УДК 342.7
DOI: 10.37635/jnalsu.28(1).2021.15-23

Олександр Віталійович Петришин
Національна академія правових наук України
Харків, Україна

Олег Сергійович Гиляка
Кафедра міжнародного приватного права та порівняльного правознавства
Національний юридичний університет імені Ярослава Мудрого
Харків, Україна

ПРАВА ЛЮДИНИ В ЦИФРОВУ ЕПОХУ: ВИКЛИКИ, ЗАГРОЗИ ТА ПЕРСПЕКТИВИ

Анотація. *Сучасний етап розвитку суспільних відносин характеризується стрімким збільшенням цифрових технологій. Інтенсивний розвиток науки та активний технологічний прогрес стали основними характерними ознаками сучасного суспільства. Це позначилось на особливостях життя людей в соціумі, реалізації їх прав та свобод, стало каталізатором формування нової категорії прав людини – «цифрових» прав. Метою статті є аналіз основних загроз та викликів, які постають перед правами та свободами людини в умовах цифровізації, та вироблення пропозицій щодо перспективних шляхів захисту від цих загроз. У статті проводиться теоретико-правове дослідження проблемних питань реалізації прав людини в умовах масової цифровізації суспільних відносин, вказується, що ера цифрових технологій дає абсолютно нові та якісно інші можливості для їх реалізації, але в той же час вона створює нові виклики та загрози для забезпечення цих прав і свобод. Відмічено, що класичні права та свободи людини трансформуються, наповнюються новими аспектами та змістом, розгалужуються на такі, що пов'язані саме з процесом цифровізації. Наголошується на тому, що результати цифровізації багатьох сфер життя вимагають осмислення та адекватного формулювання правового механізму регулювання, реалізації та захисту вже існуючих та тих, які тільки на початку формування, прав людини з метою сталого соціально-економічного розвитку, забезпечення реалізації та захисту конституційних прав і свобод людини і громадянина. У центрі уваги дослідження нові права, такі як право бути забутим, право на анонімність, право на захист персональних даних, право на цифрову освіту та доступ до цифрових знань; права, пов'язані із захистом генетичної інформації; права на участь в обороті майна в цифровій сфері*

Ключові слова: *цифровізація права, цифрова революція, права людини, свободи людини, цифрові права, захист прав та свобод*

Oleksandr V. Petryshyn
National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Oleh S. Hyliaka
Department of Private International and Comparative Law
Yaroslav Mudryi National Law University
Kharkiv, Ukraine

HUMAN RIGHTS IN THE DIGITAL AGE: CHALLENGES, THREATS AND PROSPECTS

Abstract. *The current stage of development of public relations is described by a rapid increase in digital technologies. Intensive development of science and active technological progress have become the main characteristic features of modern society. This has affected the specific features of people's lives in society, the exercise of their rights and freedoms, and has become a catalyst for the development of a new category of human rights – "digital" rights. The purpose of the study is to analyse the main threats and challenges facing human rights and freedoms in the context of digitalisation, and to develop proposals on promising ways to protect against these threats. The study conducts a theoretical and legal research of problematic issues of the implementation of human rights in the context of mass digitalisation of public relations, indicates that the era of digital technologies provides completely new and qualitatively different opportunities for their implementation, but at the same time it creates new challenges and threats to ensure these rights and freedoms. It is noted that classical human rights and freedoms are being transformed, filled with new aspects and content, and branched out into those that are related to the digitalisation process. The results of digitalisation of many spheres of life require comprehension and adequate formulation of the legal mechanism for regulating, implementing, protecting the already existing and emerging human rights for the purpose of sustainable socio-economic development, ensuring the implementation and protection of constitutional human and civil rights and freedoms. The study focuses on new rights such as the right to be forgotten, the right to anonymity, the right to protect personal data, the right to digital education and access to digital knowledge; rights related to the protection of genetic information; rights to take part in property turnover in the digital sphere*

Keywords: *digitalisation of law, digital revolution, human rights, human freedoms, digital rights, protection of rights and freedoms*

INTRODUCTION

The use of modern digital technologies has given rise to the processes of transformation in modern society – the digital transformation of social relations, which is expressed in the use of modern digital technologies in various areas of human activity. The digital revolution as a factor of dynamic development has led to the creation of a digital economy, the development of the foundations of digital law, a new configuration of social relations based on the use of the Internet, social networks, and other information and communication technologies. Modern digital technologies form a new way of production, create prerequisites for the transition to a new formation, to the digitalisation of public relations and the law itself regulating these relations. Digital transformation has a direct impact on the implementation of fundamental human rights, contributes to the emergence of new human and civil rights as a participant in the global information and digital space. The results of digitalisation require comprehension and adequate formulation of the legal mechanism for regulating, implementing, protecting the already existing and emerging human rights for the purpose of sustainable socio-economic development, ensuring the implementation of constitutional human and civil rights and freedoms.

