A MATTER OF UNDERSTANDING DIGITAL RIGHTS

Kharytonova Olena
Doctor of Law, Professor, Corresponding Member of the National Academy of Sciences of Ukraine, Head. the Department of Intellectual Property and Patent Justice National University "Odessa Law Academy"
ORCID ID: 0000-0002-9681-9605

Tokareva Vira
Candidate of Law, Associate Professor, Associate Professor of the Department of Civil Law, National University "Odessa Law Academy"
ORCID ID: 0000-0002-8409-1477

Abstract.

The paper demonstrates that digital changes in society call for a theoretical rethinking of traditional legal concepts and the creation of a legal mechanism to regulate, implement, and safeguard subjective rights and obligations of a natural person in a digital environment. The enjoying of individuals rights at the national and international level is directly impacted by digital transformation. An evolution of law is triggered by the emergence of a digital economy and the intensive development of digital technologies, which has already been expressed in the appearance of new objects of law, forms of law, ways of implementing the right, and so forth. The influence of digital technology is leading to the transformation of law, as evidenced by these events. As a result of digital transformation, individuals' rights and duties as participants in the digital space are evolving. The study examines the emergence of new rights that are justified by the development of digital society. Such as: the right to digital identity, the right to privacy on the network, the right to be forgotten, the right to offline or the right to disconnect, the right to be informed about interaction with AI, etc.

The category of "digital rights" is used in the context of digital society and the digital economy. However, the meaning of this concept is not consistent. Digital rights are understood as universal human rights adapted to the conditions of the information society, in particular the right to privacy, the right to exchange information, the right to freedom of expression on the network, the right to access the electronic network. The term 'rights to communicate' or 'rights to information' is used to mean the same thing as 'digital right', but there is no clear distinction between them. The attempt to provide clarification between this definition are made in this paper.

The development of digital law is now underway to create a set of legislative acts that govern legal relations that are happening in the digital environment. The development of legal acts to handle digital things, the ethical use of artificial intelligence and big data, strict regulation of remote automatic identification of individuals by biometrics, and the growing importance of an anthropocentric approach in the use of technologists, etc. are all related to this process.

The proposal suggests that digital rights, which are subjective rights, should be perceived as a combination of property and non-property rights that safeguard a person's capacity to operate in digital (virtual) space.

Keywords: digital rights, Internet rights human rights, AI, moral rights, Big Data, digital identity, Internet of Things, right to be forgotten, privacy.

Methodology.

The study's methodology included a set of legal methods that were both general and specific, such as the formal-logical method, method of analysis and synthesis and comparative legal method. The use of the formal-logical method enabled the exploration and consideration of digital rights as a distinct group of human rights for a new generation. Additionally, it enabled the analysis of international legal acts pertaining to the management of the Internet, the protection and implementation of human rights on the Internet. Through the formal-logical method, the necessity to distinguish between digital rights and information rights was established as a wider set of rights that are required for the normal existence, development, and satisfaction of information needs in different areas of public life.

The use of the method enabled the definition of digital rights to be improved.

The analysis and synthesis method played a significant role in the study, making it possible to analyze individual digital rights. Digital rights are understood to be a group of both tangible and intangible rights that ensure a person's ability to function in digital (virtual) space and establish their legal personality in a digital environment. The use of the methodology allowed to identify and analyze the specifics of individual digital rights as an element of a person's legal personality, namely: the right to digital identity, the right to privacy, the right to be forgotten, the right to be aware of automated processing and that the data subject interacts with the AI (agent), the right not to know. It has been proven that consolidating the right to access the Internet is insufficient for the effective implementation and harmonious development of digital rights in society. Definement and consolidation of rights and obligations at the legislative level is necessary for both individuals and legal entities.

The objective of the study is to examine digital law as a component of the human rights of a new generation, which is justifiable due to the advancement of digital society; analysis and identification of features of digital rights, in particular the right to digital identity, the right to privacy on the network, the right to be forgotten, the right to offline or the right to disconnect, the right to be informed about interaction with AI, etc.

Analysing the similarities and differences between the legal approaches used by states when regulating digital rights and freedoms can be done using a comparative legal method.

1. Digital rights as part of a new generation of human rights

The human rights generations concept is based on a generational approach and historical formation, that it is, division into fourth generations. The first generation of human rights, encompasses civil and political rights, is the basis for the institution of human rights (the right to life, the right to liberty and personal inviolability, the right to dignity, etc.). The second generation of human rights includes social, economic, and cultural rights, such as the right to work, rest, social security, medical care, and protection of motherhood and childhood. The third generation of human rights is called solidarity (collective) rights, that is, the rights of all mankind including human rights, the rights of peoples, the rights of the nation, the rights of community and association: the right to peace, security, the right to self-determination of peoples, etc [1].

The fourth generation of human rights began to form with the development of science, the increasing freedom and autonomy of man, particularly with the emergence of information technology and the increasing immersion of man in the world they created. The fourth generation of human rights comprises following the rights: right to change gender, organ transplantation, artificial insemination, child-free families, independence from state intervention etc.

The concept of the management human rights on the Internet was the first time applied at the World Summit on the Information Society in Geneva in 2003. Onward the concept of the human rights on the Internet acknowledged and support at the Tunisian meeting in 2005. The participants at the III Internet Governance Forum in Hyderabad (India) in 2008 unanimously concluded the necessity of the promotion and development of human rights and the principles on the Internet. The participants emphasized the importance of ensuring the enjoyment of human rights on the internet.

The Council of Europe's Committee of Ministers declared its human-centered and respects human rights prospect on the Internet that in Declaration on the Principles of Internet Governance in 2011. In 2012, the Council of Europe's Committee of Ministers established the Committee of Experts on the Rights of Internet Users, whose task was to implement existing human rights in the digital environment. In the Human Rights Manual for Internet Users, the Council of Europe emphasizes that children and young people have the right to education in order to acquire competence to protect themselves from Internet threats, as well as the right to special protection from threats through surfing and enjoying the Internet, including from sexual exploitation and violence, and other forms of crime.

The Committee of Ministers of the Council of Europe in its Recommendations CM/Rec (2014) 6 was mentioned that member states are required to guarantee the protection of human rights and fundamental freedoms outlined in the European Convention on Human Rights. The Recommendations emphasize that human rights and fundamental freedoms are equally applicable in both offline and online. No one shall be subject to unlawful interference with the exercise of their rights and fundamental freedoms while on the Internet, nor shall measures of general surveillance or information interception be extended. Interference with privacy in relation to personal data is permitted only in exceptional circumstances provided for by law, such as in the case of a criminal investigation. The value of the Internet as a public service cannot be overstated. The Internet is used by people, communities, public authorities, and private companies, and they are legally pursuing access to Internet services that are provided without discrimination, at a reasonable price, and are safe, reliable, and uninterrupted [2].

