34] Complaint at 6, Cullen et al v. Zoom Video Communications, Inc., Case No. 5:20-cv-02155-SVK (D. Cal. Mar. 30, 2020).

[35] Consent Order at 3-7, In the Matter of Zoom Video Communications, Inc., Docket No. C-4731 (Federal Trade Commission); Letter Agreement between Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020)

[36] In Re: Zoom Video Communications, Inc. Privacy Litigation., Case No. 5:20-CV-02155-LHK (D. Cal. Oct. 21, 2021) (order granting preliminary approval of class action settlement)

4) failed to be accountable for the users' information under its control and did not take responsibility for giving real and meaningful effect to protecting their privacy[37].

The investigation followed a complaint that a UK consulting firm, Cambridge Analytica, was able to access millions of Facebook users' private data without their consent for use in psychographic modelling for political purposes. Facebook disputed the investigation's findings and did not agree to implement the OPC's recommendations.

In February 2020, the OPC filed an application with the Federal Court seeking an order requiring Facebook to correct its privacy practices in accordance with Canada's federal private sector privacy law (PIPEDA)[38]. Facebook brought a separate application seeking judicial review of the OPC's investigation and decision. On April 13, 2023, the Federal Court dismissed both applications[39].

For organizations, the case highlights the importance of ensuring a strict process for gaining valid consent from customers, having safeguards in place for verifying third-party compliance and having an accountability process in place to implement policies and practices.

The two cases mentioned above are examples with the participation of consumers and companies that violated their rights. However, there is another negative trend-vilation, which has a consequence in the direct person`s Privacy and Personal Data violation in social networks. It has a very different nature, which is also directly connected to social manipulation issue and social networks are commonly used as a tool for it`s execution.

Preconditions. Social networks have already become common sources of information for journalists. A study conducted in 2019 proved that all-Ukrainian online media took every fifth of their news from social networks. This not only includes the Office of the President, the Cabinet of Ministers of Ukraine and other official departments in social networks, but also the accounts of officials of various ranks, politicians, public figures and others. With the growth in 2020 and 2021 of the number of Ukrainian Internet users and

[37] Office of the Privacy Commissioner of Canada, Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, April 25, 2019, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206.

[38] DAVID YOUNG LAW, Privacy Commissionerseeks court order against Facebook, 2018, from https://davidyounglaw.ca/compliance-bulletins/privacy-commissioner-seeks-court-order-against-facebook/. A version of this article was originally published by The Lawyer's Daily (www.thelawyersdaily.ca), part of LexisNexis Canada Inc.

[39] Office of the Privacy Commissioner of Canada, Privacy Commissioner appeals Federal Court decision related to Facebook investigation, May 12, 2023. From https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230512-2/

the audience of social networks, information from Facebook or Instagram is used more and more widely[40].

More than 76% of Ukrainians use social networks to get news (according to a study conducted by KMIS on behalf of the Opora network from May 3 to 26, 2022, during which 2,009 respondents were interviewed (statistical sampling error does not exceed 2.4%)[41]. A vivid example of 2022-2023 is Telegram channels. The number of subscribers of channels in Telegram is increasing even now, although not at such a pace, but steadily. Currently, from almost 1 million to more than 2 million users are subscribed to the top ten news Telegram channels of Ukraine. However, posts are regularly viewed by no more than 45% of subscribers. But even taking into account this fact, it can be said that Telegram news channels are catching up with traditional media sites in terms of the number of views. By their legal nature, such channels cannot be equated with mass media, and therefore they are private channels, - with a larger audience than traditional mass media.

Regarding the violation of privacy. Every day, these channels publish many posts in the form of news, which contain information about politicians, civil servants, the military, as well as private individuals. Such news: 1) contain textual information that is not only neutral, but also biased, inaccurate, often manipulative in nature; 2) contain photos and other forms of reproduction of the image of the participants of such events. These photos and videos of private individuals without the consent of the individuals are published every day in the relevant Telegram channels (“Ukraine сейчас”, Новости, война, Россия”; “Украина Online”; “Insider UA”, “Агент України” etc.) and the photo of every natural person on the territory of Ukraine can be posted without consent to millions of audiences if such information is interesting for readers (or such is the inner will of the owner of the Telegram channel).

Despite a wide audience, Telegram channels, even if they have conditionally news content, are not formally mass media, just as their contributors are not journalists. Therefore, they can disregard news quality standards, not follow journalistic ethics, and not pay attention to the legislation outlining media activity without any consequences.

The fact remains that in the last two years of operation of these channels, no criminal or administrative case was actually initiated against the owners of the relevant

[40] VOIUTA D., Photos From Social Networks In The Media: Where Is The Privacy Line? December 10, 2021, Centre of Democracy and Rule of Law, from https://cedem.org.ua/consultations/foto-z-sotsmerezh-u-media/

[41] BARKAR D., Almost The Media. How Telegram Manipulates The Audience, 23.11.2022, from https://imi.org.ua/monitorings/majzhe-zmi-yak-telegram-manipulyuye-audytoriyeyu-i49222

channels. Nevertheless, public display, reproduction, and distribution of a photo featuring a person is possible only with their consent. These norms of the Civil Code of Ukraine are applied by courts when considering civil cases. For example, the decision of the Supreme Court of Ukraine (Case No. 308/5318/15-ts[42] dated January 30, 2019) established that the distribution of a photo depicting the plaintiff without his consent violated non-property rights and the right to respect for private life. The Odesa Court of Appeal (case No. 520/1084/18[43] dated 02.07.2018) equated the posting of photos on a social network to the dissemination of information that belongs to a person's private (personal) life. If a person did not allow their photos to be published, and the person who did so did not have any legitimate purpose (for example, to protect the interests of the individual or to protect the interests of others), the courts will find a violation of the right to privacy.

This section provides and analyzes examples of several types of privacy violations in social networks. However, in practice, there are many more such types of violations and they are all of a different nature. These types of violations can be divided into three categories: internal - when the social network does not provide an adequate level of protection for its users and itself violates their rights (like with Zoom example); external - when the technical and legal standards of protection are met, but the violation occurs outside the social networks' responsibility (due to the specifics social network as news in Telegram); as well as constructed - when, due to improper security provision by social networks, there is a violation of privacy from third parties (Telegram case 2022[44]).

[42] Resolution of the Supreme Court of Ukraine, court proceedings: 61-21960sk18, January 30, 2019, from https://reyestr.court.gov.ua/Review/79744914

[43] Decision of the Kyiv District Court of Odessa, Proceedings No. 2/520/3686/18. From https://reyestr.court.gov.ua/Review/75030458

[44] See Chapter 4.1, p.43

PART III. Legal mechanisms of Privacy and Personal Data protection in Social Networks

3.1. Chapter I. EU Legal framework of the Privacy and Personal Data protection in Social Networks

In the context of the legal basis for the protection of privacy and personal data in the EU and other legislative systems, the definition of the model of approach to the legal regulation of the relevant sphere is of primary importance. Organizations around the world must adhere to different data protection models, depending on applicable laws and regulations. These include such regulation models as comprehensive, sectoral, co-regulatory, and self-regulation models.

The comprehensive model promotes uniformity and consistency in data protection regulation at a high legislative or governmental level. For example, in the EU, all member states are subject to the General Data Protection Regulation (GDPR), as are any countries or organizations who process individuals' data in the EU. In Brazil, the Lei Geral de Proteção de Dados (LGPD)[45] clarified and unified the prior sectoral laws into an overarching data protection law. In the U.S., California has made steps through the California Consumer Privacy Act (CCPA) and California Privacy Rights Act of 2020 (CPRA)[46] to unify its various state level and sectoral privacy laws and regulate the processing of personal data of its residents.

Thus, in the EU, the legal basis for data protection and the construction of other regulatory acts, in particular in the field of data protection in social networks, is the General Data Protection Regulation. The General Data Protection Regulation (GDPR) is a law dealing with data protection and privacy that went into effect in the EU and the European Economic Area (EEA) on May 25, 2018. Material scope, meaning the actions covered by the Regulation, is defined in Article 2 of the GDPR: "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

Provisions of the GDPR, which can directly effect social network privacy issues include the following: principles relating to processing of personal data, lawfulness of processing, conditions for consent, child`s consent pecularities, transparent

[45] Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14/08/2018, from https://www.gov.br/mds/pt-br/acesso-a-informacao/governanca/integridade/campanhas/lgpd

[46] The California Consumer Privacy Act of 2018, from November 2020, from https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/

communication, right of access, right to be forgotten, right to restricton, responibility of the controller, data protection by design, data protection impact assessment, general principles for transfers, remedies, liability, penalties and other.

One of the key effects is the emphasis on user consent, necessitating that social networks procure explicit and informed consent before collecting or processing personal data. Additionally, social networks are mandated to provide transparent and comprehensive privacy policies, detailing the purposes and methods of data processing. Moreover, the regulation has necessitated the appointment of Data Protection Officers (DPOs) within social network organizations, ensuring a designated point of contact for data protection matters and facilitating compliance. Social networks are now required to implement technical and organizational measures to safeguard user data, reducing the risk of data breaches and unauthorized access. The GDPR has also catalyzed a paradigm shift in cross-border data transfers, compelling social networks to adopt mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) when transferring data outside the European Economic Area (EEA).

In addition to it, there is also an additional array of regulatory acts (which is already sectoral in nature - to address issues and potential harms within industry sectors), which we will consider in more detail.

In particular, these acts include: 1) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive[47]); 2) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive[48]); 3) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive[49]); 4) Court of Justice of the European Union (CJEU) Decisions (such as the

[47] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

[48] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[49] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

"Schrems II" decision, impact data transfer mechanisms between the EU and third countries, affecting data processing by social networks); 5) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act[50]); 6) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act[51]); 7) Codes of Conduct and Certification Mechanisms (such as Data Protection Code of Conduct for Cloud Infrastructure Service Providers).

The European ePrivacy Regulation is "lex specialis" to the General Data Protection Regulation (GDPR). The EU accepts the legal doctrine "lex specialis derogat legi generali" (a special law overrides laws that govern general matters)[52]. According to Article 1, Subject matter, the regulation lays down rules regarding the protection of fundamental rights and freedoms of natural persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

According to Article 2, Material Scope, this Regulation applies to: (a) the processing of electronic communications content and of electronic communications metadata carried out in connection with the provision and the use of electronic communications services; (b) end-users' terminal equipment information; (c) the offering of a publicly available directory of end-users of electronic communications services; (d) the sending of direct marketing communications to end-users.

NIS 2 Directive. The NIS 2 Directive replaces and repeals the NIS Directive (Directive 2016/1148/EC). NIS 2 will improve cybersecurity risk management and introduce reporting obligations across sectors such as energy, transport, health and digital infrastructure. The directive will formally establish the European Cyber Crises Liaison Organisation Network, EU-CyCLONe, which will support the coordinated management of large-scale cybersecurity incidents – in the context of information security, which will prevent privacy incidents within Social Networks in particular.