The sphere of digital relations is described by signs of virtuality and cross-border nature, requires special attention to the sphere of fundamental human rights from the standpoint of their provision, taking into account the special properties of this environment, where subjects and objects very often act as a kind of "simulation", and the limits of the exercise of individual rights and interference in them are not always unambiguously identified. If modern practice of the development of law is any guide, the category "digital rights" (also referred to as Internet rights, network rights) is gradually being introduced into conceptual and legal circulation, which has become widespread as a substantial element for describing the legal status of a person on the Internet. At the same time, such a category of rights as "digital rights" has not yet received universal recognition either in law or in doctrine, including in view of Ukrainian legal and law enforcement experience. Evidently, this is conditioned by the fact that the problem of finding and determining the specific features of fundamental human rights (their content and implementation) in the digital environment has arisen relatively recently and, perhaps, solving this issue is a matter of the near future.

At present, when new technologies are rapidly emerging and developing, threats to privacy are also rapidly increasing. The right to privacy is one of the fundamental rights stipulated in international law. With the increasing digitalisation of modern life, protecting privacy has become more difficult. Both state and non-state organisations often interfere in the privacy of citizens. Even those legislative acts that regulate the possibility of such interference and determine cases of granting permission to the relevant authorities to do so do not keep up with the rapid development of technology. The methods of protection offered by the current legislation do not keep up with the requirements of the modern world, and there is a need to review the mechanisms of legal regulation and professional legal awareness in general. V. Hartzog and N. Richards, analysing the existing norms and methods of regulating privacy relations, fairly note that a minimised set of legal provisions frees the hands of companies that make a profit by extracting as much value as possible from users' personal data, the principle of "informing and choosing" translates the most important conditions for rendering information services into the plane of points written in small print at the end of contracts [1, p. 1193].

Other researchers note that surveillance technologies in many situations create opportunities for serious violations of privacy by governments, individuals, and the private sector [2]. In those cases when they are used in accordance with international human rights standards, surveillance technologies can often be an effective tool for law enforcement. Therewith, it is not uncommon to use software for targeted listening of communication channels and facial recognition, the use of which can lead to human rights violations (for example, the right to peaceful protest), arbitrary arrests and detentions [3, p. 235]. These technologies can also incorrectly identify certain minority groups, consolidating existing stereotypes in society [4, p. 10], and increase the probability that representatives of marginalised groups and minority communities will face discrimination more often, for example, when issuing a loan [5, p. 1268].

The study of human rights in the context of digitalisation, and digital rights in particular, is covered in the studies of such foreign scientists as N. Borisov [2], J. Coccoli [6], F. Galindo [7], J. Garcia-Marco [7], K. Hamman [4], W. Hartzog [1], S. Jahid [2], A. Kapadia [2], P. Mittal [2], Sh. Nilizadeh [2], N. Richards [1], J. Riordan [8], R. Smith [4], J. Tomalty [9] and others. The views and considerations expressed in their studies on human rights in the age of digitalisation will be considered in this study.

At the same time, a holistic theoretical legal study on the impact of digitalisation on fundamental human rights and freedoms, understanding and adequate formulation of the legal mechanism for regulating, implementing, and protecting these rights in the context of digital transformation in the legal doctrine has not been carried out, the system of Ukrainian regulations in this area is only at the initial stage of its development. Thus, the main purpose of the study is to describe human rights in the era of digitalisation, identify the challenges and threats that it can create for such rights, as well as study the prospects for their development in the future.

1. MATERIALS AND METHODS

To carry out the study, a system of methods of scientific cognition was applied, in particular general philosophical, general scientific (dialectical, analysis, synthesis, abstraction, analogies), particular methods of scientific cognition used in the branches of many sciences (comparative analysis, quantitative and qualitative analysis), as well as special legal methods (formal legal, comparative legal, system-structural).