At the 32nd session of the UN on June 27, 2016, the UN Human Rights Council adopted a resolution "Promotion, protection and implementation of human rights on the Internet" [3], which states that the same rights that a person has in the offline space should also be protected in the online space.

Thus, a separate group of rights includes rights that assist enjoyment of the right on the Internet. These types of rights are called informational and defined as a set of rights related to the development of Internet, technologies and the formation of an information society [4, p. 156]. There are following informational rights: the right to access the Internet; the right to an enjoyment of the Internet; the right to balanced use of the Internet in everyday life; the right to freedom of speech and expression on the Internet; the right to education, knowledge and communication using the Internet. Digital rights are understood in the literature as a modern manifestation of information rights, which are protected by Articles 31, 32, and 34 of the Constitution of Ukraine [5].

Additionally, aforementioned category is suggested to introduce in the light of the Concept of recodification (update) of civil legislation of Ukraine published in 2020. In accordance with the second book "Personal non-proprietary rights" of the Concept is brought radical changes in context on non-proprietary rights in Civil Code of Ukraine. The author of the Concept is proposed to develop the updated Civil Code of Ukraine the provision on "digital rights" as a type of personal

non-proprietary rights. Digital personal non-proprietary rights are suggested to help enjoyment of individual rights in the digital space. However, the Concept does not specify the meaning behind 'digital rights' and does not specify which rights are encompassed by the concept of 'digital right'. We will go back to the understanding of digital rights as a civil law category at a later time [6].

It is important to acknowledge that there is some confusion in the terminology used by scholars dealing with relevant issues. The rights that technology grants or enjoys through the Internet are known as informational, virtual, digital, Internet rights, and rights to communication.

The question arises as to whether digital rights are included in information rights. In this sense, it should be taken into account that information rights existed before the advent of information and communication technologies, the actual formation of a digital space and the wide immersion in the virtual reality of a large number of people.Our belief is that it is essential to differentiate digital rights from information rights as a wider set of rights that pertain to human being. Information rights are crucial for successful existence, development and fulfil needs in various area of the public life [7].

The central object of both groups of rights is information. The provision of distinguishing and common features of digital and information rights is necessary for that reason. Scholars have pointed out that digital rights, have a lot in common with the right to information. However digital rights have their unique characteristics as it fulfils new sphere of human rights.

However, digital rights have their unique characteristics as they fill into a new sphere of human rights. The Internet allowed for existence of digital rights, but peculiarities of digital rights do not make them a fitting analogy with other phenomena that have occurred in human history. The provision of distinguishing and common features of digital rights and information rights is necessary for that reason.

To separate digital rights from information rights, it is important to note the following.

We believe that fundamental digital rights do not encompass: the right to access the Internet, the right to expression online, the right to privacy and protection of personal data, the right to freedom and personal security online, the right to peaceful assembly, association and/or use of electronic instruments of democracy, and the right to digital self-determination (or the right to be forgotten) [8]. We believe that different types of rights are blended in this division. This classification in some sense lead to confusion between information rights and digital rights.

Herewith, rights that granted access to information and exercise persons' right are informational. The category of rights that provides access to the Internet should be called, respectively, informational and network rights. In turn, information network rights are fundamental for the emergence of digital rights.

The fact that information space is different from the real world, and therefore requires different laws to be applied to it than to the real world. To be more exact, the digitalization has resulted in the creation of a virtual world, where the architecture (code) must abide by both the laws that apply in the physical world and the rules that are developed by the specificity of the digital space. All this has led to the development of the concept of digital rights.

Thus, group of rights that make it possible to operate on the network, create and use content, etc. are digital rights. There following digital rights: the right to freedom and security on the Internet, the privacy of personal data on the network, the right to receive benefits and benefits from content, the right to work on the network, the right to privacy, the right to freedom from surveillance, the right to use encryption, the right to protect virtual identity, the right to remain anonymous, the right to determine oneself digitally (or the right to be forgotten), etc.

In addition, the information component of these rights is also complemented by the communication component, which distinguishes them from information rights and network rights.

The concept of digital rights should focus on the peculiarities of the rights that a person obtains while being in the virtual space. In this sense digital rights are related to the field of modern information technologies, in particular the Internet.

Nowadays society deal with the formation and development of a digital ecosystem, that is, a new reality of the technological mankind. This ecosystem is consisted of following elements: distributed registry platforms (blockchain, etc.), Internet of Things, artificial intelligence and machine learning (AI), cloud services, smart devices (Smart Everything), Big Data, virtual and augmented reality, cybersecurity conditions, social networks and platforms (Facebook, Instagram etc.), electronic services. These elements have been a challenge in various spheres of human life for traditional legal rules and institutions. The emergence of these technologies requires adaptation of legislation to fit the upcoming new digital era.

Agreeing with the name of the specified group of rights as digital, we need to be cautious about the following aspects.

Along with the interpretation of "digital rights" in science, there is a discussion on the attribution of such rights to the rights of participants in virtual worlds. R. Koster, who developed the Declaration of Avatar Rights in 2000 on the basis of the Declaration of Human Rights, to establish and remind the "inhabitants" of virtual worlds of all kinds who have power over the virtual space, their rights and obligations. Avatar refers to the embodiment of a real person in the online space, and their statements, actions, thoughts, and emotions should be considered as valid as those of people in any other forum, venue, or space. According to the Declaration, avatars are viewed as individuals who possess the same freedoms. According to the scientist, the most important of these rights is the right to treat the avatar as a person. The avatar's rights are directly related to the duties of the administrator, thus the administrator does not responsible for the actions of the players [9].

E. Castronova provides for the following rights of a person endowed with a conscious mind: freedom of movement and association (persons must freely leave virtual worlds and enter them of their own free will, freely form their worlds into unique communities; protect themselves and their communities from harassment and abuse); freedom of input and output information (the ability to obtain a significant amount of information from the virtual world; which is not fraudulent; the ability to send and receive information from various sources, including outside the virtual world); freedom of speech, assembly and participation in political life (agents should be given the right to participate in the formation of policies that concern them, writing code that should be subject to the will of the people). Most of these rights are guaranteed in developed countries. On one hand additional attention to the consolidation of these rights could be superfluous. On the other hand, the common violation of above-mentioned rights observed its fragility and necessity to ensure in virtual world [10].

