Digital Right Protection Principles under Digitalization

Elena Anatolyevna Kirillova
Russian Federation Southwest State University, Kursk, Russia.
South-Ural State University (National Research University), Chelyabinsk, Russia.

Vladimir Nikolaevich Koval
Sevastopol State University, Sevastopol, Russia.

Sergey Zenin
Kutafin Moscow State Law University, Moscow, Russia.
Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia.

Nikolay M. Parshin
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Belgorod, Russia.

Olga V. Shlyapnikova
Saratov State Law Academy, Saratov, Russia.

Received April 02, 2021; Accepted July 10, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI04/WEB18173

Abstract

The article deals with the main principles of protecting digital rights – a new legal category – in the digital environment. In the context of the rapid development of information and communication technologies when cyberspace becomes the platform for interaction between citizens, society, and the state, there is a need to re-evaluate traditional approaches to rights exercised through digital communications on the Internet. The purpose of the study is to examine the legal features and properties of digital rights and identify the principles for protecting digital rights online. The authors employ the general scientific dialectical method as well as the formal legal, systemic structural, and formal logical cognition methods. The synergetic method is used to identify the features and properties of digital rights, this method helps to highlight new rules and new realities in the creative potential of chaos. The authors conclude that the scope of digital legal relations has the characteristics of cross-border and virtuality, thus ensuring the protection of digital rights should be carried out considering the special properties of this environment in which subjects cannot always be identified, and objects are characterized as simulations. Digital rights are obligations and other rights, the content and the exercise of which are determined by their specific features according to the rules and functioning principles of the information and telecommunication system. The holder of a digital
right can be a person who can exercise the right. The authors identify the basic principles of protecting digital rights: the digital equality principle; the digital self-determination principle; the anonymous communication principle; the principle of confidentiality of private communications; the principle of privacy in the digital environment; the principle of secrecy of digital identification; the principle of security of data obtained through facial recognition technologies; the principle of erasure of digitalized personal information.

Keywords


Introduction

The development of information technology over the recent decades has led to the formation of a new digital reality. Digital technologies permeate the established relations and institutions, as a result, a new unique reality is being created – the Internet of Things, the digital economy, the circulation of cryptocurrency. In this context, the previous legal regulation of various spheres of social life requires significant modernization. Just as the rules of the road designed to regulate horse riding were replaced by the driving regulations, the rules of air travel and space flights, today a new law is being born – the "law of the second modernity" which regulates economic, political, and social relations in the context of the world of digits, Big data, robots and artificial intelligence (Kirillova, Blinkov, Ogneva, Vrazhnov & Sergeeva, 2020).

At the present stage, the concept of "digital rights" is gradually being introduced into the conceptual and legal circulation. The concept is understood as Internet rights, online or communication rights, these rights are a significant characteristic of the situation of citizens in emerging legal relations in the digital environment (Nersessian, 2018). However, the category of "digital rights" has not been consolidated in legislation and doctrine since the problem of determining the specific features and content of digital rights in the digital environment has emerged recently, therefore, understanding the concept of digital rights is an urgent task.

Digital rights can include a wide range of fundamental rights that are implemented using the digital environment and it is necessary to investigate these rights considering the properties of this environment. The legal category of "digital rights" is being recognized internationally and in national projects. At the national level, the idea of adopting legal documents that comprehensively regulate the issues of ensuring digital rights is being
actively promoted. In Italy, the Declaration of Internet Rights was approved by the National Parliament in 2015, New Zealand's Harmful Digital Communications Act was adopted in the same year, and the Digital Republic Act was adopted in France on 7 Oct. 2016. In Brazil, Marco Civil da Internet dated 23 Apr. 2014 No. 12.965 is in force, which has become one of the most advanced acts of this kind in world practice. In particular, the users are guaranteed the following rights (Art. 7): the right to non-suspension of the Internet connection, except if due to a debt resulting directly from its use; the right to ensure the quality of the Internet connection provided for by the contract with the provider. The United Nations (UN) adopted resolutions that regulate digital rights "On the protection of rights on the Internet", the Resolution on the right to privacy in the digital age. Fundamental rights in the digital environment require a new interpretation, particularly important is a clear interpretation of digital rights in civil legal relations, as this will make it possible to more clearly define the interests of the subjects of the digital space and carry out a stable civil circulation there.

The purpose of the study is to examine the legal features and properties of digital rights, to highlight the principles of protecting digital rights on the Internet.