The the general philosophical (universal) method of cognition was applied at all stages of the cognitive process. The dialectical method was used to analyse doctrinal approaches to the definition of the term "digital rights", which to date has not received universal recognition either in law or in doctrine, including in view of Ukrainian legal and law enforcement experience. Using the method of analysis, the study covered the inherent features and identified the individual features of human rights in the era of digitalisation, analytical interpretation made it possible to engage in reverse engineering of the concept, in particular, to distinguish a stage of development of such rights and investigate it as a separate part of the whole. The method of analysis also contributed to the identification of the inherent features and features of digital rights, made it possible to identify similarities and distinguish them with classical human rights, correlate the universal catalogue of human rights with the rights that started developing under digitalisation processes, and identify their place in it.

Using the synthesis method, the authors of the study have come to the conclusion that digital rights should be interpreted as an extension of universal human rights to the needs of an information-based society. The hermeneutical method was used in the interpretation of scientific concepts of the theory of law and the provisions of current legislation. The method of deduction made it possible, based on the doctrinal opinions of scientists, to draw a general conclusion regarding the inherent features of human rights, the grounds for their classification. The inductive method of cognition made it possible to obtain a general conclusion that mass control and analysis of publicly available information have far-reaching consequences for society, and they are particularly dangerous for various minorities and people with oppositional views. There is a need to develop a set of basic rules at both the state and local levels, which would allow monitoring the advanced technologies used in state surveillance of citizens; at the national level, it is necessary to consolidate the basic protection of citizens from excessive state monitoring of social networks and other publicly available data.

The Aristotelian method was useful in analysing the content of the current legislation of Ukraine on digitalisation of spheres of public life, clarifying the problems of its legislative technique in the relevant regulations. The comparative legal method facilitated a comparative analysis and made it possible to investigated the features of legislative regulation and protection of human rights in the context of digitalisation in order to identify the

most advanced legal means that can be incorporated into national legislation in the relevant area.

Special legal methods have also been used, in particular, formal legal and system-structural methods used in the development and research of the terminology of this paper, namely, in clarifying the content of the categories "human rights", "digitalisation", "digital rights", as well as upon formulating the definition of the specified legal categories.

The theoretical framework of the study comprises scientific articles and opinions of leading foreign experts covering the study of issues of ensuring the protection of human rights in the context of mass digitalisation of public relations. The regulatory framework for this study includes current laws and other regulations of Ukraine governing social and legal relations arising in connection with digital transformation, regulations of European and international organisations. The empirical basis for the study comprises the judicial decisions of the European Court of Human Rights, which actively takes into account current challenges to human rights upon interpreting the provisions of the articles of the European Convention for the Protection of Human Rights and Fundamental Freedoms. In addition, the study uses doctrinal sources that cover the content and characteristics of the implementation of human rights and freedoms in the context of digitalisation, and offer promising ways to protect them from possible threats.

2. RESULTS AND DISCUSSION

Today, everyone is aware that access to the global network can cause problems related to the violation of human rights in the process of using web technologies, including due to inappropriate behaviour of people operating within different jurisdictions, legal, political, and information cultures. As the researchers note, the advent of the Internet has not created a set of "new behaviours" – for the most part, it largely reproduces previous models. Only the consequences of such behaviour and the problems associated with its legal regulation have changed [7, p. 2]. The state and society face important tasks: to identify new rights and prospects for the development of conventional rights. Legislators, scientists, and specialists in the field of information and communication technologies are called upon to offer conceptual and acceptable solutions to these tasks and issues.

Any analysis of the impact of new technologies on human rights, as Jacopo Coccoli points out, is extremely complex and requires prior consideration of two aspects. The first is conditioned by the evolutionary period of time that separates the achievements of technological progress and their legal registration. Adaptation of both national and international legal provisions to innovations in science and technology, in particular to digital technologies, is too slow and ineffective. The second aspect reflects the trend of their development at the international level. Taking these aspects into account should determine the goals in the field of human rights protection: firstly, there is a need to reinterpret conventional human rights in the light of scientific and technological development; secondly, new human rights appear, which can be defined as "sui generis" – a generation of digital rights [6, p. 224-225].