[50] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[51] REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

[52] The European ePrivacy Regulation, from https://www.european-eprivacy-regulation.com

Shrems II Decision. On 16 July 2020, the Court of Justice of the European Union (ECJ) in its Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called “Schrems II case”[53]) invalidated the EU-US Privacy Shield. The Court cast doubt over the extent transfers can be legitimised by the European Commission’s Standard Contractual Clauses (SCC) for personal data transfers to the US and globally. The SCCs were still valid as a transfer mechanism in principle but would require additional work[54].

Thus, the regulatory system for the protection of privacy and personal data in the European Union is based on the GDPR and is characterized in the same way as a comprehensive model of privacy protection (not only in social networks). However, there are other sectoral or special acts that regulate specific aspects of data protection in the digital environment. While the GDPR is the key European Union law governing the collection and processing of personal data, member states have their own specific cybersecurity laws and standards, which may also include requirements for social media. These standards include technical and organizational measures to protect users' personal data.

Such provisions, in particular, are contained in the law on the protection of personal data in Germany (BDSG - Bundesdatenschutzgesetz[55]), the law on the protection of personal data in France (Loi Informatique et Libertés[56]), the law on the protection of personal data in Italy (Codice in materia di protezione dei dati personali[57]) , the law on the protection of personal data in Poland (Ustawa o Ochronie Danych Osobowych[58]), etc. These laws introduce three main national mechanisms for the protection of personal data in social networks: legislative, judicial and administrative. Depending on the composition of the offense - its subjects, victims, guilt, degree of public danger and the nature of legal relations, they can be divided into civil-law, administrative-law, criminal-law and legislative national mechanims of privacy protection in OSNs.

[53] Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems Request for a preliminary ruling from the High Court (Ireland), from https://curia.europa.eu/juris/liste.jsf?num=C-311/18

[54] Sharp Cookie Advisors, Schrems II a summary – all you need to know, 23 November 2020, from https://www.gdprsummary.com/schrems-ii/

[55] Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

[56] La loi Informatique et Libertés, December 17. 2015, from https://www.cnil.fr/fr/la-loi-informatique-et-libertes

[57] Codice in materia di protezione dei dati personali, 10 agosto 2018, from https://www.garanteprivacy.it/codice

[58] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000, 2018-05-25 from https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

Having revealed the basic normative regulation of privacy and personal data protection in social networks within the EU, we came to the conclusion that a unified approach to legal regulation within the EU involves the creation of one act, which is a standard and a basis for domestic regulation of privacy and data protection, in particular in social networks. In addition, in other legal systems there are other approaches, the effectiveness of which may differ from the European one and have their own characteristics and advantages, which require research and analysis. The next section is dedicated to these systems.

3.2. Chapter II. Privacy and Personal Data protection in social networks within separate data protection models

As indicated earlier, different states have chosen different approaches to the regulatory regulation of personal data protection, and therefore to the protection of personal data and privacy in social networks. When closely examining the different models in operation around the world, it will be useful to consider why different parts of the world have adopted different approaches to data protection and privacy protection on social networks in particular.

The sectoral model, as the name suggests, approaches data protection by sector, usually based on market sector or population. The U.S. utilizes the sectoral model at the federal level. These laws are built on legislation to address issues and potential harms within industry sectors. There are several federal laws that touch on social media privacy concerns, including the Communications Decency Act (CDA)[59][60] and The Children's Online Privacy Protection Act (COPPA)[61].

CDA, in particular, Section 230, emphsizes on the online speech and COPPA imposes certain requirements on operators of websites or online services when they are collecting personal information online from a child under 13 years of age[62]. Microsoft will pay $20 million to settle FTC charges that it violated COPPA by collecting personal information from children who signed up to its Xbox gaming system without notifying their parents or obtaining their parents' consent, and by illegally retaining children's personal information[63]. Google LLC and its subsidiary YouTube, LLC paid a record $170 million to settle allegations by the Federal Trade Commission and the New York Attorney General that the YouTube video sharing service illegally collected personal information from children without their parents' consent[64].

[59] S. 314 (IS) - Communications Decency Act of 1995

[60] NEWTON C., Everything you need to know about Section 230, Dec 29, 2020, from https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation

[61] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

[62] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

[63] Federal Trade Comission, FTC Matter/File Number 1923258, Civil Penalties, from https://www.ftc.gov/legal-library/browse/cases-proceedings/1923258-microsoft-corporation-us-v

[64] Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, September 4, 2019, from https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

There have been many other efforts to enact federal legislation to better address social media protections, but no national comprehensive social media privacy laws exist yet and there is no U.S. equivalent to the EU General Data Protection Regulation (GDPR).

The comprehensive model promotes uniformity and consistency in data protection regulation at a high legislative or governmental level. For example, in the EU, all member states are subject to the General Data Protection Regulation (GDPR), as are any countries or organizations who process individuals' data in the EU. In Brazil, the Lei Geral de Proteção de Dados (LGPD) clarified and unified the prior sectoral laws into an overarching data protection law. Lei Geral de Proteção de Dados Pessoais (LGPD) is a Brazilian data protection law that governs how companies collect, use, disclose and process personal data belonging to people in Brazil. LGPD applies to companies that process data about individuals in Brazil. LGPD establishes a new standard of consent in Brazil and broadens individuals' rights with respect to accessing and porting their data. From July 2020, Facebook began to ask people in Brazil to grant it permission to use certain types of data, such as data with special protections under LGPD[65].

In the U.S., California has made strides through the California Consumer Privacy Act (CCPA) and California Privacy Rights Act of 2020 (CPRA) to unify its various state level and sectoral privacy laws and regulate the processing of personal data of its residents. China also has designed several uniform acts, which help to better protect Privacy and personal data, in particular, in social networks. The Cybersecurity Law (CSL)[66] went into effect on June 1, 2017, and effectively amalgamated a number of regulations and laws related to cybersecurity under one umbrella. The CSL is intended to protect China's national security, combat online crime and improve information and network security. The Data Security Law (DSL)[67] became effective September 1, 2021. It expands on areas of the CSL, focusing on national security as well as classifying data based on its import to Chinese national security. This in turn has a flow-through effect on how the data may be stored and transferred. The most recent of the three laws, the Personal Information Protection Law (PIPL)[68], has a number of elements strongly reminiscent of the EU GDPR and went into effect on November 1, 2021. The PIPL is designed to protect personal information, regulate its processing and promote the reasonable use of personal

[65] Meta Business Help Centre, How does Lei Geral de Proteção de Dados Pessoais (LGPD) affect advertising on Facebook?, from https://en-gb.facebook.com/business/help/327111418314780?ref=search_new_185

[66] China's Cyber Security Law (CSL), Passed November 6, 2016. Effective June 1, 2017, from https://www.informatica-juridica.com/ley/chinas-cyber-security-law-csl/

[67] DLA PIPER, Data Protection Laws of The World, November 2023, from www.dlapiperdataprotection.com

[68] Personal Information Protection Law of the People's Republic of China, 21st October 2020, from https://personalinformationprotectionlaw.com

information. Unlike the CSL and DSL, it also restricts itself to information about natural persons. For example, a Chinese social media platform was recently fined 1.5 million RMB for violating the regulations on excessive data collection and unauthorized sharing of user data[69].

The self-regulation model typically refers to a stakeholder-based model for ensuring data protection. In this situation, the term "stakeholders" does not necessarily mean individuals who hold stock or a controlling interest in an organization. Instead, it means those who decide how the organization will operate on a day-to-day basis. This model came from the need for industry bodies and associations to both improve and inform data protection practices in their industries and processing activity areas. The DAA (Digital Advertising Alliance) is a U.S.-based industry self-regulatory program for online behavioral advertising. They offer tools for users to opt out of targeted advertising, as well as guidelines for advertisers and companies on how to provide transparency and choice to consumers regarding data collection and use[70].

The co-regulatory model emphasizes industries developing enforceable codes or standards for data protection that are regulated by the government. Co-regulatory models can exist under both comprehensive and sectoral models. For example, the co-regulatory model adopted in Australia and New Zealand came from a desire to improve data protection practices for businesses in a sustainable and pragmatic way. This approach is based on the concept of reasonableness. Applying generally accepted Fair Information Practices and supporting these principles through codes enables businesses to proportionately achieve the law's objectives. Unlike the comprehensive model, the co-regulatory model tends to avoid providing individuals with absolute data rights; the co-regulatory model focuses on what is reasonable under the circumstances instead. For example, the Ministry of Electronics and Information Technology in India proposed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules[71], 2021. These rules include requirements for social media platforms to establish grievance redressal mechanisms and comply with content takedown requests.

[69] OneTrustDataGuidance (Regulatory Research Software), China: CAC fines Didi RMB 8 billion for CSL, DSL, and PIPL violations, 21 July 2022, from https://www.dataguidance.com/news/china-cac-fines-didi-rmb-8-billion-csl-dsl-and%C2%A0pipl

[70] Digital Advertising Alliance, DAA Self-Regulatory Principles, June 2023, from https://digitaladvertisingalliance.org/principles

[71] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 06.04.2023), https://www.meity.gov.in/content/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

3.3. Chapter III. Legal mechanisms of the right to Privacy and Personal Data protection in social networks policies, terms of service and Privacy agreements

In addition to the basic methods of protecting privacy and personal data of users at the level of the state and international organizations, there are also direct local regulators of relations between users of social networks and providers of relevant services. Such regulators are based on the legislation but can provide additional safeguards to the users of social networks. These include social networks policies, terms of service, and privacy agreements.

A privacy policy acts as an explanation of how OSN plans to use personal information which it collects through the mobile app or website[72]. Privacy policies are sometimes called privacy privacy notices or privacy statements. They serve as legal documents aimed to protect company and consumers. Privacy policies are different from data protection or security agreements and cookie policies. A data protection agreement is an internal document that outlines how service and any third-party vendors will work to safely handle customers' personal information. A cookie policy allows users of the website or app know that services uses pieces of code stored on their hardware called cookies to track and store some of their activity. These policies tend to pop up when users first access a website, as opposed to a privacy policy which will likely only come up when users of social networks enter their personal data – for example, register an account.

Privacy policies contain provisions on the order of data collection, user consent, data usage, third-party sharing, security measures, data retention, user rights, cookies and tracking, children's privacy, legal compliance, updates to policies, termination an account deletion, contact information etc.

The GDPR (General Data Protection Regulation) laws set guidelines starting in 2016 for how data can be collected and processed if a party lives or does business in the EU. Same in the US, the CCPA (California Consumer Privacy Act) is a state statute signed in 2018 meant to protect the residents of California from predatory data collection practices. Thus, with the adoption of GDPR, CCPA, CPRA, PIPA, PIPEDA and other local government and international regulations, all the most popular social networks, such as Facebook (Meta), Twitter, Instagram (Meta), LinkedIn, Snapchat, TikTok, Pinterest,

[72] Ironclad Journal, What Is a Privacy Policy? Everything You Need to Know, from https://ironcladapp.com/journal/contracts/how-to-create-the-best-privacy-policy-for-your-business/

Reddit, Tumblr, WhatsApp (Meta), YouTube (Google), Discord implemented such policies.