Literature Review

The problem of digital rights was examined by many researchers: Parviz Bagheri, Kamal Halili Hassan (2015) investigated the legal problems of denial of Internet contacts and raised issues of restricting digital rights, such restrictions are a direct violation of fundamental human rights, as with a digital environment, citizens are actively involved in public life, study, vote, invest, work, use of various services. The modern stage of life is difficult to imagine without the Internet, with the help of telecommunications. Innovations are created, such as artificial intelligence, blockchain, Big Data technologies, and many others, which can only be accessed in a virtual environment, so every citizen should have the right to access the Internet and implement their rights in the digital environment. Huang-Chih Sung (2020) explored the topic of online courts that are used in China, the right to review the facts of a case in an online court can be attributed to digital rights, while it should be borne in mind that typical cases can still be considered online. The variety of digital rights does not allow creating a closed list of them, perhaps over time they will be classified and more precisely defined. At the present stage, digital rights include those rights that can be implemented using the Internet in a digital environment. Mathew Y.H. Wong, Ying-ho Kwong, Venisa Yeuk Wah Chau (2021) investigated the constitutional framework for human rights implemented in the digital environment, the right to freedom of speech. This right may be exercised in the online environment, if the one who expresses his/her
opinion does not promote violence, does not call for the violation of existing legal orders, does not engage in illegal activities, and so on. The right to the confidentiality of private life – in the digital environment, is the right to maintain the secrecy of personal information that users are forced to provide to certain digital services, the right to freedom of choice is the right to vote in support of the selected candidate, the right to choose preferred content, the right to a remote work format, etc.; the right to a decent standard of living is the right to access the Internet, when, using a virtual environment, citizens will be able to exercise many constitutional and civil rights. Dan Jerker B. Svantesson (2018) researched jurisdictional issues of Internet use and civil law situations that arise in the Internet environment, while legal relationships arise that can be called digital legal relationships, for example, the conclusion of transactions when a third party is a digital platform, in such legal relationships, digital rights of citizens manifest themselves especially clearly and therefore require additional analysis.

Sulan Wong, Eitan Altman, Julio Rojas-Mora (2011) analyzed the development of technology and the transformation of rights considering the use of the Internet and concluded that citizens in modern society have digital rights, the volume of which can be compared with constitutional and civil rights, while there are digital rights that can be exercised both offline and online, and there are digital rights that cannot be exercised offline, for example, the right to be forgotten on the Internet. Warren B. Chik (2010) devoted to the work to Internet rights, these are rights that can be realized only in the digital environment, only with the help of the Internet, the list of these rights will be constantly updated, and the introduction of innovations will contribute to the creation of completely new fundamental rights of citizens, while they will be cross-border, generally recognized and it will be difficult to violate them since technologies such as smart contracts will be involved, which lead to self-fulfillment. Perhaps in the future, compliance with digital rights will proceed from the following conditions: "if ... then", that is, upon the occurrence of certain conditions, consequences occur, so the digital right to oblivion will be realized in automatic mode when in electronic form state bodies will notify of the death of a citizen, and providers will block social networks and other content in which a citizen was registered or for example, for inciting interethnic enmity in the online environment, there will be disconnection of a citizen who violated the law, also using a self-execution algorithm from the content for a certain period, etc. Mimi Tatlow-Goldena and Amandine Gard argued in their work that states should recognize the particularly pervasive, exciting nature of digital marketing with its appeal to children and young people, which limits the digital rights of citizens, as they suppress the will and force them to act within a certain beneficial direction for the manufacturer. The regulation should apply not only to advertising "spots" between programs but also to the entire range of promotion methods used in programs and media content (for example, advertising games, influencers), as well
as to all forms of marketing, including sponsorship, peer-to-peer distribution in social networks and more.

States should give up on the emphasis on advertiser intent (restricting marketing that is "child-friendly") or child audience proportions, and instead regulate media locations where the largest child audience is found to effectively limit exposure to children.

Research on marketing effects shows that advertising acts through emotional and covert pathways, and there is no evidence that the cognitive ability to recognize an advertisement and its compelling intent protect against marketing effects. Digital content has the potential to reduce user freedom and autonomy. Children's rights shall therefore be protected from the harmful effects of digital marketing and media. States should recognize the cross-border effects of digital marketing, which limit rights and emphasize the need for international cooperation. Cross-border cooperation is particularly important in regions where cross-border marketing is widespread due to cultural and linguistic proximity.

Cor Verdouw, Bedir Tekinerdogan, Adri Beulens, and Sjaak Wolfert considered the problems of digital rights on the example of digital twins. A digital twin is the digital equivalent of a real object, whose behavior and state are reflected in the virtual space throughout its life. The scope of the rights of the digital twin and the real citizen was analyzed by the authors using digital twins as a central means of managing the farm, and as a result, farmers can manage operations remotely based on (almost) digital information in real-time, instead of relying on direct observation and manual operations on the spot. This allows them to act immediately in the event of (expected) deviations and model the effects of interventions based on real data. The authors explore what digital rights digital twins have and define the concept for implementing digital twins.