Digitalisation catalyses the blurring of boundaries between conventional branches of law. Information and technologies are already present in every industry, they become a common denominator and are capable of determining a unified logic of law. The value of the boundaries of branches of law decreases in legal practice, which inevitably affects the theory of law. The category of digital rights is gradually being recognised in global, regional, and national contexts. Sometimes this happens in the procedure of regulating specific human rights, which are usually referred to as digital or communication rights, but sometimes on a more comprehensive basis – when determining a detailed list of such rights. At the same time, such a category of rights as "digital rights" has not yet received universal recognition either in law or in doctrine, including in view of Ukrainian legal and law enforcement experience. Evidently, this is conditioned by the fact that the problem of finding and determining the specific features of fundamental human rights (their content and implementation) in the digital environment has arisen relatively recently and, perhaps, solving this issue is a matter of the near future. Be that as it may, the task of today should be to understand the existing ideas about digital rights and who they belong to and what they represent, what benefits they are intended to protect, how they correlate with fundamental rights and freedoms (how independent they are). In a general understanding, digital rights should be interpreted as an extension of universal human rights to the needs of an information-based society. The authors of this study believe that digital rights can include a wide scope of fundamental rights that are implemented in a digital environment and require research in terms of the properties of this environment. Therewith, fundamental digital rights are primarily derived from information rights, but they are not reduced to them.

At present, such digital rights are already actively distinguished as follows: the right to access information; the right to access information platforms and technologies; the right to protect personal data (individual 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 take part in property turnover in the digital sphere; the right to be forgotten; the ability to exercise personal, social, economic, political and cultural rights based on new technological platforms. That is, conventional and worldwide human rights and freedoms are being transformed, filled with new aspects and content, and branched out into those that are related to the digitalisation process. Discussions regarding the right to access the Internet are currently ongoing. Some scientists insist that the right to access the internet should be singled out as a separate category, referring it to the group of digital rights. Others believe that the existence of the right to access the Internet remains a controversial issue at the doctrinal level. The researchers note that access to the Internet cannot be considered as a universal natural right that belongs to all

people by virtue of their nature. Human nature does not make provision for access to the Internet, people have lived without it for centuries without harm to their nature and, perhaps, will do without it in the future, if the Internet is replaced by new, more efficient technologies [9, p. 6].

Access to the internet itself has no legal value, it is important as a means of realising other human rights and freedoms in general – the basis of all the human's natural rights. The social forms and ways of human freedom are diverse and historically variable. At present, they are becoming more technologically equipped and technologically dependent. The internet (and the need for access to it) is one of the manifestations of this trend. Specific socially, historically and culturally determined (including technologically) ways of exercising personal freedom may well qualify as human rights. Admittedly, the exercise of almost all human rights remains possible without the access to the Internet, but is certainly less effective.

The issue of human rights security upon using the Internet remains extremely relevant from the standpoint of protecting human rights. Thus, representatives of one of the oldest educational and research centres in Spain at the University of Zaragoza, Professor F. Galindo and Professor J.G. Marco, question whether the Internet can help strengthen freedom of expression and information without restricting the freedom of its users. Scientists reasonably note that the widespread use of information and search engines and their automatism, on the one hand, facilitate access to various information stored on the Internet, and thus contribute to strengthening freedom. On the other hand, it creates problems related to privacy, lack of transparency in the use of information and control by users. F. Galindo and J.G. Marco fairly point out that query keywords in conjunction with related metadata can enable almost anyone to obtain information about the user, including his or her interests, habits, and preferences. Moreover, some queries may contain identifiers and quasi-identifiers that allow them to be linked to a particular person [7, p. 8].

Another important issue arises both from the standpoint of theory and practice of legal regulation – this refers to the responsibility of Internet intermediaries. This problem is not new, it is the subject of many studies, the most interesting of which is the monograph of the University of Liverpool J. Riordan "The Liability of Internet Intermediaries" [8]. The author attempts to define the limits of liability and consider them from the standpoint of various branches of law. This study aims to help judges, practitioners, and academics propose clearer and more consistent rules governing the activities of the next generation of internet intermediaries, as well as disputes related to their services.