The importance of policies goes far beyond simple compliance with the current legislation[73]. In effect, with policies, it is not just a simple guaranteeing the fulfillment of a set of normative obligations because their content, on numerous occasions, goes beyond them and covers a certain legal void. This extreme can be linked to both the advocacy work of legislators regarding self-regulation - of which privacy policies are a manifestation - and that the companies themselves significantly value the privacy concerns that citizens generally express[74].

Regarding the effectiveness of the implementation of appropriate privacy protection measures. Let's look into the privacy policy, user agreement and terms of service introduced by YouTube (Google)[75] and analyze them for compliance with the legislation on the protection of privacy.

The requirement of conformity of the acts that determine the relationship in the field of privacy between the user and the service is contained in articles 1-3 of the GDPR, namely the territorial and material criteria. Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.

In fact, the framework norm to which the privacy policy must comply is Article 12 of the GDPR, which contains blanket norms to which it refers in turn. The legal nature of the privacy policy is due to the fact that it is an informative document and does not create rights and obligations for the parties, but only informs the client about how his data is protected, used, transferred, etc. Therefore, the critical question to be clarified is: a) whether such a policy (notice) exists at all and b) whether its content and availability meet the

[73] MAROTTA-WURGLER F., Understanding Privacy Policies: Content, Self-Regulation, and Markets, NYU Law and Economics Research Paper No. 16-18, January 3, 2016, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513

[74] DITTMAR, E. C.; JINÉNEZ, D. L.; PORTILLO, P. V. *Safeguarding Privacy in Social Networks*. The Law, State and Telecommunications Review, Brasilia, v. 12, no. 1, p. 58-76, May 2020. DOI: https://doi.org/10.26512/lstr.v12i1.31238.

[75] Google Privacy Policy, November 15, 2023, https://policies.google.com/privacy?hl=en#infocollect

requirements of Article 12 of the Regulation. In turn, Article 12 already imposes other regulatory requirements, failure to comply with which entails its violation.

The first thing that becomes noticeable when opening the policy page is the possibility to download a privacy policy in pdf format which seems more convenient for the user than the classic format in which it is placed. In this part, this approach corresponds to the provision of part 1 of article 12 of the GDPR, namely that the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Article 13, to which Article 12 of the Regulation refers, contains a specific list of requirements for information that the controller shall, at the time when personal data are obtained, provide the data subject. In particular, this includes the fact that the controller intends to transfer personal data to a third country, as well as the contact details of the data protection officer - which is absent in the YouTube policy, but necessary given the vagueness of the information about whose servers the processing takes place user data and a large number of requests regarding personal data or their violations by Google.

The Policy also lacks information about the right to rectification, which is a violation of Article 16 of the Regulation, in the context of the impossibility of correcting or clarifying one's data. In addition, Article 22 of the Regulation directly grants the data subject the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The policy states that "we analyze your content to better detect violations such as spam, malware, and prohibited content". Such decision-making is possible, however, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

The next object of our legal analysis is the YouTube user agreement, in our case it is the YouTube Terms of Service[76]. The fact is that, by its very nature, the contract for the use of Google services is an accession contract, the terms of which we agree to after reading the aforementioned Terms of Service, which actually establish the real rights and obligations of the parties to the contract.

[76] Terms of use, You Tube, January 5, 2022, from https://www.youtube.com/static?template=terms

Let's define the articles of the Regulation, which must comply with the agreement between the user and the YouTube service. Here, first of all, we can refer to Article 5 - Principles relating to processing of personal data. In addition to the principles, this includes grounds for lawful data processing (Article 6), criteria for consent (Article 7). This also includes the aforementioned requirement regarding transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12), as well as information to be provided where personal data are collected from the data subject (Article 13) - limited in scope of our study, compliance with this article will be the object of our analysis. In addition to the articles mentioned above, the Agreement or Terns of Service (as well as the actual actions of the data controller) must comply with articles 14-22, 24-39, and especially - 44-50, as far as cross-border data transfers are concerned.

The Service is provided by Google LLC, which operates under the laws of the state of Delaware (the address of the main office is: 1600 Amphitheater Parkway, Mountain View, CA 94043). However, this does not affect the validity of the provisions of the Regulations, based on articles 1-3 of the GDPR, which we mentioned earlier.

Regarding the content of the Terms themselves. Only one section is actually dedicated to privacy and refers us to YouTube's general Privacy Policy[77]. In general, the entire regulatory and informational base of YouTube's activity is built on such a blanket principle, where there are 5-7 sources that are cross-referenced.

YouTube's personal data processing procedure defines the terms of processing of the User's Personal Data. This procedure is an addendum to the agreement between the user and Google about his use of YouTube services.

The procedure uses the term "User's Personal Data", by which YouTube means audio and audiovisual content that is uploaded by the User to YouTube in accordance with the terms of the Agreement and processed by Google on behalf of the User in the provision of Google Services of the Administrator of Personal Data. In fact, Google thus replaces the category of "Personal Data" according to the Regulation with its own definition in the context of the specifics of the service itself. However, in our opinion, such a replacement is not appropriate, because although it is understandable that the service tries to highlight the specific data with which it deals, the range of personal data that YouTube receives is not limited to audiovisual content, but also other user data - for example, data that it obtains information from the user during registration (e-mail, name, age, etc.). At the same time,

[77] How YouTube processes personal data, effective date: November 24, 2020, from https://www.youtube.com/t/terms_dataprocessing

the Procedure separately states that the term "personal data" when used in this Procedure for the processing of personal data is used in the meanings given to them in the GDPR Regulation. What is unclear then is the need to isolate the user's personal data from the general category of personal data.

In the context of Article 13 of the Regulation, when personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with six main categories of information.

The first one is the identity and the contact details of the controller and, where applicable, of the controller’s representative. Although information about the data controller is specified in the Order, neither his contact details nor the representative's contact details are clearly indicated. In section 12 of the Procedure entitled “Appeal to Google” it is stated that the user can apply to Google regarding the exercise of his rights under this Procedure for the processing of personal data by the methods described in https://support.google.com/youtube/answer/2801895[78] or other in ways that may be provided by Google at the relevant time.

After clicking on several links, we come to the fact that there are two possible ways to remove unacceptable content that violates your right to privacy in the YouTube service - these are the report procedure, which is general, and the Privacy Complaint, which contains a standardized form and is submitted by filling out a separate questionnaire. And again, exactly where and to which address we send this complaint is unclear. In this context, point (a) of the Article 13 of the Regulation is not fully implemented satisfactorily, and clause (b) of the Regulation is not satisfied - the contact details of the data protection officer[79].

Next is the requirement to indicate the purposes of the processing for which the personal data are intended as well as the legal basis for the processing as well as the legitimate interests pursued by the controller or by a third party (clause (c), (d)). Such purposes are somewhat vaguely described in the above-mentioned Privacy Policy, in particular, they include: provision of services, support and improvement of services, development of new services, personalization of services, content and ads, performance tracking, communication with the user, protection of users and the public[80].

[78] Protecting your identity, You Tube Help, Privacy and safety center, from https://support.google.com/youtube/answer/2801895?ref_topic=2803240

[79] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[80] You Tube Privacy Policy, valid from November 15, 2023, from https://policies.google.com/privacy?hl=uk

The next requirement of the Regulation is point (e), namely the recipients or categories of recipients of the personal data, if any. Such information is not specified in the Data Processing Procedure. Nevertheless, in the context of the last requirement (clause (f) - the fact that the controller intends to transfer personal data to a third country or international organization), the Procedure states that: "if the storage and/or processing of the User's Personal Data includes the transfer of the User's Personal Data from the EEA, Switzerland or Great Britain to any third country for which there is no decision recognizing the appropriateness of personal data protection measures in such countries in accordance with the European Legislation on the Protection of Personal Data: (a) The User (as the exporter of personal data) shall be deemed to have entered into the Standard Contractual Provisions with Google LLC (as the importer of personal data); (b) the transfers will be governed by the Standard Contractual Clauses; and (c) Google will ensure that Google LLC complies with its obligations under such Standard Contractual Terms with respect to such transfers." In this case, we believe that Google properly informed the user about the legal possibility to transfer data to third parties for the purposes of fulfilling the terms of the service agreement (Terms of Service).

Conclusions regarding the effectiveness of local methods of regulating legal relations in the field of personal data protection. As already mentioned above, the privacy policy, or privacy notice, privacy policy - is a purely informative document that does not establish the rights and obligations of the parties regarding the use of the service and issues related to privacy protection. Such acts which establich those rights are the user agreement and Terms of Service. However, in practice, as we can see from the activity of Google, namely the YouTube service, these acts can have a different nature, a specific structure, and be not only informative.

Despite the fact that the main act that regulates the relationship in the field of privacy between consumers and the YouTube service is the YouTube Terms of Service and YouTube's general Privacy Policy, separate issues of data transfer and protection of one's rights are still contained in a separate privacy policy. Therefore, if the user of the service has certain problems related to the privacy or protection of his personal data on YouTube, it will be necessary to examine at least four documents, without distinguishing or separating the normative from the introductory documents of the service. In this way, the user will be able to objectively assess exactly how his privacy and personal data are protected and which protection mechanisms will be the most beneficial for him to use in a particular case.

PART IV. Privacy and Personal Data protection in Social Networks: court and DPA practice

4.1. Chapter I. ECHR parctice in the sphere of Privacy and personal data protection in Social Networks

As can be seen from the previous sections, the issue of privacy protection in social networks is multifaceted in its structure. It covers both the normative mechanism of protection, which we have described in the context of legislation and local acts, and the organizational one, which mainly includes the activities of courts and National Data Protection Authorities. Determining the role of the court, judicial practice, as well as the activities of Data Protection Authorities in the field of privacy and personal data protection in social networks provides clarity in understanding the existing system of protecting right to Privacy and helps to build proposals for improving the relevant system. This section will analyze the role and practice of the European Court of Human Rights in the context of the most recent court cases in the field of privacy and personal data protection in social networks on the EU territory.

The first case – Ekimdzhiev and Others v. Bulgaria[81] touches the protection of privacy and personal data of individuals, namely their communication data, in particular from social networks. And although it is not directly related to specific examples of privacy violations in OSN, it is of a nature that raises the issue of information security of social network users in Bulgaria, as well as the issue of the possibility of interference in private life in the case of criminal prosecution of individuals. The application no. 70078/12 against the Republic of Bulgaria was lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by two Bulgarian nationals, Mr Mihail Tiholov Ekimdzhiev and Mr Aleksandar Emilov Kashamov, and by two non-governmental organisations, the Association for European Integration and Human Rights and the Access to Information Foundation (“the applicants”). It concerns the compatibility of the Bulgarian laws and practices relating to (a) secret surveillance and (b) the retention of and access to communications data with Article 8 of the Convention[82].