The weakness of ensuring of digital rights is connected both the failure assignment to a certain category of human rights that exist and legally regulated. There is also unified understanding of digital rights. Although there are lot of attempts to generate a clear definition. For example, O. V. Petrishin and O. S. Gilyaka propose understanding of digital rights as the expansion of universal human rights to the needs of a society based on information [11].

According to O. Bratasyuk and N. Mentukh, digital human rights are an autonomous group of human rights that are associated with the use and/or implemented on the Internet using special devices (computers, smartphones, etc.) [12].

Digital rights are also understood as a set rules of conduct that enshrines human rights and freedoms regarding the proper access and use of electronic devices, the possibility of creating, using and publishing digital works, as well as communication networks [13].

YU. Razmetaeva notes that the term 'digital human rights' actually covers two understandings. Firstly, it refers to all those rights, the exercise and protection of which is closely connected today with the use of digital tools or has a significant online component. Secondly, it refers only to those rights that emerge or begin to claim the status of fundamental in the digital era. Therefore, such fundamental rights as freedom of expression and speech, privacy, the right to information, the right to participate in the management of public affairs, etc., and such as the right to be forgotten, the right to anonymity or even the right to the Internet are also classified as digital [14, c. 19].

Lesko N., Antonov M. believe that from a practical point of view, digital rights should not be considered not an autonomous group of human rights (for example, as political, economic, social, etc.). Scholars suggest understanding digital rights as a conditional category that covers the peculiarities of the implementation and guarantees of the shield of fundamental human rights on the Internet [15].

Some researchers consider that digital rights derive from information rights. However, there are not identical to them. Despite their similarity, it is necessary to provide differentiation between these categories. Digital rights are also understood as the users' rights to access, to use, to create and to publish digital works, the right to free access on the Internet, to use computers and other electronic devices [16, c. 130].

Even a cursory review of existing points of view on the category "digital rights" indicates a lack of unanimity in their understanding.

Therefore, summing up, we can offer our own vision of concept of human rights in the digital space, which are associated with the use of digital technologies and electronic devices and are aimed at ensuring the security and autonomy of a person in this space.

Information and communication technologies allow users to collect, process, receive and transmit information at the local, national and international levels.

The network went through three stages of its development. The first was the creation of Web 1.0, a fairly limited functionality that allowed users to read information and buy things. In the early 2000s, thanks to the rapid development of new technologies, more powerful websites and more reliable web infrastructures appeared, which allowed users both consume data and publicly express their works through the Internet it. At the stage of Web 2.0, the Network was transformed into something more significant than a giant shopping center and an online encyclopedia. By allowing users to perform various actions on the Internet, it became the place where people could express themselves in different way. Web 3.0 technologies led to the emergence of a social network based on the new Facebook platform. Thanks to social platforms people are able to discuss and share information [17]. Thus, thanks to the Internet, social integration occurs as a process of forming relationships between individuals and groups. The emergence of social networks is a vivid illustration of this. It should be noted that the emergence of social networks is of great importance in developing a digital society that surpasses the number of internet users. It consistently approaches the development of artificial intelligence systems, where people are completely immersed in the network and stay there for a long time, working, learning, and communicating.

Therefore, the leading importance is acquired by social networks – such as social structures formed by individuals and entities in order to sharing information and communication. Through communication, a society can identify itself, inform its participants about intellectual communication, question information and communication, and determine whether excessive communication is permissible or unacceptable. [18]

Internet and telecommunication technologies contribute to the increasingly rapid virtualization of the modern world, which involves the transfer of human interests and activities into the virtual space. In this virtual realm, the importance of human communication through images, signs, and stereotypes is steadily increasing - which is what makes virtual reality unique. From the philosophical point of view, virtual reality is technically constructed with the help of technical means. This artificial reality is an interactive environment for generating and operating objects which is similar to real or imaginary ones. These objects could base on three-dimensional graphic representation, simulating their physical properties (volume, movement, etc.), simulating their ability to influence or independently presence in space.

In our opinion, digital rights can comprise a wide range of fundamental rights that are realized in a digital space. Therefore, analysis of digital rights should conduct by taking into account the characteristics of this environment. At the same time, basic digital rights are primarily derived from information rights, but they are not reduced to them. The digital rights mentioned below are observed by scholars today: the right to access information; the right to access information platforms and technologies; the right to protection of personal data (personal and biometric); the right to freedom of assembly and association online; the right to digital education and access to digital knowledge; rights related to the protection of genetic information; the right to participate in the turnover of property in the digital sphere; the right to be forgotten; the possibility of realizing personal, social, economic, political and cultural rights based on new technological platforms. That is, traditional and human rights distributed throughout the world are transformed, acquiring with new properties and content. Finally, a branch or generation of human rights that is exclusively focused on the digitalization process is established.

2. Digital rights as non-property rights of a private individual.

Let's reminisce about the Concept of updating civil legislation, where "digital rights" should be understood as a type of personal non-property rights, that will allow individuals to exercise their personal non-property rights and freedoms in the digitalization space [19].

Digital rights should recognize as an element of legal capacity of natural persons, which will allow him or her to perform various actions in this in the digital world. The harmonization of the development of digital rights in society cannot be achieved by consolidating or systematizing digital rights.

To successfully consolidate digital rights into legislation for individuals and legal entities, it is important to define and understand them.

From our perspective the concept of subjective rights in digital space should be viewed as a set of both property and personal non-proprietary rights that ensure the well-being and performance of a natural person in digital space.

Non-property digital rights are reported to encompass the right to digital identity, the right to digital death, the right to access the Internet, the right to information, the right to be aware of information about oneself (the right to know), the right to be forgotten, the right to anonymity, the

right to creativity on the Internet, the right to protect honour and dignity, the right to perform legally significant actions, etc.

B. Custers advocates for legal regulation of digital rights as a result of the rapid transition of various spheres of life to the Internet. The scholar lists the following digital rights that should obtain legal regulation: the right to digital identity the right to offline, the right not to know, the right to change of mind, the right to know the value of personal data, the right to a clean digital environment, the right to a protected digital environment, etc.

Consider some of these rights in more detail.

The right to digital identity is a new right that is generated by a person's immersion and, with the new ways and means for self-expression that the digital era provides. Through social networks, blogs, video platforms, and other sources, individuals can present themselves, modify their images, and express themselves digitally to the public through the entirety of the digital space. These technologies have made digital identity more dynamic at the same time. Individuals can use social networks to express themselves in various ways depending on the context and primary goal of the platform. Such possibilities that social platforms granted to their users permit to upload various digital profiles on the platforms [20]. Therefore, it is necessary to define the concept of identity.