The responsibility of internet intermediaries covers a wide scope of issues, thereby arousing the interest of the scientific community in solving them. Therewith, the results of the study demonstrate that increasing the responsibility of internet intermediaries and pressure on them can negatively affect the activities of the business sphere related to data. As noted, when establishing such responsibility, it is always necessary to remember that when making appropriate decisions, care must also be taken to ensure that working business models are not destroyed. J. Riordan fairly believes that intellectual property, data protection, net neutrality, service infrastructure, and competition law are areas where policymakers and legislators should take a balanced, proportionate approach in determining accountability. The committee of Ministers of the Council of Europe has issued a recommendation[1] on the role and responsibilities of internet intermediaries. The document summarises international human rights standards in situations where states restrict the work of internet intermediaries (including by blocking and deleting content or any other measures that may lead to restrictions on the right of access to information and freedom of speech). In accordance with this recommendation, states should:

– evaluate the potential impact of planned measures on human rights and take only those measures that achieve the necessary goal with minimal restriction of rights;

– ensure the existence of procedural guarantees: a judicial procedure for making a decision on restricting access to content, legal remedies, etc.;

– refrain from imposing a general obligation on internet intermediaries to monitor the content of third parties that such platforms host, transmit, or store;

– ensure that the liability measures that apply to internet intermediaries are proportionate, since excessively strict liability measures lead to the fact that internet intermediaries begin to independently restrict acceptable content;

– refrain from imposing liability on internet intermediaries for the content of third parties that they post. Internet intermediaries can be held accountable if they do not restrict the distribution of content as soon as they become aware of its illegal nature;

– encourage the development of self-regulation or joint regulation of internet platforms.

Digital technologies can help overcome discrimination (for example, by expanding access to financial services through the development of mobile money) or strengthen it. The latter is often associated with the potential ability of algorithms to reproduce discriminatory practices. Thus, in the Declaration on the manipulative capabilities of algorithmic processes, the Committee of Ministers of the Council of Europe notes that technological progress makes it possible to draw fairly detailed conclusions regarding people based on available data, referring them to certain categories [10]. This practice only reinforces the currently existing forms of social, cultural, religious, legal, and economic segregation. This allows distributing people based on their digital profiles. Such actions can have a direct impact on their lives, in particular when an artificial intelligence system is used to make decisions on who should primarily be eligible for a mortgage or healthcare service. Network security expert H. Abelson also writes about privacy issues. He

1. Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. (2018, March). Retrieved from https://rm.coe.int/1680790e14.

claims that the harm that granting the exclusive right of access to information to law enforcement agencies can cause will be very serious. Apart from the expected technical difficulties, the number of problems related to general regulation will increase. In such a situation, there are no guarantees that the principles of respect for human rights and the rule of law would remain [11, p. 72]. Thus, the risk of spreading confidential data is quite high. The issue of ensuring privacy is constantly evolving. Society is increasingly immersed in the internet space, and the authorities are attempting to control the publicly available data that is posted on social networks as much as possible. Undoubtedly, such a high level of state supervision undermines the individual's rights to freedom of speech and compromises the foundations of democracy.

Mass control and analysis of publicly available information have far-reaching consequences for society, and they are particularly dangerous for various minorities and people with oppositional views. There is a need to develop a set of basic rules at both the state and local levels that would allow monitoring the advanced technologies used in state oversight of citizens. Furthermore, it is at the national level that it is necessary to consolidate the basic protection of citizens from excessive state monitoring of social networks and other publicly available data. The impact of new technologies on human rights is also gradually gaining the attention of scientists from various branches of law. Thus, digital technologies have made obvious changes to labour law. In many areas of the economy, modern technologies allow performing a labour function outside the location of work and workplace, not only at home (home office), but also in any convenient place (mobile office).

The employer often expects an employee to be available at all times. If in developing economies this is rather a plus and is perceived positively both by the workers themselves, who want to earn more money, and by consumers who are comfortable, for example, shopping at night, then in developed countries traditional values (the right to rest and privacy) prevail. In France, in August 2016, the law on Labour, modernisation of social dialogue, and ensuring professional careers[1] was adopted, one of the sections of which is called "adaptation of labour law in the digital age". For the first time, the law established the right of an employee to turn off digital devices (in particular, telephone and e-mail) in order not to violate their recreation time, vacation, as well as to respect their private and family life. In other words, French employees have the right not to answer their employer's calls and emails during non-working hours. And indeed, on weekends and holidays, the French are practically "inaccessible". France became the first country to include this right in labour legislation.

Since employees' rest time can no longer be occupied by professional requests (such as email responses), one promising possibility is that a considerable proportion of these employees spend even more time on social networks such as Facebook, YouTube, or Twitter. Thus, paid professional time can be replaced with digital work, especially on microtechnological services such as Amazon Mechanical Turk.