[81] CASE OF EKIMDZHIEV AND OTHERS v. BULGARIA, ECHR, (Application no. 70078/12), from https://hudoc.echr.coe.int/#_Toc92116208

[82] Guide on Article 8 of the European Convention on Human Rights, Updated on 31 August 2022, from https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

Under Bulgarian law, all communications service providers in the country had to retain all the communications data of all of their users for six months, with a view to making that data available to the authorities for certain law-enforcement purposes. Various authorities might then access that data. By section 12(1) to (3) of the 1997 Act, special means of surveillance may be used with respect to (a) persons suspected of, or unwittingly used for, the preparation or commission of one or more of the above-mentioned "serious intentional offences"; (b) persons or objects related to national security; (c) objects necessary to identify such persons; (d) persons who have agreed to being placed under surveillance to protect their life or property; or (e) a witness in criminal proceedings who has agreed to being placed under surveillance in order to expose the commission of one of the offences listed in section 12(3) by another (those include terrorist offences, hostage holding, human trafficking, taking and giving a bribe, and being the leader or member of a criminal gang).

It was stated by court, that in view of the technological and social developments in the past two decades in the sphere of electronic communications, communications data can nowadays reveal a great deal of personal information. If obtained by the authorities in bulk, such data can be used to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who that person has interacted with. The acquisition of that data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, § 277, and *Big Brother Watch and Others*, § 363)[83].

The court made a conclusion, that the general retention of communications data by communications service providers and its access by the authorities in individual cases had to be accompanied, mutatis mutandis, by the same safeguards against arbitrariness and abuse as secret surveillance. However, the Bulgarian laws fell short of those minimum safeguards. These safeguards, in particular are: 1) the authorisation procedure was not capable of ensuring that retained communications data was accessed by the authorities solely when that was "necessary in a democratic society"; 2) no clear time limits had been laid down for destroying data accessed by the authorities in the course of criminal proceedings; 3) no publicly available rules existed on the storing, accessing, examining,

[83] CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM, 25 May 2021, from https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-210077%22]%7D

using, communicating and destroying of communications data accessed by the authorities; 4) the oversight system, as currently organised, was not capable of effectively checking abuse; 5) the notification arrangements, as currently operating, were too narrow; and 6) there did not appear to be an effective remedy. The Court found a violation of Article 8 of the Convention and held that the findings of violation in themselves constituted sufficient just satisfaction for any non-pecuniary damage suffered by the four applicants as a result of the two violations of Article 8 of the Convention established in the case. Such wording does have the right to exist in view of the circumstances of the case, but there are certain doubts about its practicality in the context of the termination of the violation, which, most likely, has not ceased since the court decision was issued.

What implications might this have for further legislative practice and our research. First, the state, as can be seen from the decisions of the ECHR, can really establish a similar type of procedure to ensure safety in society; secondly, such means, as indicated by the court, may also include mapping of social networks, which includes research and analysis of relationships and interactions between individuals or entities in social networks in order to reveal patterns, structure and nature of interactions between them; such interference in privacy in social networks in certain cases, clearly provided by law, the court recognizes as legal and necessary in a democratic society, which, however, was not adequately ensured by the Bulgarian government; such intervention must have clearly defined grounds and procedure for its implementation, start and end time limits, as well as guarantees against arbitrary interference and abuse by state authorities in relation to those categories of persons whose networks are monitored; in the case of exceeding such limits or abuses by the state, there should be an effective system of guarantees for the person, which consists in a) immediate restoration of his previous legal status and removal of information obtained illegally, b) compensation for the damage caused.

The next case shows that complete information security in the context of the right to privacy in social networks should not be expected. The case of Big Brother Watch and others v. the United Kingdom[84] originated in three applications (nos. 58170/13, 62322/14 and 24960/15) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The three applications were introduced following revelations by Edward Snowden relating to the electronic surveillance

[84] CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM, 25 May 2021 from https://hudoc.echr.coe.int/#_Toc524359875

programmes operated by the intelligence services of the United States of America and the United Kingdom.

As it was stated in the text of the decision of 2021, Internet communications are primarily carried over international sub-marine fibre optic cables operated by CSPs. Each cable may carry several “bearers”, and there are approximately 100,000 of these bearers joining up the global Internet. A single communication over the Internet is divided into “packets” (units of data) which may be transmitted separately across multiple bearers. These packets will travel via a combination of the quickest and cheapest paths, which may also depend on the location of the servers. Consequently, some or all of the parts of any particular communication sent from one person to another, whether within the United Kingdom or across borders, may be routed through one or more other countries if that is the optimum path for the CSPs involved.

The Edward Snowden revelations indicated that GCHQ (being one of the United Kingdom intelligence services) was running an operation, codenamed “TEMPORA[85][86]”, which allowed it to tap into and store huge volumes of data drawn from bearers. The United States’ National Security Agency (“NSA”) has acknowledged the existence of two operations called PRISM and Upstream. The US Government has publicly acknowledged that the Prism system and Upstream programme ... permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or ... pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.

However, it was stated by the court, that it is a justifiable interference with an individual’s rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds: in the interests of national security; to prevent or detect serious crime; to safeguard the economic well-being of the UK so far as those interests are also relevant to the interests

[85] Digital Citizenship and Surveillance Society, 4th March 2016, Cardiff University, from https://dcssproject.net/tempora/index.html

[86] The Gurdian, UK-US surveillance regime was unlawful ‘for seven years’, February 2015, from http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa

of national security.The collected information covers “nearly everything a user does on the Internet,” according to a presentation on the XKEYSCORE system[87]. The slides specifically mention emails, Facebook chats, websites visited etc[88].

Despite the fact that the European Court of Human Rights indicated the possibility and legality of such interference in personal communication, in the context of privacy in social networks it should be borne in mind that complete information security does not exist, and the ways to obtain information from it are very diverse, as well as the actual grounds for such actions.

The last ECHR case that we will analyze is the case of Glukhin v. Russia[89]. The court's decision concerned, in particular, a violation of Article 8 of the Convention - unjustified processing of applicant's personal biometric data by using highly intrusive facial recognition technology in administrative offense proceedings in order to identify, locate and arrest him. This case is not about privacy within social networks. However, it points to the specificity of social networks, which cannot completely hide the data of their users, since they are designed for the opposite - the distribution of this data, for example, Telegram or Instagram. It is interesting not only the conclusion of the court, which expectedly recognized such actions as illegal, but also the very case of the possibility of using personal data by the police in a way that raises questions about information security in the Telegram network and in social networks in general. In particular, this concerns the possibility of cooperation of Telegram with the special services of the Russian Federation and the possibility of transferring the data of demonstrators.

The relevant parts of the report of 17 January 2022 by OVD-Info, an independent human rights media project, entitled “How the Russian state uses cameras against protesters” read as follows: “Detentions of protesters after the end of the event, or, as we call them, ‘post factum detentions’, have taken place before 2021. In 2018, OVD-Info counted 219 such cases in 39 regions of Russia; they were mostly isolated in nature: one or two people were detained in connection with one event, in exceptional cases the number of detainees reached ten. They began to be widely used in 2020 ... We believe that the increase in the number of post factum detentions is based on the development of technologies for monitoring social networks and facial recognition ... Our report is devoted to the use of facial recognition systems to restrict freedom of assembly. Although our research focuses

[87] The Guardian, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', from https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[88] Internet surveillance after Snowden: A critical empirical study of computer experts’, November 2017, Journal of Information Communication and Ethics in Society 15(1)

[89] CASE OF GLUKHIN v. RUSSIA, ECHR, 04/10/2023, Final Judgement.

on Moscow, according to our data, the geography of this phenomenon goes far beyond the capital. To identify the protesters, recordings from surveillance cameras ..., recordings made on the ground by law enforcement officers, photos and videos from the Internet (Telegram channels, chats, personal pages on social networks, YouTube) have been used. There are cases when cameras – for example, installed in the entrances of residential buildings or in the subway – were also used to determine the location of a person to hold him administratively responsible. For identification, the police use databases with photos from documents (internal and external passports, social cards) and from social networks.

This event takes on a different color in the context of the "ban" of Telegram in Russia. In 2018, the FSB of Russia wanted to receive from Telegram the keys to decrypt user correspondence. To which she received a refusal from Pavlo Durov - this was logically followed by a lengthy legal process. On October 16, 2018, the court fined Telegram 800,000 rubles for refusing to cooperate with the FSB, and attempts to block Telegram began. On June 28, the owner of Telegram, Pavlo Durov, agreed to provide "Roskomnadzor" with the data necessary to register the messenger. The department agreed to register the company.

Subsequently, the deputy head of the Ministry of Communications of the Russian Federation, Oleksiy Volin, said that Roskomnadzor and the prosecutor's office decided to stop blocking Telegram in Russia, as it is technically impossible, and the messenger team itself is already cooperating with the authorities. In addition, Volin explained the unlocking by the need to spread information about covid. Thus, the authorities officially admitted that, despite the loud statements, at least since the summer of 2018, Telegram had already been giving the special services of the Russian authorities the data of the suspects.

In the summer of 2020, a draft law was submitted to the State Duma of the Russian Federation to prohibit the blocking of Telegram, because it is a means of obtaining operational information for a large number of Russians. Roskomnadzor announced that it will remove restrictions on access to Telegram thanks to an agreement reached with the Prosecutor General's Office of the Russian Federation. And later, Putin's comment appeared that he and Telegram had come to an agreement.

Thus, the question regarding the telegram's violation of the privacy policy and cooperation with the authorities of the Russian Federation, although not proven, but in the light of the decision of the ECHR... has the right to exist. In its decision, nevertheless, the ECHR ruled that there has been a violation of Article 8 of the Convention. Nevertheless, the violation that occurred in this case can have both an external and an internal nature, which is not fully within the competence of the ECHR.

4.2. Chapter II. National Data Protection Authorities. Role and practice in the sphere of Privacy and Personal Data protection in Social Networks

Pursuant to Article 51(1) of the GDPR, each Member State shall provide for one or more independent public authorities responsible for monitoring the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons with regard to processing and to facilitate the free flow of personal data within the Union ("supervisory authority"). Such bodies are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws[90]. Decisions os such bodies (including concurring or dissenting opinions) establish influential or persuasive precedent outside its jurisdiction. Such decisions may strongly impact on other EU Data Protection Data Protection Authorities' approach towards different issues in the context of social media platforms.

All national DPAs are part of the European Data Protection Board (EDPB). The European Data Protection Board (EDPB) is an independent European body. It is the umbrella organization which brings together the national data protection authorities (National Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS). The EDPB ensures that the General Data Protection Regulation and the Law Enforcement Directive are applied consistently and ensures cooperation, including on enforcement[91].

As indicated above, the practice of these national bodies has a significant impact on the activity of social networks in the EU and the protection of the privacy of their users. The Irish Data Protection Authority (IE DPA) has imposed an administrative fine of €1.2 billion on Facebook parent company Meta for breaching the General Data Protection Regulation (GDPR) after Meta transferred European Facebook users' data to the US. Technically, the fine was imposed on Meta Platforms Inc.'s Irish subsidiary Meta Platforms Ireland Limited, but as the fine was based on Meta's total global turnover, it is appropriate to refer to Meta in general.