Identity is a multifaceted concept that includes a person's idea of himself, values, beliefs, social roles and belonging to certain groups. In psychology, identity is associated with the awareness of one's own uniqueness, formed in the process of interaction with other people and the surrounding world.

Digital identity, according to A.V. Goncharova, is an edition of a person's social identity. This is an edition of data obtained as a result of an individual's of online activities, which can manifest itself in the form of a name, publications, comments, etc. [21, p. 187].

According to the definition of V.N. Morteza, by using the Internet, the individual person creates his own digital copy, which enjoy rights and freedoms in a virtual environment [22]. Similarly to the above positions, V.N. Mortez proposes to consider digital identity on the Internet as the creation and presentation of a person in a virtual space, which may coincide with the identity of a real individual or not coincide with it, in the case of creating a non-real, fake digital person [22].

O. Maksimenyuk believes that 'digital identity' encompasses all data about a person that exists in the information space. This data includes both the data publicly open by the individual about himself on the Internet and all data existed on the Internet, collected by social platforms and may regard this individual [23].

According to A. Kravchenko, the concept of 'digital identity' covers all data collected, stored and generated in the information space about a person, including personal data that can be collected without the person's consent. Scholar defines digital identity as a very broad concept, that is encompassed personal data, confidential and privacy data, and data on the interaction of a person in the Internet environment [23].

In line with common understanding the category of "digital identity", its encompassed personal data regarding an individual, a virtual or "digital" image (nickname, network name), an IP address and other data on the Internet. However, the understanding of digital identity is believed not to exhaust by mentioned components. Thus, S. Crawford observes that the concept of identity is broader than process of comparing a person with their digital identity, as it also encompasses other aspects. The way others perceive someone in games and virtual worlds determines his or her digital identity. Interaction and communication with other individuals during discourse are the means by which this identity is formed. Therefore, identity is closely related to reputation, being

formed by a certain group and in a certain context [24]. Thus, digital identity is not limited by amount of personal data. According to C. Crawford identity is a collective (group) project created in the process of communication during the person's expression and activity that identify him. However, the scholar does not provide distinguish between a digital identity and an avatar. According to C. Crawford an avatar has certain features, connections (relationships) and interests that have arisen as a result of his adventures in certain worlds, which are taken together as a "cloud" of reputation, experience and objective factors that make up its "identity". All of these elements cannot be predicted at the time of digital identity's birth or creation

The term digital identity is closely related to the category 'digital footprint', which encompasses data accumulated through using the Internet and social platforms, including geolocation tags, photos, videos, messages, search queries, passwords, card numbers, and posts on social networks. Digital footprint data can be a valuable resource for companies, teaching AI, political parties, marketing researchers, and others. It should be mention that the news evidences the frequent occurrence of personal data leaks, which is a weakness [25].

Digital identity and digital footprint are of high importance during an employment and applying for loans etc. Nowadays the trust in data about their clients, subordinates, and consumers on the Internet and social platforms is higher among commercial structures and government bodies than in data that individuals reveal about themselves. For example, credit history will be considered a more reliable argument than the filled and submitted questionnaire for financial institutions when making decision to grant or refuse a loan [26, p. 163].

The digital footprint is believed to be divide into three types of data.

The first type is the data that users reveal and publish about themselves and that allow to control and manage them. These types of data include publication or texting on social media and metadata: information through users' profile in social media (Telegram, YouTube, Facebook, Instagram, TikTok, Twitter, Viber), public and private messages, search queries, uploaded photos, videos, stories, tests and surveys in which users took part, visited websites and other results of conscious interactions in the network.

The second type of footprint of contains information that a person most likely does avoid to share with. For example, real time location (looking at the location trajectories that the devices show, companies can tell a lot about who a particular person spends their time with). It also tracks the content a person has viewed, the time users spent reading it, the keystroke dynamics, typing speed and finger movement on the screen. This is a solid basis for analysing human emotions and identifying psychological characteristics such as: character, temperament, inclinations, attitudes etc.

The third type of footprint is the result of interpreting and processing of the first and second type of footprints. Personal data is analysed with the help of various algorithms. All these data processing and comparing with data of other users to identify statistical correlations. By analysing such data, Big Tech companies can draw conclusions about the person, their activity, work, habits, and preferences. These algorithms processing data in order to predict certain data and aspects of person: this is his psychometric profile, IQ level, weaknesses, intentions, dependencies, family situation, diseases, small obsessions (for example, shopping, games, loans) and serious commitments (for example, investments, business projects). Individuals are often prevented from accessing these types of data due to its closed nature [26, p. 163].

The Initiation of Identification for Development should be mention in this regard. The Initiation suggests interpretation of the concept of Digital identity refer to a number of electronically recorded and stored properties and data that can uniquely identify a person [27].

Thus, the category of digital identity constitutes as the all data regarding a person in the digital space, namely: personal data, "digital trace", "digital reputation", data on interaction with other actors in the network and data about performed actions, even if they were removed from public access on the Internet, etc. Taking into account the aforementioned the right to digital identity should defined as the right on all above data.

There is narrow interpretation of digital identity as a profile of natural person on the Internet. The number of profiles (accounts) is currently unlimited. This opinion is shared by a number of scientists, including G. A. Terpstra [28]. Thus, the narrow meaning of digital identity is synonymous with digital profiles or accounts registered in private or state systems. The digital profiles are created by a person each time when registering in state or private systems. As the singularity process is achieved, the content of the digital profile will be enriched by attracting data from newly generated systems [29].

C. Crawford rises question, regarding the rights to digital identity. The scholar asserted that online tech companies that establish rules and terms of use that permit them to possess the digital identities of users and even dispose of them [30] According to K. Trotier corporations and companies both private and state, issue digital identity cards and monetize, obtaining personal data. That's why he suggested establishing rules that grant an individual the right to their digital identity and ensure protection of their personal data.

The scientist criticizes when corporations, not even the state, issue digital identity cards and monetize, obtain personal data. He stressed that only users have to grant rights and ensure proper protection to their digital identity and should be recognized as an owner. The scientist is contemplating whether tech corporations acquire the rights to users' personal data [31]. The ownership of user's personal data is suggested to be rather controversial issue in media and literature nowadays.

We believe that Along with the right to know the purpose of data processing that are processed in relation to them [32], data subjects have been obtained the right to be aware of data (right to know) to what extent the products, services are produced by humans or AI. Data users need to know whether they are subjected to automated processing during decision-making and if they are communicating with an AI agent or a person, as part of these rights [33].