Digitalisation can also modernise the field of environmental law. In particular, legal disputes regarding the state of the environment in a particular area would be resolved faster if a mechanism were provided for transmitting data on the state of pollution to the population in real time. In administrative law, there are also many new phenomena that affect the procedure for implementing public administration. Mechanisms for electronic participation of citizens in governance are being developed, and ways of informing society by state institutions are being enriched. However, not just concerns are voiced, but particular confirmations that social networks, and the Internet in general, pose a threat to both democracy and the state itself. The state conventionally supports coordination and mediation mechanisms for society, minimising direct contacts of citizens. Back in 2013, the UN warned that states risk being sidelined from citizens' communication with each other. This is what encourages states to actively "go" to the Internet themselves. Government involvement in the digital environment is becoming an important component. These processes have not passed Ukraine by. Thus, the Ukrainian authorities, while remaining in the trend of these changes, contribute in every possible way to the process of digital transformation, the current result of which is the adoption of the Decree of the Cabinet of Ministers of Ukraine No. 67 "On Approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Action Plan for its Implementation" dated January 17, 2018[2]. To activate the development of digitalisation within the Cabinet of Ministers of Ukraine, a specialised ministry has also been created – the Ministry of Digital Transformation of Ukraine, which in particular is designed to ensure the development and implementation of national policy in the field of digitalisation, digital economy, digital innovations, e-governance and e-democracy, the development of the information society; the development and implementation of national policy in the field of digital skills and digital rights of citizens; the development and implementation of national policy in the field of open data, the development of national electronic information resources and interoperability, the development of infrastructure for broadband internet access and telecommunications, e-commerce and business.

The adaptation of both national and international legal provisions that are designed to regulate the sphere of science and the latest technologies is slow, and the current legislation is incapable of adequately regulating the situations generated by technological

1. Law No. 2016-1088 "Of relating to work, the modernization of social dialogue and the securing of professional careers". (2016, August). Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032983213/.

2. Decree of the Cabinet of Ministers of Ukraine No. 67-p "On Approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Action Plan for its Implementation". (2018, January). Retrieved from https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text.

innovations. At the global level, this problem was fixed by UN resolution 2450 (XXIII), which proposes to commence an interdisciplinary research at the national and international levels aimed at determining standards for the protection of human rights and freedoms from the potential impact of new technologies. The resolution calls for focusing efforts on establishing a balance between scientific and technological progress and the intellectual, spiritual, cultural, and moral wealth of nations [12, p. 4]. At the level of the Council of Europe, the impact of new technologies on human rights was considered by all key authorities. The committee of ministers and the Parliamentary Assembly have adopted relevant declarations and recommendations, conferences and scientific research are constantly held on the legislation and practice of various Council of Europe countries in the field of Internet freedom [13]. The European Court of Human Rights (ECtHR) also considers current challenges to human rights upon interpreting the provisions of the articles of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Issues related to the collection and storage of human data by public authorities usually occupy a considerable part of the total number of cases concerning the right to respect for private life (Article 8 of the ECHR). As the ECtHR has repeatedly noted in its practice, modern technologies for data collection and storage can endanger human rights [14].

Back in 2008 in the case of S. and Marper vs the United Kingdom [15], which concerned the indefinite retention of the applicants' fingerprints, cell samples and DNA profiles in the database, after the criminal prosecution had ended for one of them with an acquittal and for the other with the termination of the case, the Grand Chamber of the ECtHR pointed out that the use of modern scientific methods in the criminal justice system at all costs was unacceptable. A balance must be struck between the potential benefits of widespread use of such methods and the interests associated with the protection of privacy. Any state that applies cutting-edge technological advances has a special responsibility to "maintain a fair balance". The court found that the unquestioning and indiscriminate nature of the powers relating to the retention of fingerprints, cell samples and DNA profiles of persons suspected of crimes but not convicted of them, as was the case in the cited case, did not strike a fair balance between the competing public and private interests.

A number of cases relate to data collection through secret interception of communications and, in particular, the existence or absence of effective safeguards against abuse in this area. In Szabo and Vissy vs Hungary [16] 2016 concerning Hungarian legislation on secret anti-terrorist surveillance, the applicants complained that they could potentially become targets of such surveillance under the pretext of protecting public safety, with measures of interference with their private life unjustified and disproportionate due to the imperfection of that legislation, in particular because it did not provide for judicial control over decisions of the special services. The ECtHR noted that the consequence of the fight against manifestations of modern terrorism is the desire of states to resort to advanced technologies for collecting information, such as mass monitoring of communication lines. However, to prevent terrorist acts, the state is obliged to take measures to ensure that the legislation governing the use of such technologies does not allow for the possibility of their abuse. The court found that in this case such a condition was not met – according to the law, surveillance measures could be applied to virtually any person in Hungary, and technology made it possible to collect information en masse, including persons who were outside the scope of the operation. Moreover, the order to apply such measures was issued by the executive authorities and could not be appealed.