[90] European Commission, What are Data Protection Authorities (DPAs)? Article 4(16), Chapter VI (Articles 51 to 59) and Recitals (117) to (123) of the GDPR, from https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

[91] European Data Protection Board, EDPB Chairmanship, from https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en

The administrative fine was imposed under Article 84 of the GDPR after the authorities found Meta in breach of Article 44 of the GDPR when transferring Facebook users' data from Europe to the United States. The fine is the largest administrative sanction imposed by EU authorities for a GDPR violation to date. The severity of the fine was influenced, among other things, by the fact that the authorities considered Meta to have acted intentionally or at least negligently in accordance with Article 83(2)(b) of the GDPR. Other contributing factors included the large amount of personal data transferred, the large number of data subjects and the duration of the infringement[92].

The decision reflects the rather strict position of the EU authorities regarding transfers of personal data to third countries. This severity is somewhat understandable when you are dealing with one of the largest companies in the world. However, it is not clear that the same criteria cannot be applied to the transfer of personal data by much smaller companies.

The next case has emerged in the context of children`s privacy protection in social networks. The measures were issued following the death of a child who took her own life by accident while allegedly trying to take part in the "Blackout challenge" on TikTok. The Italian Data Protection Supervisory Authority issued two interim measures restricting the ability of social media platform, TikTok, from processing the data of users, residing in Italy, whose age could not be determined with certainty[93].

The SA issued two decisions: 2021/20, on January 22, 2021; and 2021/61, on February 11, 2021.

In measure 2021/20 the SA imposed on TikTok a temporary restriction on the processing of personal data of users, residing on the Italian territory, whose age could not be determined with certainty. Although the measure was preliminary, this restriction had immediate effect (subject to any further assessment carried out by the SA), and lasted until February 15, 2021.

The SA took into account that TikTok had not yet provided a written reply to the statement from the SA in December, and highlighted that the preliminary investigation carried out had brought to light serious shortcomings with regard to the age verification procedure adopted by the company. The SA made specific reference to three provisions which highlighted the importance of protecting children's interests. It referred to article 24(2) of the Charter of Fundamental Rights of the European Union ("The rights of the

[92] SKURNIK T., Future transfers of personal data outside the EU, Nordia Law, 29.05.2023, from https://nordialaw.com/insights-data-privacy/

[93] Columbia Univerity, Italian Data Protection Authority v. TikTok, Case analysis, from https://globalfreedomofexpression.columbia.edu/cases/italian-data-protection-authority-v-tiktok/

child”), which states that “[i]n all actions relating to children, whether taken by public authorities or private institutions, the child’s best interests must be a primary consideration.” It also relied on recital number 38 of the GDPR which establishes that – with regard to personal data – “children merit specific protection” because they “may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”. Recital number 38 notes that processing of children’s personal data must be specifically protected for “the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”

In the second measure, the SA noted that as the notifications TikTok were sending to verify users’ ages had appeared only three days earlier, it was not possible to assess at that stage whether the measure adopted by TikTok was appropriate and effective. Accordingly, it extended the restriction established in the first measure to March 15, 2021.

The next case represents an example of privacy violation when a social media provider collected and stored personal data concerning its members' contacts for the purpose of sending invitations to connect on the platform.

On May 19, 2020, the Belgian Data Protection Authority (the “Belgian DPA”) announced that the Litigation Chamber had imposed a €50,000 fine on a social media provider for unlawful processing of personal data in connection with the “invite-a-friend” function offered on its platform[94].

In its decision, the Litigation Chamber recalled that consent must be provided by the data subject himself (except in certain situations, e.g., with minors). Therefore, the social media provider could not rely on the consent obtained from its members to legitimize the processing of personal data of contacts who were not members of the platform and thus never consented to the processing of their contact information. With respect to contacts who are members of the platform, the Litigation Chamber indicated that, at least at the beginning of the process, users were presented with pre-selected boxes at the stage where they are able to invite contacts. The Litigation Chamber emphasized that consent obtained through pre-selected boxes does not meet the standard for valid consent under the GDPR. With respect to the validity of consent, the Litigation Chamber also stated in its decision

[94] PRIVACY & INFORMATION SECURITY LAW BLOG, Global Privacy and Cybersecurity Law Updates and Analysis, Belgian DPA Sanctions Social Media Company for Unlawful Processing of Personal Data in Connection with “Invite-a-Friend” Function, May 27, 2020, from https://www.huntonprivacyblog.com/2020/05/27/belgian-dpa-sanctions-social-media-company-for-unlawful-processing-of-personal-data-in-connection-with-invite-a-friend-function/

that the practice of sending an initial, non-promotional email to obtain an individual’s consent for receiving electronic marketing is not in line with the GDPR.

Thus, we can see that national privacy protection authorities can and do have a significant impact on the situation with privacy protection in social networks. Their activities make it possible to relax national judicial institutions and quickly and effectively apply the necessary measures to protect the privacy of consumers in social networks.

PART V. Overview of existing privacy-enhancing technologies (PETs) and their applicability to Privacy protection in Social Networks. Privacy by design and user held data model

5.1. Chapter I. Overview of existing privacy-enhancing technologies (PETs) and legal benefits of their applicability to social networks

In addition to legal mechanisms for protecting privacy and personal data in social networks, technical means of combating violations in this area also play an important role. In particular, the report of the Committee on Digital Economy Policy of the OECD from 27 February 2023 indicates, that the key benefit of PETs is the promised opportunity to give data subjects full control over how their data is used in certain circumstances. This ensures that data is only used for approved purposes and by those who are authorized to do so[95]. Such technical means, by specifics of their orientation, aim to fulfill the relevant provisions of the law, which impose on social network services the obligation to observe the security of personal data and information security in general.

To the concept of privacy-enhancing technologies. There is no unified regulatory act that would give the concept of these technologies. Instead, within various studies and reports, the term PETs is still revealed. Thus, the aforementioned OECD Digital Economy Papers define PETs as a collection of digital technologies and approaches that permit collection, processing, analysis and sharing of information while protecting the confidentiality of personal data.

Early examinations of PETs can be traced back to a report titled “Privacy Enhancing Technologies (PETs): The Path to Anonymity,” first published in 1995 by Canadian and Dutch privacy authorities. This piece used the term"privacy-enhancing” to refer to a “variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data.”

Another early definition comes from “Inventory of privacy-enhancing technologies,” published by the Organisation for Economic Co-operation and Development in 2002, which describes PETs as “a wide range of technologies that help protect personal privacy[96]”.

[95] OECD Papers, Emerging privacy-enhancing technologies, Current regulatory and policy approaches, March 2023, from https://www.oecd-ilibrary.org/docserver/bf121be4

[96] KOERNER K., LALONDE B., Cheering emerging PETs: Global privacy tech support on the rise, iapp, The Privacy Advisor, January 24, 2023, from https://iapp.org/news/a/cheering-emerging-pets-global-privacy-tech-support-on-the-rise/

German early seed investor fund published a comprehensive report on PETs in 2021 titled "The privacy infrastructure of tomorrow is being built today." The report defines PETs as: "a set of cryptographic methods, architectural designs, data science workflows, and systems of hardware and software that enable adversarial parties to collaborate on sensitive data without needing to rely on mutual trust." The report predicts that by 2030, "data marketplaces enabled by PETs will be the second largest information communications technology market after the Cloud."

PETs can be divided into four categories: data obfuscation, encrypted data processing, federated and distributed analytics and data accountability tools. There are a few types of data obfuscation techniques but the most popular in social networks include: encryption, tokenization, Data masking[97].

Data masking. Another term used for this technique is data anonymization. It involves modifying data in some way to ensure data security. This can include techniques such as replacing data with asterisks or other symbols, truncating data, or removing it altogether. Data tokenization. This data obfuscation technique involves replacing sensitive data with randomly generated values, or "tokens." The tokens are stored in a secure location, typically in a separate database or file that is encrypted and accessible only to authorized personnel who can retrieve the original data when necessary. Tokens help prevent the theft of sensitive data by making it meaningless to anyone who might intercept it. Data encryption. As a method of data obfuscation, it involves transforming data into an unreadable form using an algorithm, called a cipher.

Masking techniques are essential for protecting social media publishers' identity and privacy from advanced metadata analysis. Especially this becomes important when using such social networks as Facebook or Twitter. Technically, they are able to expose valuable user privacy-related metadata, such as the camera model identification number and Global Positioning System (GPS) coordinates of where the content was created[98]. For instance, authorities were able to locate a fugitive based on the GPS information in a picture taken with an iPhone and published on social media[99]. Masking techniques, such as URL shortening, pseudonymization, and obfuscation, can help hide or distort metadata, making

[97] EPAM solutions hub, Data Obfuscation - Methods and Best Practices, April 21, 2023, from https://solutionshub.epam.com/blog/post/data-obfuscation

[98] KHADER M., KARAM M., Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis, 13 June 2023, from https://doi.org/10.3390/data8060105

[99] CLULEY, G. Fugitive John McAfee's Location Revealed by Photo Meta-Data Screw-Up. Available online: https://nakedsecurity.sophos.com/2012/12/03/john-mcafee-location-exif/

it difficult for adversaries to identify social media publishers. For example, URL shortening services can be used to mask the original URLs of social media posts, preventing adversaries from tracking the source of the posts based on the metadata in the URLs[100].

Encrypted data processing. Advanced metadata analysis techniques pose significant risks to the privacy and identity of social media publishers. Metadata, including timestamps, geolocation, device information, and user interactions, can be used to infer sensitive information about social media publishers, even if they have attempted to anonymize or mask their data. For example, studies have shown that metadata from social media posts can reveal users' real-world identities, interests, and behaviors, allowing potential adversaries to track and profile users with high accuracy[101]. Advanced metadata analysis can also lead to re-identification attacks, where seemingly anonymized data can be de-anonymized using metadata to reveal the identities of social media publishers, leading to privacy breaches and identity exposure[102].

Encryption techniques, such as cryptographic algorithms and protocols, can secure metadata by transforming it into a ciphertext that can only be decrypted by authorized parties, preventing unauthorized access to sensitive information. These techniques can provide an additional layer of protection against advanced metadata analysis attacks, safeguarding social media publishers' identity and privacy[103].

Data obfuscation can help in compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and other industry-specific regulations, is a legal requirement for businesses. Data obfuscation helps companies meet these compliance requirements by protecting sensitive data from unauthorized access or unintended disclosure, reducing the risk of regulatory fines, penalties, and legal liabilities[104].

Federated and distributed analytics in privacy and personal data protection in social networks. One additional drawback of OSNs is the lower quality of services. Recommender systems are typically used in OSNs to improve the services by recommending interesting content for users. To build a recommender system, a variety of data analytics techniques

[100] Zook, M.; Graham, M.; Shelton, T.; Gorman, S. Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake. *World Med. Health Policy* 2010, *2*, 7–33.

[101] De Montjoye, Y.A.; Shmueli, E.; Wang, S.S.; Pentland, A.S. openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLoS ONE* 2014, *9*, e98790.

[102] Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 111–125.