As noted by J. Gakutan, N. Selvadurai opacity of decision-making, the secrecy of the logic of decision-making by the system and the inability to get an explanation of the decisions made by interested persons put the need for legislation to introduce the right to interpret algorithmic decisions and challenge them if they violate the right to privacy and the right to dignity. Therefore, the lack of transparency, evaluation and decision-making without disclosing the rationale for such decisions jeopardizes the right to privacy and dignity [34]. Ensuring transparency of decisions and effective control over automated decision-making systems should be giving the data subject the right to clarify decisions regarding him, in particular those that affect the fate of the subject.

Among the concrete ways to overcome the challenges of AI of the Research Service of the European Parliament in the document "Artificial Intelligence": How it works, why it is important and what can we do about it?" Suggests following solutions: to introduce mechanisms that will enable human review of decisions made by algorithms; granted individuals right to know to what extent the products, services they consume are produced by a natural person or AI; whether users are subjected to automated processing during decision-making; whether users interact with an AI agent or a natural person [35].

Therefore, it is crucially important to give data subjects (users) the right to be aware of the presence of the participation of the automated system in the products, services and goods that are provided by AI, including the right to be informed about the interaction of an AI agent or a natural person. In turn, the lack of proper notification of data subjects should be recognized as a violation of a term of use and ethical principles of AI.

The need to clarify decisions made by automated systems is currently being actualized along with the right to be informed about presence of AI in products and goods. In the opinion of B. Goodman, S. Flaxman, that the "right to clarification" can be achived relatively easily. It is enough only to answer questions such as whether the system is more or less likely to recommend granting a loan if the applicant is from minorities, which characteristics play the sufficient role in forecasting [36].

Traditionally EU members express the respect for human rights and freedoms. So, certain provisions of member states mandate the transparency of public authorities' activities and the obligation of controllers to disclose certain data. Therefore, in order to provide users with protection against algorithmic, to ensure transparency, control over algorithms and to prevent discrimination the Law on the Digital Republic of France (2016) was provided rules and principles of data processing by algorithm. According to the Law on the Digital Republic of France in order to provide transparency of algorithmic system the principles of algorithmic processing should be published on the state website [37]. The principles of transparency in the functioning of automated decision-making systems give data subjects the right to challenge not fair decisions or discriminatory ones.

G. Malgieri, J. Team, and A. Selbst adhere to a broad interpretation of Article 22 of EU Regulation 2016/679 and impose an obligation on controllers to disclose the logic of decision-making and the technical components when the algorithms assist in making legally significant decisions. [38]. At the same time, this position is quite controversial and requires further research.

The right not to know, that is, the right not to be unaware of certain information regarding oneself, as one of the digital rights, in terms of digital age, should contribute to the well-being of an individual. In contrast of right to be aware of collected and processing data about individuals, the right not to know concerns mainly the results of medical research caused by the development of preventive medicine [39]. In the context of the development of preventive medicine [40], the right not to know is of practical importance in the event of the detection of a disease or predisposition to a disease that can be diagnosed but which, cannot be eliminated or cured at the modern level of medicine. The right not to know is sometimes called the right to secrecy about the state of health [41]. The right not to know the results of genetic research is legislated in some EU states, like Switzerland, Austria and Germany. R. Chadwick, M. Levitt D. Schickle and others note that the rights of the nobility and the rights to remain unaware are closely related to the ideas of autonomy of the individual [42].

The rapid development of technologies and communication, the excess volume of data on the Internet, and the ease of searching data on search engines may have far-reaching negative consequences for the perception of a person from the point of view of public opinion. Individuals may live in constant fear of suddenly encountering their own past actions or public statements in a wide variety of contexts, such as during a job search or as part of a business relationship [43]. Therefore, it became necessary to ensure such a right in the digital environment as the right to be forgotten.

The right to be forgotten is recognized as a human right, which allows an individual to demand, under certain conditions, the removal of his personal data from public access through

search engines, that is, links to those data that, in his opinion, could harm him. That is, the right to be forgotten or the right to oblivion is recognized as the right of a person to request search engines, in particular Google, to remove their data from the results of search queries. At the same time, it should be noted that the right to be forgotten provides the possibility to delete specific search results. While removing of unwanted content from sites is carried out by contacting the owners of the sites on which the information itself is posted [44].

Despite the relevant norms being enshrined at the legislative level, Ukrainian legislation lacks a definition for the right to be forgotten. Thus, according to the provisions of the Law of Ukraine "On Protection of Personal Data", personal data are subject to deletion or destruction, in particular, in case of entry into force of a court decision on the deletion or destruction of personal data (paragraph 4 of part 2 of article 15).

In the EU, the concept of the right to be forgotten appeared thanks to the decision of the European Court of Justice in the case of Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. According mentioned decision EU data protection legislation gives individuals the right to contact search engines (for example, Google) with a request to delete search results by person's name [45]. EU law allows for the submission of a complaint or lawsuit to the Internet search engine operator or a higher authority or court regarding the removal or modification of links to pages that contain a person's name before a search term. In the case of Google Spain SL v. Agencia Mario Costeja González the plaintiff demanded the removal of information about the sale of his housing for debts. The plaintiff contended, the announcement of the auction, which contained only 36 words, damaged his reputation. The Court of Justice of the European Union ruled that Mr. Gonzalez has the right to leave this story in the past, and ordered Google to remove search results that contain information about the bidding of his property. The court decision explains that the decision to withdraw the links will depend on the nature of the information in question and its sensitivity to the private life of the data subject and the public's interest in disclosing this information, played role by the data subject in public life [46].

It is not the information itself (text, picture, video, etc.) that is deleted, but the link to it. That is, if a user recognizes their right to be forgotten, the data will not show up in search engine results when searching but undesirable publication itself will remain available [44].

When considering such requests, search engines should take into account whether the information is inaccurate, inappropriate, inappropriate or unnecessary and whether it is of public interest.

Since the appearance of this decision, Google has received 415,359 requests to remove information from the search engine according to its statement. Company satisfied 42.6% of requests and removed 1,444,021 links on the Internet.

The GDPR developer incorporated the relevant law into the Regulations after considering the courts' decisions on the right to be forgotten. The GDPR's adoption has resulted in the right to be forgotten becoming a final legal status. Thus, Article 17 defined the right of data subjects to be forgotten and the right to delete information about themselves in detail. This article was further improved and expanded with the participation of the European Council and the European Parliament [47]. This Regulation restricts the use of the right to be forgotten, in particular in cases listed in Article 17 (3): 1) where the processing of personal data is necessary for the exercise of the right to freedom of expression and information; 2) compliance with the legal requirements of the legislation of the European Union and Member States and the performance of tasks performed

in the public interest or within the framework of the exercise of official powers entrusted to the administrator; 3) when information is used in the public interest in the field of health; 4) when information is archived in the public interest, scientific and historical research, for statistical and other similar purposes; 5) when the information is used for the purposes of litigation, in case of challenging legal claims and claims [48].