In May 2014, the European Court of Justice issued a decision [17] granting citizens of EU countries the right to apply to any search engines with a request to remove certain links containing private information about applicants. The court pointed out that if the request is justified and there are no obstacles to its execution, the search engine administrator shall be obliged to grant the request. The court's decision came as a surprise, as it contradicted the opinion of the Advocate General of the EU Court of Justice, who believed that the Google search engine should not be considered as an entity that controls personal data on the pages it processes. Notably, the Advocate General has the same qualifications as judges, and it is his duty to provide an independent and reasoned opinion on a particular case that has come to the European Court of Justice, before the judges themselves begin to consider the claim on its merits. The opinion of the Advocate General does not have the force of a court decision, but for the most part the court takes into account its recommendations. The trial on the "right to be forgotten" was an exception where the court did not take into account the position of the Advocate General. The decision of the European Court of Justice was positively assessed, it was a real victory in the fight for the protection of personal data of Europeans. The court's decision confirmed the need to transfer the norms of information protection from the "stone digital age" to the modern world, and provided an opportunity to strengthen and expand the right of citizens to be forgotten on the Internet.

Thus, ideas about the universality of human rights can be harmoniously linked to the neutrality and universality of digital technologies [18]. In the era of digitalisation, the essence of a person and their main needs are unlikely to change, as well as the basic values associated with them. And it is human rights that can become a unifying purposive perspective upon determining the attitude towards various technologies, which involves analysing the effect they have on the rights and freedoms, honour and dignity of people [19, p. 14]. This idea is quite promising, given the certain confusion of scientists and practitioners in the face of the challenges that the digital age brings.

CONCLUSIONS

The era of digital technologies provides new, broader opportunities for the exercise of human and civil rights and freedoms, but at the same time it creates new challenges and threats to ensuring these rights and freedoms. Digitalisation of almost all spheres of life also leads in some cases to a negative impact, primarily on ensuring

natural, inalienable human rights, especially when it comes to privacy. In most cases, users of digital technologies and the World Wide Web protect personal information individually, using a wide variety of technologies. But this is not always effective due to both objective and subjective reasons, which means that there is a direct threat to many fundamental natural human and civil rights and freedoms.

At present, there is no doubt that an effective mechanism for ensuring human and civil rights and freedoms is impossible without effective information content. But at the same time, it is clear that information technologies and their use in the implementation of human rights are not always completely positive. The widespread use of digital technologies not only ensures the exercise of human and civil rights and freedoms, but also sometimes directly affects fundamental human rights, in many cases violating them. This objectively poses difficult tasks for the states of the world and the international community to solve existing problems in this area to ensure a balance of the rights and legitimate interests of individuals, society, and the state. Digitalisation catalyses the blurring of boundaries between conventional branches of law. Information and technologies are already present in every industry, they become a common denominator and are capable of determining a unified logic of law, which inevitably affects the theory of law. The category of digital rights is gradually being recognised in global, regional, and national contexts. Sometimes this happens in the procedure of regulating specific human rights, which are usually referred to as digital or communication rights, but sometimes on a more comprehensive basis – when determining a detailed list of such rights.

The current task should be to understand the existing ideas about digital rights and who they belong to and what they represent, what benefits they are intended to protect, how they correlate with fundamental rights and freedoms (how independent they are). In a general understanding, digital rights should be interpreted as an extension of universal human rights to the needs of an information-based society. Digital rights can include a wide scope of fundamental rights that are implemented in a digital environment and require research in terms of the properties of this environment. Therewith, fundamental digital rights are primarily derived from information rights, but they are not reduced to them.

RECOMMENDATIONS

The scientific value of the study lies in the fact that it outlines the main challenges facing human rights and freedoms in the context of digitalisation based on the study of theoretical and statutory issues, and makes proposals on promising ways to protect these rights in new conditions. The study covered such a category of rights as "digital rights", which has not yet received universal recognition either in law or in doctrine, including in view of Ukrainian legal and law enforcement experience. The study provided a definition of digital rights, which should be interpreted as extending universal human rights to the needs of an information-based society. Digital rights can include a wide scope of fundamental rights that are implemented in a digital environment and require research in terms of the properties of this environment. Therewith, fundamental digital rights are primarily derived from information rights, but they are not reduced to them.