[103] KHADER M., KARAM M., Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis, 13 June 2023, from https://doi.org/10.3390/data8060105

[104] OvalEdge Team, What is Data Obfuscation and why is it important to your business?, May 09, 2023, from https://www.ovaledge.com/blog/data-obfuscation

(data mining and machine learning) can be applied. The application of these techniques to distributed data is called distributed analytics, where multiple entities process subsets of data and share collective insights[105]. However, applying distributed analytics in DOSNs while maintaining user privacy is challenging. Some research works proposed cryptography-based solutions, where the user data is encrypted, thus, protected throughout the process. These solutions employ secure multi-party computation[106], homomorphic encryption, and other cryptography primitives[107]. However, despite some improvements, the computational and communication overhead of these approaches remains high (per operation). Also, this overhead remarkably increases with the number of users in the system, which introduces scalability issues and renders these approaches impractical for large-scale applications, such as OSNs.

Data accountability tools include accountable systems, threshold secret sharing, and personal data stores. These tools do not primarily aim to protect the confidentiality of personal data at a technical level and are therefore often not considered as PETs in the strict sense. However, these tools seek to enhance privacy and data protection by enabling data subjects' control over their own data, and to set and enforce rules for when data can be accessed. Most tools are in their early stages of development, have narrow sets of use cases and lack stand-alone applications[108]. In Articles 16 and 17 of the GDPR, data subjects have the right to rectify, be forgotten, and withdraw their consent at any time. Although some PDS platforms might allow users to exercise some of these rights, there are situations where it could be difficult or impossible to achieve that, especially in a decentralised environment. GDPR enforces data processors to be transparent. This includes purpose specification, recipient, transfers, and salient details of automated processing. Thus, personal data store platforms need to provide mechanisms to show the potential risks related to data access, processing, and sharing[109].

Barriers for adoption. Despite the large number of PETs and the wide opportunities they open up for companies, in particular, social network services in the context of

[105] WAINAKH A., Dissertation on Privacy-Enhanced Distributed Analytics in Online Social Networks, 21 March 2022, from https://tuprints.ulb.tu-darmstadt.de/21034/1/2022-02-07_Wainakh_Aidmar.pdf

[106] TASSA, T. Secure mining of association rules in horizontally distributed databases. IEEE Transactions on Knowledge and Data Engineering 26, 970– 983 (2014).

[107] CHAHAR, H., KESHAVAMURTHY, B. N. & Modi, C. Privacy-preserving distrib- uted mining of association rules using Elliptic-curve cryptosystem and Shamir's secret sharing scheme. *Sadhana - Academy Proceedings in Engi- neering Sciences* 42, 1997–2007 (2017).

[108] OECD Papers, Emerging privacy-enhancing technologies, Current regulatory and policy approaches, March 2023, from https://www.oecd-ilibrary.org/docserver/bf121be4

[109] KHALID U., BARHAMGI M., PERERA C., Personal Data Stores (PDS): A Review, 28 January 2023, from https://doi.org/10.3390/s23031477

compliance with personal data protection regulations, there are still factors that create obstacles for the comprehensive implementation of these technologies.

One such barrier is general knowledge and awareness of PETs[110]. While those researching the technologies are familiar with traditional privacy practices (such as anonymization, pseudonymization, encryption, and data minimization), it is unclear what PET can add to these approaches[111]. PETs include some of the most technically challenging and least used technologies to date, such as secure multiparty computing and federated learning. And while they may be among the most promising technologies for social media privacy compliance, the risk inherent in using new and poorly studied technologies is a strong barrier to their adoption[112]. PETs are subject to the relevant legal framework and existing regulators, such as the ICO in the UK. However, they are not specifically regulated as technologies, and their effectiveness is not fully understandable to non-experts. Nevertheless, professional certifications and online courses for privacy professionals could integrate the PETs training course into existing courses to increase awareness and expertise in the profession[113].

[110] London Economics and the Open Data Institute. 2022 Privacy Enhancing Technologies: Market readiness, enabling and limiting factors, The Royal Society, from https://royalsociety.org/topics-policy/projects/privacy-enhancing- technologies/

[111] Lunar Ventures (Lundy-Bryan L.) 2021 Privacy Enhancing Technologies: Part 2—the coming age of collaborative computing. From https://docsend.com/view/db577xmkswv9ujap?submissionGuid=650e684f-93eb-4cee-99e8- 12a92d5d88a0 (accessed 20 September 2022).

[112] London Economics and the Open Data Institute. 2022 Privacy Enhancing Technologies: Market readiness, enabling and limiting factors, The Royal Society, from https://royalsociety.org/topics-policy/projects/privacy-enhancing- technologies/

[113] British Computing Society (The Alliance for Data Science Professionals: Memorandum of Understanding July 2021). From https://www.bcs.org/media/7536/alliance-data-science-mou.pdf (accessed 2 September 2022).

5.2. Chapter II. Privacy by design and user held data model as a basis for Privacy and Personal Data protection in Social Networks

Organizations that process personal data, including online social networks, must determine how best to safeguard that data and how the data can and will be used throughout the data life cycle. The data life cycle involves every stage of data processing – from the moment it is collected, throughout its use and storage and until it is deleted. To properly initiate privacy by design and follow privacy engineering practices, it is necessary to understand the stages of the data life cycle. Since organizations have different levels of data use and types of technology used to process personal data, the finer details of each stage will vary from organization to organization. Typically, privacy professionals identify five stages in the data life cycle: collection; use; disclosure; retention, and destruction.

Privacy by design (PbD) is the concept of embedding privacy throughout the entire life cycle of processing personal data, including technologies, systems, processes, practices and policies, from early design state to deployment, use and ultimately disposal. Privacy should be incorporated into all levels of operations organically, rather than viewed as a trade-off or something to consider after a product, system, service or process has been built. Article 25(1)[114] stipulates that controllers should consider DPbDD early on when they plan a new processing operation. Controllers shall implement DPbDD before processing, and also continually at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards. DPbDD also applies to existing systems that are processing personal data[115].

From PbD to the user held data model. Due to the specifics and types of privacy violations in social networks (which we have previously divided into internal, external and constructed), the following model of dealing with personal data is a kind of protection against internal and some external violations. Since personal data, no matter how protected, can always be used - for example, displayed images, however, the data provided to the service during registration or while working with the service (meta data) can be reliably protected by using the user held data model, which can provide protection against internal violations.

[114] GDPR text, Article 25 GDPR. Data protection by design and by default, from https://gdpr-text.com/uk/read/article-25/

[115] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2022, from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de

To describe the human-centric (user held) data model, it is necessary to pay attention to the following aspects: the preconditions that create the need for its introduction, the concept of the model itself (term and philosophy), its main features and advantages that can be used for data protection in social networks.

Regarding preconditions. The development of existing markets of goods and services, online social networks and, as a result, an increase in the number of communications has led to an increase in the number of personal data processing. This has led to the accumulation of a large amount of data in large companies (such as GAFA[116]). Such processing, of course, required regulatory regulation, which was embodied in the adoption of such acts as GDPR, CCPA, and the California Privacy Rights Act ("CPRA)".

Nevertheless, with the effort to regulate the approach to personal data processing, new regulations brought with them new requirements, such as the right to be informed, the right of access, the right to rectification, erasure, restrict processing, data portability and others. This approach is correct, as it ensures the rights of consumers, however, it does not solve all problematic issues. These problems can be conditionally divided into two categories: a) those that arise in relation to companies – as new regulations mean increased compliance costs; b) in relation to consumers - in relation to the convenience of managing their data, the ability to manage them as much as their nature allows, and not the legal framework and market needs. That is why a new approach to managing data (user-held data model) was proposed.

The concept. User held data model primarily involves the creation of a separate personal data cloud. This cloud is filled with data due to the connection (linking) to it of various data sources - smartphones, smartwatches, personal computers, IoT, accounts, etc. Thus, all data about and generated by the data subject (in particular metadata in social networks) will be placed in a personal environment inaccessible to third parties. An important factor is that after entering the cloud, these data will be automatically unified in one format, which greatly simplifies their perception (which is difficult, for example, to achieve when making inquiries about the users information used in large companies where this information is simply unreadable). And another feature, perhaps the most important from the point of view of data protection, is that third parties will be able to access certain data only based on the consent of the data owner. Applications will be able to run locally on top of the cloud, which will minimize the use of data to only those that are really

[116] Whats.com, GAFA (the big four) – definition, Compliance, risk and governance, May 2019, from https://www.techtarget.com/whatis/definition/GAFA

necessary for the correct operation of the application and which will be understandable to the user at the same time.

If we try to define this model in one term, it is the closed cloud service that is filled with some personal- and meta data, unifies data in a single, understandable format for the data owner and gives the owner the opportunity to independently make decisions about the use or prohibition of the use of data by third parties.

The idea is proposed by Prifina company, which is building an ecosystem that is based on the user-held data. It is stated, that it is the technological architecture where each individual is able to connect various data sources to one's own "personal data cloud". The core principle of the user-centric, user-held data model is that the individual should have full ownership and control over their personal data. The main principles are: ownership of user-held data, consent and control, purpose limitation, data minimization, lawfulness, fairness, and transparency, security of personal data, data interoperability[117].

As the study "The Future of International Data Transfers" by Paulius Jurcys, Marcelo Corrales Compagnucci and Mark Fenwick shows, user held data models mostly deals with data created within wearable devices with sensors measuring location, daily steps, heart rate, and capturing numerous other physical parameters[118]. Nevertheless, there still is a huge amount of metadata generated in social networks.

Facebook's policy on metadata is to collect, use, and share metadata in order to provide and improve its services. Metadata refers to information that is generated or collected about a user's activity on Facebook, such as the time and date of posts, likes, comments, and other interactions. However, such data, in accordance with OMB Circular No. A-130, where under the term Personally Identifiable Information (PII) we should understand information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, – may also be interpreted as personal data.

This means that the default personal data protection model, namely the user-held data model, can and should be applicable to this data as well, since its owner is not the company or service, but the user who generated it. Such information is useful and profitable for the service, and therefore should not by default be transferred to the ownership or use

[117] JURCYS P., User-Centric, User-Held Data Model: Key Principles, Medium, Aug 3, 2020, Published in Prifina, from https://medium.com/prifina/user-centric-data-model-key-principles-d02a69cf45d0

[118] JURCYS P., COMPAGNUCCI M.C., FENWICK M., The future of international data transfers: managing legal risk with a 'user-held' data model, The Computer Law and Security Review, Vol. 46 (2022), 17 Jan 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4010356

of social network services. Facebook is no exception, almost all companies collect meta data, such as: Telegram[119], WhatsApp[120], Snapchat[121], Viber[122] and many others.

A recurring theme of such a model is the empowerment of individuals with user-friendly, privacy-preserving tools that grant individuals more personal agency and control over data-driven consumer products and, by extension, their lives, and at the same time help companies shift away from product-centred business models and offer a stickier yet friction-free customer experience, in particular – in social networks.

Features. The main features of the user-centric, user-held data model are: personal data ownership, which assumes that the owner of personal data keeps all his data in his own cloud environment - in fact, what he generates remains in it, and not on the server or elsewhere. The second feature is that personal data is private by default, because although generated by applications, it remains effectively private by being placed in a secure environment without access by third parties. The third feature is data usage limits, which are reduced because the owner himself decides whether to provide this data and clearly understands the purpose of its use. This also includes the owner's own consent to the use of meta data, the legality of its use in accordance with GDPR, CCPA, CPRA, data security and data portability.