At the same time, it should be emphasized that, in accordance with the provisions of Art. 17 of GDPR, the concept of right to be forgotten was generalized in comparison with the aforementioned decision of the European Court of Justice. Thus, this provision establishes that a person has the right to erase his personal data, without any specificities of the way of realisation of the right.

The erasure of personal data is entrusted to controllers – legal entities that determine the goals and means of processing personal data. Herewith rrocessing of personal data is entrusted to search engines and their owners. The search results provided namely by search companies are determined by their accuracy and relevance. [44].

The right to be forgotten is also reflected in the practice of the European Court of Human Rights. So, deciding in the case of "Hurbain v. Belgium", the ECHR stressed that" people have the right to be forgotten as part of the right to privacy. If data about individuals is not of public interest, irrelevant, or distorted, it should not negatively affect their lives. In the digital age, the absence of published results in search engines almost suggests that this publication or news is non-existent.

The balance between privacy and freedom of information in the context of the right to be forgotten is a very significant challenge. Ensuring the deletion of personal data should not restrict freedom of information and freedom of speech. Developing effective mechanisms that take into account both individual rights and public interest is a key challenge for legislators and technical experts in the digital age. Also, one of the key problems of fulfilling the right to be forgotten is the technical complexity of deleting data completely. Backup storage, information archiving and other technical aspects make it difficult to securely delete data from all aspects and places of the digital space [49].

Right to privacy. In the past, the right to privacy was understood as protection against physical encroachment on life and property, from causing harm vi et armis (lat. by force of arms) [50]. This understanding of privacy identified him with the "right to be left alone" [51].

Over time, under the influence of various factors, there was a need to expand the content of the right to privacy. Scholars suggested to distinguish the following types of privacy: physical, territorial, information and privacy of communications [52]. Modern technologies have provided society with new types of communication, which contributed to the construction of new relationships, which based on trust and transparency. This resulted in a gradual modernization of the understanding of the right to privacy, especially in allocating and comprehending privacy components like information and communications privacy. Both of these components of the right to privacy are in close relationship. Information privacy is understood primarily as the establishment of proper protection of personal data during their processing from unauthorized and misuse. In this context, scientists distinguish such legal possibilities of a natural person as: a) to be protected from interference in his personal and family life and relationships through the publication of information; b) know by whom, when, how and within what restrictions information about it can be or will be used by other persons [53]. As for the privacy of communications, its

content is to distribute, receive and other actions related to information that are carried out using technical means [54].

Consider the 2011 decision of the Court of Appeal in Hamm, Germany, which vividly illustrates the situation with anonymity. A psychotherapist initiated this trial because he was dissatisfied with a mediocre assessment given to him by a former patient on an online rating platform. The court denied his appeal because it believed that the obligation to support a specific opinion could discourage people from expressing their own opinions because they fear reprisals. The court states that self-censorship is not in line with the fundamental right to freedom of expression [55]

In terms of digitalization the need to reduce the pressure of the disturbing. The principles of labour protection and the right of employees to exclude their phone, the computer during off-hours stipulated the emergence and development of the right to offline or the right to disconnect. The spread of information and communication technologies, along with the improvement of the conditions of employees, on the one hand, posed challenges to erasing the boundaries of working and free time, the risk of reworking due to continuous inclusion and communication on the Internet. Similarly, E. Castronova noted that the rights of avatars should be considered as agents should have the right to leave virtual worlds and enter them on their own free will [10]. About the change of values and priorities in everyday life, the diminishment of the distinction between private and public, free and working time, that smartphone on vacation has become a necessary component of life draws the attention of Z. Bauman [56, c. 51].

According to B. Casters, the right to offline should be considered as a broader right compared to the right to disconnect. The right to offline extends to various spheres of life and is not limited to labour relations alone [33]. In regards to processing personal data in accordance with the EU Regulation, the right to disconnect or remain offline is somewhat similar to the right to confidentiality, which is referred to as ‘the right to be left alone’.

Conclusions

The article presents a brief analysis on the evolving of human rights in digital space. Theoretical rethinking of traditional legal concepts and mechanism for regulating, implementing the rights and obligations of a natural person in a digital environment are necessary for digital changes in society. The realization of individual rights at the national and international level is directly affected by digital transformation, resulting in the emergence and evolution of digital rights thanks to the existence of the global information digital space.

Digital rights can include a wide range of fundamental rights that are realized in a digital environment and require analysing the properties of this environment. Well-known digital rights, which are mostly derived from information rights, are fuelling the widespread adoption of updated digital rights, but they are not exclusive to them. The difference between information rights and digital rights has been proven through research.

It is substantiated that the development of digital society, the Internet of Things and AI has led to the development of digital rights. The concept of digital rights focuses on the rights that a natural person obtains in the digital space. There are following digital rights: the right to digital identity, the right to privacy, the right not to know, the right to be forgotten, the right to offline or the right to disconnect, the right to be informed about interaction with AI, the right to clarify decisions made with the participation of AI, etc. As technology advances, these rights may not be exhaustive and may expand to other digital rights that are justified by technology and AI.