REFERENCES

[1] Richards, N., & Hartzog, W. (2017). Privacy's trust gap [Resensio]. *The Yale Law Journal*, 126, 1180-1224.

[2] Nilizadeh, Sh., Jahid, S., Mittal, P., Borisov, N., & Kapadia, A. (2012). Cachet: A decentralized architecture for privacy preserving social networking with caching. In *CoNEXT 12: Proceedings of the 8th international conference on Emerging networking experiments and technologies* (pp. 337-348). New York: Association for Computing Machinery.

[3] Wang, J. (2018). *Carceral Capitalism*. South Pasadena: Semiotext(e).

[4] Hamman, K., & Smith, R. (2019). Facial recognition technology: Where will it take us? *Criminal Justice*, 34(1), 8-17.

[5] Prince, A.E.R., & Schwarcz, D. (2020). Proxy discrimination in the age of artificial intelligence and big data. *Iowa Law Review,* 105(3), 1257-1318.

[6] Coccoli, J. (2017). The challenges of new technologies in the implementation of human rights: An analysis of some critical issues in the digital era. *Peace Human Rights Governance*, 1(2), 223-250.

[7] Galindo, F., & Garcia-Marco, J. (2017). Freedom and the Internet: Empowering citizens and addressing the transparency gap in search engines. *European Journal of Law and Technology*, 8(2), 1-18.

[8] Riordan, J. (2016). *The liability of Internet intermediaries*. Oxford: Oxford University Press.

[9] Tomalty, J. (2017). Is there a human right to Internet access? *Philosophy Now*, 118, 6-8.

[10] The age of digital interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation. (2019). Retrieved from https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

[11] Abelson, H. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1, 69-79.

[12] Access to Internet and freedom to receive and impart information and ideas: Factsheet of the European Court of Human Rights. Strasbourg. (2018). Retrieved from http://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf.

[13] Freedom of expression, the Internet and new technologies. Thematic factsheet. (2017, August). Retrieved from https://rm.coe.int/factsheeton-freedom-of-expression-internet-and-new-technologies-11aug/1680738366.

[14] New technologies: Factsheet of the European Court of Human Rights. Strasbourg. (2018, February). Retrieved from http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

[15] Case of S. and Marper v. The United Kingdom. Judgment. European Court of Human Rights, Application No. 30562/04 and No. 30566/04. (2008, December). Retrieved from https://rm.coe.int/168067d216.

[16] Szabo and Vissy v. Hungary, Judgment, European Court of Human Rights, Application No. 37138/14. (2016, January). Retrieved from https://www.statewatch.org/media/documents/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf.
[17] Google Spain SL Google Inc. v. Agencia Española de Protección de Datos (AEPD) Mario Costeja González, Judgment of the Court (Grand Chamber) in Case C-131/12. (2014, May). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=794833.
[18] Petryshyn, O.V. (2020). *General theory of law*. Kharkiv: Pravo.
[19] Brownsword, R., Scotford, E., & Yeung, K. (2017). Law, regulation, and technology: The field, frame, and focal questions. *The Oxford Handbook of Law, Regulation and Technology*, 1, 3-40.

Oleksandr V. Petryshyn
Doctor of Law, Professor
Full Member (Academician) of the National Academy of Legal Sciences of Ukraine
President of the National Academy of Legal Sciences of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Pushkinska Str., Kharkiv, Ukraine

Head of the Department of Theory and Philosophy of Law
Yaroslav Mudryi National Law University
61024, 77 Pushkinska Str., Kharkiv, Ukraine

Oleh S. Hyliaka
Candidate of Law
Assistant of the Department of Private International and Comparative Law
Yaroslav Mudryi National Law University
61024, 77 Pushkinska Str., Kharkiv, Ukraine

Head of Department of Planning and Coordination of Legal Research in Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Pushkinska Str., Kharkiv, Ukraine

Suggested Citation: Petryshyn, O.V., & Hyliaka, O.S. (2021). Human rights in the digital age: Challenges, threats and prospects. *Journal of the National Academy of Legal Sciences of Ukraine,* 28(1), 15-23.

Submitted: 08/01/2021
Revised: 05/02/2021
Accepted: 11/03/2021