Advantages. The main advantages in this case can be divided into several categories:

a) advantages for data owners (which were mentioned above);

b) advantages for businesses (trading platforms, applications, service providers, etc.), which will not make a need to invest a lot of money in order to ensure compliance of their activities in accordance with the law;

c) for the state, since the user-held data model will ensure compliance with the relevant array of legal norms in the field of personal data protection;

d) advantages for providers of cloud provisioning and maintenance services, because most likely, if the user-held data model becomes widespread, it will improve and new challenges will arise in relation to its development.

Conclusions. The proposed model of personal data protection aims to create conditions under which service providers will not be able to use user-generated data by

[119] Telegram Privacy Policy, 8 July 2023, from https://telegram.org/privacy/ua

[120] Meta, Help Center, What information does WhatsApp share with the Meta Companies?, from https://faq.whatsapp.com/1303762270462331

[121] Snapchat Support, About Snap and Chat Metadata, from https://help.snapchat.com/hc/en-gb/articles/7012318664852-About-Snap-and-Chat-Metadata

[122] Rakuten Viber, Viber Privacy Policy, August 22, 2023, from https://www.viber.com/en/terms/viber-privacy-policy/

default. Ownership of personal data belongs to the user, and the existing practice of collecting and using meta data by default, although provided for in the Agreement with the user, is rather unavoidable, since such agreements are accession agreements, and without some services it is almost impossible to conduct work, which puts puts the user in a hopeless situation and thereby forces him to join the existing terms of use. Although the user held data model itself was invented for application to data from a wearable device, in our opinion, it is able to offer the greatest popularity and practical benefit precisely in the context of social networks, since it can completely change the approach to understanding personal data and ensure compliance with the requirements of legislation in areas of personal data protection. In addition, this model is able to minimize the risk of cross-border transfer of personal data and the number of internal violations by social network services.

CONCLUSIONS AND PROPOSALS

Having studied the legal mechanisms of Privacy and Personal Data protection as well as Privacy Enhancing Technologies in the legal context, we can draw the following conclusions:

1) The general term Privacy is equally applicable in the context of social networks as in other areas. However, the components of the Right to Privacy in social networks are still different in nature and may include certain powers that are specific only to users of social networks. These include specific technical protection of personal data and information shared by individuals on social networks – exposed data, the right to file complaints and seek remedies if their privacy rights are violated by social networks – which should include, in particular, internal mechanisms for submitting such applications within the networks, comprehensive privacy policies, outlining the types of personal data collected, the right to access their personal data held by social networks and the right to rectify any inaccuracies or errors.

Privacy in social networks as an object for the protection should be characterized as a state of inviolability of a person's private life in social networks, where both a person's interests arising from the concept of the right to privacy and social networks benefits can be freely satisfied. When creating conditions under which there is no possibility to protect your private life, social networks will continue to exist, however, privacy can then be forgotten. If the provision of social network services is regulated too much, privacy will be fully protected, but the nature of social networks themselves would be taken. Therefore, there must be a proper balance that allows both to receive the benefits of the networks themselves, while at the same time ensuring the conditions under which the right to privacy cannot be violated;

2) The specifics of violations in the field of Privacy and Personal Data is that there is a strong connection between data protection (in legal context) and information security (technical measures). In order to qualitatively distinguish the violation of privacy or personal data in social networks, it should be distinguished from other risks in social networks. It is recommended to divide risks into three categories: security incident, privacy incident and data breach;

3) International organizations and states have chosen different approaches to the regulatory regulation of Personal Data protection, and therefore to the protection of Personal Data and Privacy in social networks.These include such regulation models as comprehensive, sectoral, co-regulatory, and self-regulation models. Each of the models is

effective in its own way, but the most popular in the Personal Data protection sector is the comprehensive approach, which allows for a more unified regulation of Personal Data protection in social networks. Nevertheless, as shown by the practice of using social networks and the legislative practice itself, the protection of Personal Data in social networks is often carried out precisely in a combination of comprehensive and sectoral legislation - such as in the EU, where in addition to the GDPR, the provisions of the ePrivacy Directive, NIS2 Directive, etc. are applied. Self-regulation models include Privacy Policies and User Agreements, which can provide additional guarantees for the user of social networks;

4) The framework norm to which the privacy policy must comply is Article 12 of the GDPR, which contains blanket norms to which it refers in turn. The legal nature of the privacy policy is due to the fact that it is an informative document and does not create rights and obligations for the parties, it only informs the client about how his data is protected, used, transferred, etc. Therefore, the critical question to be clarified is: a) whether such a policy (notice) is developed within the social network documentation (pursuade to Article 12 and 13 of the GDPR) and b) whether its content and availability meet the requirements of Article 12 of the Regulation;

5) The practice of the ECHR and national DPA is important in the context of preventing violations of privacy and personal data in social networks by the state and its public bodies. The state, as an interested party, has an interest in having access to the personal data of users of social networks, but the limits of the legality of such an interest must be formed on the basis of a legitimate goal - namely the protection of public or state interests and only in compliance with the legal procedure, which must be clearly regulated, substantiated, and act without violation of human rights, with observance of the balance of private and public interests. The cases of Ekimdzhiev and Others v. Bulgaria, Big Brother Watch and others v. the United Kingdom and Glukhin v. Russia is an example of such an interest of states, which should result in an immediate response of civil society, international human rights organizations and the states themselves, as they act as a negative example of legislative approach;

Decisions of DPAs, in turn, (including concurring or dissenting opinions) establish influential or persuasive precedent outside its jurisdiction. Such decisions may strongly impact on other EU Data Protection Data Protection Authorities' approach towards different issues in the context of social media platforms. Mostly they deal with internal Privacy and Personal Data violations in social networks, as it was shown by Meta, TikTok, YouTube and other examples.

6) PETs as a collection of digital technologies and approaches that permit collection, processing, analysis and sharing of information while protecting the confidentiality of personal data play an important role in the protection of Personal Data of users of social networks and also contribute to ensuring compliance with the legislation on personal data protection in general. However, despite the large number of PETs and the wide opportunities they open up for companies, in particular, social network services in the context of compliance with Personal Data protection regulations, there are still factors that create obstacles for the comprehensive implementation of these technologies. Professional Certification as well as further study of these technologies, as well as their popularization as a means of data protection in social networks is recommended;

7) Ownership of personal data should belong to the user, and the existing practice of collecting and using meta data by default is unavoidable, since user agreements are accession agreements, and without some services it is almost impossible to conduct profession or social life, which puts puts the user in a desperate situation and thereby forces to join the existing terms of use. The user held data model itself was invented for application to data from a wearable device, but it is able to offer a great practical benefit precisely in the context of social networks, since it can completely change the approach to understanding personal data and ensure compliance with the requirements of legislation in areas of personal data protection. In addition, this model is able to minimize the risk of cross-border transfer of personal data and the number of internal violations by social network services.

LIST OF REFERENCES

Legal normative acts

1) Universal Declaration of Human Rights. Adopted and proclaimed by UN General Assembly Resolution 217 A (III) of 10 December 1948 Text: UN Document A/810, p. 71 (1948).

2) International Convenant on Civil and Political Rights (1967). [1976] UNTSer 141;999 UNTS 171.

3) European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 3 November 2023].

4) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

5) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

6) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

7) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

8) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

9) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

10) SHIELD Act, July 25, 2019, from https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

11) The United States Constitution (1787), 1th, 3th, 4th, 5th, 9th Amendment, from https://constitution.congress.gov/constitution/amendment-4/.

12) Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

13) Circular No. A-130, Revised, (Transmittal Memorandum No. 4) (November 28, 2000)

14) California Consumer Privacy Act (CCPA) (2018), from https://oag.ca.gov/privacy/ccpa.

15) Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), from https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

16) Communications Decency Act of 1995, S. 314 (IS)

17) The California Consumer Privacy Act of 2018, from November 2020, from https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/

18) Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

19) Codice in materia di protezione dei dati personali, 10 agosto 2018, from https://www.garanteprivacy.it/codice

20) Data Protection Act (2018), from https://www.legislation.gov.uk/ukpga/2018/12/cont

21) Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. From https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

22) Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14/08/2018, from https://www.gov.br/mds/pt-br/acesso-a-informacao/governanca/integridade/campanhas/lgpd

23) La loi Informatique et Libertés, December 17. 2015, from https://www.cnil.fr/fr/la-loi-informatique-et-libertes

24) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000, 2018-05-25, from https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

25) China’s Cyber Security Law (CSL), Passed November 6, 2016. Effective June 1, 2017, from https://www.informatica-juridica.com/ley/chinas-cyber-security-law-csl/

26) Personal Information Protection Law of the People’s Republic of China, 21st October 2020, from https://personalinformationprotectionlaw.com

27) Digital Advertising Alliance, DAA Self-Regulatory Principles, June 2023, from https://digitaladvertisingalliance.org/principles

Special literature

1) BARKAR D., Almost The Media. How Telegram Manipulates The Audience, 23.11.2022, from https://imi.org.ua/monitorings/majzhe-zmi-yak-telegram-manipulyuye-audytoriyeyu-i49222

2) BERRIORS S., Social Media and Privacy, Modern Socio-Technical Perspectives on Privacy, 2022, from https://www.academia.edu/76360943/Social_Media_and_Privacy

3) BULAVKO A.. Technical Review of End-to-End Encryption in Mobile Social Networks. Published 2018/01/05, from https://arturasbulavko.com/documents/E2EE_In_MSN.pdf.

4) Burke, Moira, and Robert E. Kraut. 2016. The relationship between Facebook use and well-being depends on communication type and tie strength. *Journal of Computer-Mediated Communication* 21 (4): 265–281.

5) Burke, Moira, Robert Kraut, and Cameron Marlow. 2011. Social capital on Facebook: Differentiating uses and users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 571–580.

6) CHAHAR, H., KESHAVAMURTHY, B. N. & Modi, C. Privacy-preserving distributed mining of association rules using Elliptic-curve cryptosystem and Shamir's secret sharing scheme. *Sadhana - Academy Proceedings in Engi- neering Sciences* 42, 1997–2007 (2017).

7) CLULEY, G. Fugitive John McAfee's Location Revealed by Photo Meta-Data Screw-Up. Available online: https://nakedsecurity.sophos.com/2012/12/03/john-mcafee-location-exif/
Columbia Univerity, Italian Data Protection Authority v. TikTok, Case analysis, from https://globalfreedomofexpression.columbia.edu/cases/italian-data-protection-authority-v-tiktok/

8) COOLEY, T. A Treatise on the Law of Torts or the Wrongs which arise independent of contract. Chicago: Callaghan, 1888.

9) Coursaris, Constantinos, Wietske Van Osch, Jieun Sung, and Younghwa Yun. 2013. Disentan- gling Twitter's adoption and use (dis)continuance: A theoretical and empirical amalgamation of uses and gratifications and diffusion of innovations. *AIS Transactions on Human-Computer Interaction* 5 (1): 57–83.