REFERENCES

1. Malozhon, O.I. (2021). Chetverte pokolinnya prav lyudini v konteksti ukrayinskoyi suchasnosti. Yuridichnij naukovij elektronnij zhurnal. [The fourth generation of human rights in the context of Ukrainian modernity. Legal scientific electronic journal]. 12, 41-44.
2. Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies) URL: https://www.coe.int/en/web/ (Accessed: 22 March 2025).
3. Rada OON z prav lyudini uhvalila rezolyuciyu pro prava onlajn – Centr demokratiyi ta verhovenstva prava [UN Human Rights Council adopts resolution on online rights - Centre for Democracy and Rule of Law]. (2016) URL: https://cedem.org.ua(Accessed: 24 March 2025).
4. Vakaryuk, L. (2018). Osnovni pidhodi do rozuminnya ponyattya «informacijni prava lyudini». *Pidpriyemnictvo, gospodarstvo i parvo,* [Basic approaches to understanding the concept of 'information human rights.' Entrepreneurship, economy and law.] 2, 155-159.
5. Bochkovoj, V.A., Baadzhi, N.A. (2024). Obmezhennya cifrovih prav lyudini v umovah suchasnih pravovih viklikiv. *Naukovij visnik Uzhgorodskogo Nacionalnogo Universitetu, Seriya Pravo*, [Limitations of digital human rights in the context of modern legal challenges. Scientific Bulletin of Uzhgorod National University, Series Law]. 84 (4), 228-233.
6. Koncepciya onovlennya Civilnogo kodeksu Ukrayini / A.S. Dovgert ta in. Kiyiv: Vid. dim «ArtEK», 2020. URL: https://drive.google.com/file/d/1ExwdnngsmvpAZJtWi836Rr6-x1quaZJQ/view (Accessed: 22 March 2025).
7. Popovich, T.P. (2021). Osoblivosti pravovoyi prirodi cifrovih prav lyudini. *Chasopis Kiyivskogo universitetu prava,* [Features of the legal nature of digital human rights. Journal of Kyiv University of Law]. 1, 135-140.
8. Tverezovska, K.S. (2024). Ponyattya, vidi ta znachennya cifrovih prav lyudini. *Yuridichnij naukovij elektronnij zhurnal,* [The concept, types and meaning of digital human rights. Legal Scientific Electronic Journal]. 6, 472-476.
9. Koster, R. (2000). Declaring the Rights of Players. http://www. raphkoster.com/gaming/playerrights.shtml.
10. Castronova, E. (2003). Theory of the avatar. CESIFO *Working Paper*, 863, 1-45. Retrieved March 20, 2025, URL: https://ssrn.com/abstract=385103 (Accessed: 22 March 2025).
11. Petrishin, O.V., Gilyaka, O.S. (2021). Prava lyudini u cifrovu epohu: vikliki, zagrozi ta perspektivi. *Visnik Nacionalnoyi akademiyi pravovih nauk Ukrayini,* [Human rights in the digital age: challenges, threats and perspectives. Bulletin of the National Academy of Legal Sciences of Ukraine]. 1, 7-35.
12. Bratasyuk, O.B., Mentuh, N.F. (2021). Ponyattya ta klasifikaciya cifrovih prav v Ukrayini. *Yuridichnij naukovij elektronnij zhurnal*, [The concept and classification of digital rights in Ukraine. Legal Scientific Electronic Journal]. 10, 58-61.
13. Gololobova, Ye., Mina A. Cifrovi prava ukrayinciv abo Deklaraciya cifrovih prav lyudini. [Digital rights of Ukrainians or Declaration of digital human rights]. URL: https://www.businesslaw.org.ua/digital-rights-t/ (Accessed: 24 March 2025).
14. Razmyetayeva, Yu.S. (2020). Cifrovi prava lyudini ta problemi ekstrateritorialnosti v yih zahisti. *Pravo ta derzhavne upravlinnya,* [Digital human rights and problems of extraterritoriality in their protection. Law and Public Administration]. 4, 18-23.
15. Lesko, N., Antonov, M. (2021). Cifrovi prava lyudini v epohu globalizaciyi. *Visnik Nacionalnogo universitetu Lvivska politehnika. Seriya: Yuridichni nauki,* [Digital human rights in the era of globalization. Bulletin of Lviv Polytechnic National University. Series: Legal Sciences]. 3 (13), 160-166.
16. Verlos, N.V. (2020). Konstitucionalizaciya cifrovih prav lyudini: vitchiznyana praktika ta zarubizhnij dosvid. *Chasopis Kiyivskogo universitetu prava,* [Constitutionalization of digital human rights: domestic practice and foreign experience. Journal of Kyiv University of Law]. 2, 129-133.
17. Shmidt, E., Rozenberg Dzh. (2016). Yak pracyuye Google / Per. s angl. Yu.Gordiyenka. K: KM-BUKS, 274-275.
18. Andreyev, D. (2015). Zasobi masovoyi informaciyi yak mehanizm intelektualnoyi komunikaciyi v procesi rozvitku informacijnogo suspilstva, [Teoriya i praktika intelektualnoyi vlasnosti, Media as a mechanism of intellectual communication in the development of the information society. Theory and practice of intellectual property]. 5, 54-56.

19. Dovgert, A.S. (2020). Koncepciya onovlennya Civilnogo kodeksu Ukrayini. [The concept of updating the Civil Code of Ukraine.]. ArtEK. URL: https://drive.google.com/file/d/1ExwdnngsmvpAZJtWi836Rr6-x1quaZJQ/view (Accessed: 24 March 2025).
20. Sirotyuk, P. (2025) Suchasni teoriyi identichnosti: poshuk sebe u cifrovu epohu. [Modern theories of identity: the search for oneself in the digital age]. URL: https://psihologonline.pro/yakymy-ye-suchasni-teoriyi-identychnosti/ (Accessed: 24 March 2025).
21. Goncharova, A.V. (2024). Elementi cifrovoyi identichnosti. *Naukovij visnik Uzhgorodskogo Nacionalnogo Universitetu, Seriya Pravo,* [Elements of digital identity. Scientific Bulletin of Uzhgorod National University, Series Law]. 83, 187-191.
22. Morteza, V.N. (2016). Person and Personality in Cyber Space: A legal analysis of virtual identity. *Masaryk University Journal of Law and Technology,* 10 (1), 1-17.
23. Kravchenko, A. (2025) Cifrovaya identichnost cheloveka. Kak ee zashitit? [Digital identity of man. How to protect her?]. URL: https://www.ukrinform.ru/amp/ rubric-society/3316996-cifrovaa-identicnost-celovekakak-ee-zasitit.html
24. Crawford S.P. (2004). Who's in Charge of Who I Am? Identity and Law Online. New York Law School Law Review, Cardozo Legal Studies Research Paper, 49, 210-211.
25. Tokareva, V.O. (2022). Shodo pitannya cifrovoyi identichnosti u merezhi internet. *Privatne ta publichne pravo*, [On the issue of digital identity on the Internet. Private and Public Law]. 4, 35-40. URL: http://clj.nuoua.od.ua/archive/36/11.pdf (Accessed: 22 March 2025).
26. Gavrilenko, N.V. (2024). Pravovi zasadi cifrovoyi identifikaciyi i reprezentaciyi osobistosti. Aktualni problemi politiki. [Legal basis of digital identification and representation of personality. Current policy issues]. 73, 162-167. URL: DOI https://doi.org/10.32782/app.v73.2024.23 (Accessed: 22 March 2025).
27. Digital identity. Identification for Development. Retrieved March 30, 2025, URL: http://documents1.worldbank.org/curated/en/ 199411519691370495/Technology-Landscape-forDigital-Identification.p (Accessed: 27 March 2025).
28. Terpstra, G. (2016). Al. Self VS. Digital Self. *Graduate Theses and Dissertations* URL: https://lib.dr.iastate.edu/etd/16027 (Accessed: 27 March 2025).
29. Tokareva, V.O. (2022). Transformaciya virtualnoyi identichnosti: vid mnozhinnosti do yedinoyi avtentichnosti v merezhi Internet. *Aktualni problemi vitchiznyanoyi yurisprudenciyi.* [Transformation of virtual identity: from multiplicity to a single authenticity on the Internet. Actual problems of domestic jurisprudence]. 3, 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf (Accessed: 28 March 2025).
30. Crawford, S.P. (2004). Who's in Charge of Who I Am? Identity and Law Online. *New York Law School Law Review, Cardozo Legal Studies Research Paper*. 130, Vol. 49, 211-215.
31. Tottier, C. Who Owns your Digital Identity? The Answer May Shock You. URL: https://peer.social/ technology/who-owns-your-digital-identity/ (Accessed: 22 April 2025).
32. Own Your Data Foundation. URL: https://ownyourdata.foudation (Accessed: 22 April 2025).
33. Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer law & security review.* 44, 1-13. URL: https://doi.org/10.1016/j.clsr.2021.105636 (Accessed: 12 March 2025).
34. Gacutan, J., Selvadurai N., (2020), A statutory right to explanation for decisions generated using artificial intelligence, *International Journal of Law and Information Technology*, 3 (28), 193-216.
35. Boucher, P. (2020). Artificial intelligence: How does it work, why does it matter, and what can we do about it? *Scientific Foresight Unit (STOA)*. URL: http://www.europarl.europa.eu/stoa (Accessed: 15 March 2025).
36. Goodman, B., Flaxman, S. (2016), EU Regulations on Algorithmic Decision Making and "a Right to an Explanation" URL: https://ora.ox.ac.uk/objects/uuid:593169ee-0457-4051-9337-e007064cf67c/download_file?safe_filename=euregs.pdf&file_format=application%2Fpdf&type_of_work=Journal+article [https://perma.cc/C6UP-DZQE (Accessed: 22 March 2025).
37. Sartor, G. (2017) Human Rights and Information Technologies. The Oxford Handbook of Law, Regulation and Technology / ed. by R. Brownsword, E. Scotford, K. Yeung. Oxford, 442-450.
38. *Malgieri G.*, *Comandé G. (*2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. International Data Privacy Law, 7(4), 243-265.
39. Hood L, Auffray C. (2013). Participatory medicine: a driving force for revolutionizing healthcare, *Genome medicine,* 12 (5), 110-115.