10) DAVID YOUNG LAW, Privacy Commissionerseeks court order against Facebook, 2018, from https://davidyounglaw.ca/compliance-bulletins/privacy-commissioner-seeks-court-order-against-facebook/. A version of this article was originally published by The Lawyer's Daily (www.thelawyersdaily.ca), part of LexisNexis Canada Inc.

11) De Montjoye, Y.A.; Shmueli, E.; Wang, S.S.; Pentland, A.S. openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLoS ONE* 2014, *9*, e98790.

12) Digital Citizenship and Surveillance Society, 4th March 2016, Cardiff University, from https://dcssproject.net/tempora/index.html

13) DITTMAR, E. C.; JINÉNEZ, D. L.; PORTILLO, P. V. *Safeguarding Privacy in Social Networks*. The Law, State and Telecommunications Review, Brasilia, v. 12, no. 1, p. 58-76, May 2020. DOI: https://doi.org/10.26512/lstr.v12i1.31238.

14) DIXON S.J.. Social media – Statistics & Facts. Published August 31, 2003, from https://www.statista.com/topics/1164/social-networks/

15) DULLEA A., BEEBE M., Zoom's Popularity Leads to New York Investigating Its Security Flaws, May 18, 2020, Byte Back – Husch Blackwell`s Data Privacy and Cybersecurity Legal Resource, from https://www.bytebacklaw.com/2020/05/zooms-popularity-leads-to-new-york-investigating-its-security-flaws/

16) European Commission, What are Data Protection Authorities (DPAs)? Article 4(16), Chapter VI (Articles 51 to 59) and Recitals (117) to (123) of the GDPR, from https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

17) European Data Protection Board, EDPB Chairmanship, from https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en

18) Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, September 4, 2019, from https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

19) How YouTube processes personal data, effective date: November 24, 2020, from https://www.youtube.com/t/terms_dataprocessing

20) Internet surveillance after Snowden: A critical empirical study of computer experts', November 2017, Journal of Information Communication and Ethics in Society 15(1)

21) JURCYS P., COMPAGNUCCI M.C., FENWICK M., The future of international data transfers: managing legal risk with a 'user-held' data model, The Computer Law and Security Review, Vol. 46 (2022), 17 Jan 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4010356

22) JURCYS P., User-Centric, User-Held Data Model: Key Principles, Medium, Aug 3, 2020, Published in Prifina, from https://medium.com/prifina/user-centric-data-model-key-principles-d02a69cf45d0

23) KHADER M., KARAM M., Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis, 13 June 2023, from https://doi.org/10.3390/data8060105

24) KHALID U., BARHAMGI M., PERERA C., Personal Data Stores (PDS): A Review, 28 January 2023, from https://doi.org/10.3390/s23031477

25) KOERNER K., LALONDE B., Cheering emerging PETs: Global privacy tech support on the rise, iapp, The Privacy Advisor, January 24, 2023, from https://iapp.org/news/a/cheering-emerging-pets-global-privacy-tech-support-on-the-rise/

26) London Economics and the Open Data Institute. 2022 Privacy Enhancing Technologies: Market readiness, enabling and limiting factors, The Royal Society, from https://royalsociety.org/topics-policy/projects/privacy-enhancing- technologies/

27) MAROTTA-WURGLER F., Understanding Privacy Policies: Content, Self-Regulation, and Markets, NYU Law and Economics Research Paper No. 16-18, January 3, 2016, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513

28) Meta Business Help Centre, How does Lei Geral de Proteção de Dados Pessoais (LGPD) affect advertising on Facebook?, from https://en-gb.facebook.com/business/help/32711141831

29) Naeem A. Nawaz, Kashif Ishaq, Uzma Farooq, Amna Khalil, Saim Rasheed, Adnan Abid, and Fadhilah Rosdi, A comprehensive review of security threats and solutions for the online social networks industry, 16 January 2023, from https://peerj.com/articles/cs-1143.pdf
Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 111–125.

30) NEWTON C., Everything you need to know about Section 230, Dec 29, 2020, from https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation

31) OECD Papers, Emerging privacy-enhancing technologies, Current regulatory and policy approaches, March 2023, from https://www.oecd-ilibrary.org/docserver/bf121be4

32) OneTrustDataGuidance (Regulatory Research Software), China: CAC fines Didi RMB 8 billion for CSL, DSL, and PIPL violations, 21 July 2022, from https://www.dataguidance.com/news/china-cac-fines-didi-rmb-8-billion-csl-dsl-and%C2%A0pipl

33) P. J. Wisniewski and X. Page, Privacy Theory and Methods. Published June 29, 2021. From https://doi.org/10.1007/978- 3- 030- 82786- 1.

34) RISKOPTICS, 9 Common Types of Security Incidents and How to Handle Them. From https://reciprocity.com/blog/common-types-of-security-incidents-and-how-to-handle-them/
Sharp Cookie Advisors, Schrems II a summary – all you need to know, 23 November 2020, from https://www.gdprsummary.com/schrems-ii/

35) SKURNIK T., Future transfers of personal data outside the EU, Nordia Law, 29.05.2023, from https://nordialaw.com/insights-data-privacy/

36) SOVEREN, What is a privacy incident? Mar 2, 2022, from https://soveren.io/blog/what-is-privacy-incident

37) Tabassum Tamboli, Aditya Shende, Archana Varade. Impacts of Vulnerabilities on Security and Confidentiality in Online Social Networks along with Preventive Measures. Special Issue - 2020 International Journal of Engineering Research & Technology (IJERT). From https://www.ijert.org/research/impacts-on-security-and-confidentiality-in-online-social-networks-along-with-preventive-measures-IJERTCONV8IS05038.pdf

38) TASSA, T. Secure mining of association rules in horizontally distributed databases. IEEE Transactions on Knowledge and Data Engineering 26, 970– 983 (2014).

39) The Gurdian, UK-US surveillance regime was unlawful ‘for seven years’, February 2015, from http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa [1] The Guardian, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', from https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

40) VOIUTA D., Photos From Social Networks In The Media: Where Is The Privacy Line? December 10, 2021, Centre of Democracy and Rule of Law, from https://cedem.org.ua/consultations/foto-z-sotsmerezh-u-media/

41) WONG L.. 9 Types of Social Media and How Each Can Benefit Your Business. Published September 2, 2021, from https://blog.hootsuite.com/types-of-social-media/

42) Zook, M.; Graham, M.; Shelton, T.; Gorman, S. Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake. *World Med. Health Policy* 2010, *2*, 7–33.

43) WAINAKH A., Dissertation on Privacy-Enhanced Distributed Analytics in Online Social Networks, 21 March 2022, from https://tuprints.ulb.tu-darmstadt.de/21034/1/2022-02-07_Wainakh_Aidmar.pdf

44) Cambridge Dictionary, from https://dictionary.cambridge.org/dictionary/english/data-protection.

Court and DPA practice

1) CASE OF EKIMDZHIEV AND OTHERS v. BULGARIA, ECHR, (Application no. 70078/12), from https://hudoc.echr.coe.int/#_Toc92116208

2) CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM, 25 May 2021, from https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-210077%22]%7D

3) CASE OF GLUKHIN v. RUSSIA, ECHR, 04/10/2023, Final Judgement.

4) Resolution of the Supreme Court of Ukraine, court proceedings: 61-21960sk18, January 30, 2019, from https://reyestr.court.gov.ua/Review/79744914

5) Decision of the Kyiv District Court of Odessa, Proceedings No. 2/520/3686/18. From https://reyestr.court.gov.ua/Review/75030458

6) Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems Request for a preliminary ruling from the High Court (Ireland), from https://curia.europa.eu/juris/liste.jsf?num=C-311/18

7) In Re: Zoom Video Communications, Inc. Privacy Litigation., Case No. 5:20-CV-02155-LHK (D. Cal. Oct. 21, 2021) (order granting preliminary approval of class action settlement)

Case No. 5:20-CV-02155-LHK (D. Cal. Oct. 21, 2021) (order granting preliminary approval of class action settlement)

8) Federal Trade Comission, FTC Matter/File Number 1923258, Civil Penalties, from https://www.ftc.gov/legal-library/browse/cases-proceedings/1923258-microsoft-corporation-us-v

9) Complaint at 3-7, *In the Matter of Zoom Video Communications, Inc.*, Docket No. C-4731 (Federal Trade Commission) and *In Re: Zoom Video Communications, Inc. Privacy Litigation.*,

10) Complaint at 3-7, In the Matter of Zoom Video Communications, Inc., Docket No. C-4731 (Federal Trade Commission) and In Re: Zoom Video Communications, Inc. Privacy

11) Complaint at 6, Cullen et al v. Zoom Video Communications, Inc., Case No. 5:20-cv-02155-SVK (D. Cal. Mar. 30, 2020).

12) Consent Order at 3-7, In the Matter of Zoom Video Communications, Inc., Docket No. C-4731 (Federal Trade Commission); Letter Agreement between Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020)

13) Letter Agreement between Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020)

14) Office of the Privacy Commissioner of Canada, Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, April 25, 2019, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206.

15) Office of the Privacy Commissioner of Canada, Privacy Commissioner appeals Federal Court decision related to Facebook investigation, May 12, 2023. From https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230512-2/
Zoom and the NYAG, State of New York Office of the Attorney General (May 7 2020)

Normative documents

1) Google Privacy Policy, November 15, 2023, from https://policies.google.com/privacy?hl=en#inf

2) Rakuten Viber, Viber Privacy Policy, August 22, 2023, from https://www.viber.com/en

3) Telegram Privacy Policy, 8 July 2023, from https://telegram.org/privacy/ua.

4) Terms of use, You Tube, January 5, 2022, from https://www.youtube.com/static?temp

5) You Tube Privacy Policy, valid from November 15, 2023, from https://policies.google.com/privacy?hl=uk

SUMMARY

Protection of Privacy and Personal Data in Social Networks

Rostyslav Prystai

The Master's Thesis reveals the pecularities of Privacy and Personal Data protection in social networks. The stydy analyzes the legal mechanisms of such protection - namely, regulatory and institutional. Analysis of Privacy and Personal Data protection mechanisms in social networks is made through the prism of normative approaches to Personal Data protection. Some of the models are comprehensive (unified), while others are aimed at industry-sectoral protection due to the specifics of the object of legal protection. Therefore, the work also describes 1) the specifics of Privacy and Personal Data as categories subject to protection in social networks; 2) the pecularities of social networks environment in the context of Privacy risks and violations, which will justify the need to combine both a unified and sectoral approach to the regulation of relevant legal relations.

In order to study the effectiveness of organizational mechanisms for the protection of Personal Data within the framework of the European Union, the practice of national Data Protection Authorities was studied, which, after the entry into force of the provisions of the GDPR, has a significant impact on the activities of social networks in the EU. The relevant practice of the ECHR was also studied, which reveals the specifics of privacy violations in social networks by the state - the obtained results can further be applied in justifying the need to introduce additional guarantees of Privacy protection for users of social networks in public legal relations.

Separately, privacy-enhancing technologies, as an instrument to ensure compliance with existing Data Protection legislation, are investigated. The concepts and features of the Privacy by design concept and user-held data model, as a tool that is quite effective in creating a Privacy by design environment, are revealed.