40. Macik, V. Perspektivi rozvitku preventivnoyi medicini. Aktualni problemi menedzhmentu ta publichnogo upravlinnya v umovah innovacijnogo rozvitku ekonomiki. Vseukrayinska- naukova praktichna konferenciya z mizhnarodnoyu uchastyu. [Prospects for the development of preventive medicine. Actual problems of management and public administration in terms of innovative development of the economy. All-Ukrainian scientific practical conference with international participation]. S. 116-119.
41. Yepifanova, N. (2017). Ne povinno buti pravdi na shkodu nadiyi. *Yuridichna gazeta.* [There should be no truth at the expense of hope. Legal newspaper]. URL: https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/ne-povinno-buti-pravdi-na-shkodu-nadiyi-.html (Accessed: 22 April 2025).
42. Chadwick, R., Levitt, M. (Ed.), & Shickle, D. (Ed.) (2014). *The Right to Know and the Right not to Know: Genetic Privacy and Responsibility*. (2 ed.) (Bioethics and Law). Cambridge University Press.
43. Pravo na zabuttya. Praktika YeSPL ta Sudu YeS. 2024. European Courts of Human Rights. European Union Agency for Fundamental Rights. URL: https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten-ukr (Accessed: 23 April 2025).
44. Kunicin, N. (2023). Pravo na zabuttya: pravovij kontekst i sudova praktika. Protokol. [The right to be forgotten: legal context and judicial practice. Протокол]. URL: https://protocol.ua/ua/pravo_na_zabuttya_pravoviy_kontekst_i_sudova_prak (Accessed: 22 March 2025).
45. Google Spain SL and Google Inc. v. Agencia Española
46. Maksimyuk, O. (2022). Pravo buti zabutim. Sogodennya ta majbutnye. Chernivtsi Law School Blog. [The right to be forgotten. Present and future. Chernivtsi Law School Blog]. URL: https://law.chnu.edu.ua/pravo-buty-zabutym-sohodennia-ta-maibutnie/ (Accessed: 22 March 2025).
47. Tokareva, V.O. (2022). Okremi pitannya realizaciyi prava na vidalennya. Aktualni problemi vitchiznyanoyi yurisprudenciyi. [Separate issues of the right to delete. Actual problems of domestic jurisprudence]. 4, 42-47. URL: http://apnl.dnu.in.ua/4_2022/8 (Accessed: 22 April 2025).
48. European Parliament. General Data Protection Regulation 2016/679. URL: https://gdpr-info.eu (Accessed: 22 April 2025).
49. Byelov, D.M., Byelova, M.V., Gornilo, O.T. (2024). Pravo lyudini na zabuttya. *Naukovij visnik Uzhgorodskogo Nacionalnogo Universitetu, Seriya pravo.* [The human right to be forgotten. Scientific Bulletin of Uzhgorod National University, Series Law]. 81 (2), 57-62.
50. Warren, S.D., Brandeis, L.D. (1890). The right to privacy. Harvard law review, 4, 193-220.
51. Serogin, V.O. (2010). Prajvesi yak pravo «buti zalishenim u spokoyi». Pravo i Bezpeka. [Privesi as the right 'to be left alone'. Law and Security]. 3, 6-9. URL: http://nbuv.gov.ua/UJRN/ Pib_2010_3_3 (Accessed: 22 March 2025).
52. Banisar D., Davies, S., Madsen, W., Kassner, M., Breckheimer, R., Van Dongen S. (1999). *Privacy & Human Rights.* Privacy International and Electronic Privacy Information Center. http://gilc.org/privacy/survey/intro.html (Accessed: 15 April 2025).
53. DeCew J.W. (1997). In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, N.Y.: Cornell University Press, 208 p.
54. Kovalenko, O.O., Tihomirov, O.O. (2020). Pravo na privatnist v umovah suchasnih komunikacij. *Yuridichnij naukovij elektronnij zhurnal.* [The right to privacy in the conditions of modern communications. Legal scientific electronic journal]. 5, 133-136.
55. Arrêt I-3 U 196/10 du 3 août 201. URL: http://www.justiz.nrw.de (Accessed: 22 April 2025).
56. Bauman, Z. (2008). Globalizaciya. Vidavnictvo Kiyevo-Mogilyanska Akademiya. [Globalization. Publishing House of Kyiv-Mohyla Academy].