Samer Faraj, Wadih Renno, and Anand Bhardwaj analyzed how the COVID-19 pandemic acted as an experiment in the natural violation of human rights, including digital rights. The pandemic has identified four major challenges in the area of digital rights violations: uneven access to digital infrastructure, the persistence of analogs in the process of digitalization, the fragility of uncontrolled digitalization, and panoramic surveillance. The sudden shift to digital work has revealed self-evident assumptions about the universality of digital access. The crisis also showed that many processes with a high degree of digitalization are still based on analog elements. The pandemic has also shown that many of the algorithms used in digitized inter-organizational processes are fragile due to over-reliance on historical models. Finally, the pandemic has violated fundamental digital privacy rights, as surveillance by organizations has spread to private and public places. Thus, the pandemic
has exposed the fundamental problems of digital rights violations, the transition to
digitalization, for example, in telehealth applications, while showing many positive aspects,
exposes a persistent digital divide that leaves socially and technologically marginalized
groups – rural, immigrant, uninsured, low-income, digitally illiterate, and elderly
populations – with even more limited access to basic services, and this indicates a violation
of the digital rights of certain categories of citizens.

However, digital rights as rights with certain characteristics and specific features, as well
as the protection of digital rights, have not received enough attention. The need for special
guarantees of basic digital rights, considering their vulnerability on the part of a wide range
of network actors, has not been sufficiently discussed. Digital rights in general terms
continue to be perceived as an indefinite and self-regulatory area that does not imply
sufficient clarity about the content of the duties corresponding to these rights. Prospects for
the study of digital rights as well as the legal status of an individual in the information
environment can be associated with the elaboration of specific directions for the
development of information law.

Methods

In the study, we used the general scientific dialectical method as well as the formal legal,
 systemic structural, formal-logical methods of cognition.

The general scientific dialectical method made it possible to comprehensively investigate
the essence of human rights in the context of the development of digital technologies,
analyze the most important problems of protecting rights that have arisen at the present
stage of development of society, formulate proposals that can contribute to the creation of
the most thorough and efficient system for protecting human rights.

With the help of the systemic-structural method, we described and analyzed the legal
support for the implementation of rights in the context of the digitalization of the social life
of society.

Without being limited to description and generalization, we aimed to define the principles
of digital rights and the category of "digital rights", as there is a profound difference
between the legal principle and the legal definition.

The legal principle is the result of analysis, the legal definition is the result of synthesis. In
some cases, the legislator gives definitions but this task must be solved by science.
The synergistic method was used to identify the features and main properties of digital rights; the method made it possible to isolate new rules and a new reality from the creative potential of chaos. Considering law as a variable phenomenon, it has been proven that law is constantly changing in response to new factors of reality. As the development of the Internet has led to the emergence of a new legal category – "digital rights", this entailed a change in legal approaches to the definition of property and non-property rights in the context of the development of the digital environment.

Results

Digital human rights are the concretization (through law and law enforcement, including judicial, acts) of universal human rights guaranteed by international law and the constitutions of states, concerning the needs of a person and a citizen in a society based on information. Digital rights are understood as the rights of people to access, use, create and publish digital works, to access and use computers and other electronic devices as well as communication networks, in particular, the Internet (Taylor, 2020). The right to an Internet connection, to communicate on the Internet is tacitly recognized by many countries as a fundamental right of modern times, when using the Internet, citizens not only communicate and conduct business correspondence but also have the right to access electronic public services, the right to vote, access to necessary services that can be provided remotely, for example, during the Covid-19 pandemic, when countries declared lockdown, schools, universities carried out the educational process remotely, many employees worked in the remote mode, that is, while at home, performed their duties using the Internet. In such conditions, depriving people of access to the Internet is a deprivation of basic constitutional rights, which, considering the development of digital technologies in their offline format, have moved to the online format.

In civil circulation, digital rights can be considered from the standpoint of property circulation to protect economic entities when concluding smart contracts, when using big data technologies, in cases of acquiring cryptocurrency, and in many other cases.

At the present stage, there is a tendency to "nationalize" the digital environment and to shift legal regulation towards control activities that involve interference in the field of digital rights. There are several directions for the implementation of control activities at present (Figure 1).
Figure 1 Directions for the implementation of control activities in the digital environment

The latest legislative proposals include the abolition of anonymity on the Internet, streamlining the registration procedure on social networks, the introduction of the obligation to use reliable data that allows the identification of the user's identity from the moment of account activation.

The rights exercised in the field of digital communication require special attention from the point of view of their civil legal assessment.

To efficiently protect digital rights, it is necessary not only to determine the scope and features of these rights the legal status of network actors (multi-stakeholders), which should be understood as numerous interested parties, which, in addition to users, include representatives of government, business, organizations (De Graaf, 2019). The emergence of a term that united such different groups of subjects and entailed scientific disputes about their equality in modern information and telecommunication processes, allows one to assume the presence of factors that equalize these subjects in terms of opportunities for the implementation of rights and obligations. It is necessary to highlight the factors that equalize the subjects in the digital environment (Figure 2).

Figure 2 Factors that equalize subjects in the legal environment

- control over personal and private data. In particular, the law introduced the possibility of storing, receiving and using information
- control over broadcasting and distributing information on the Internet
- control over anonymous activity on the Internet
- technological functionality of the Internet
- transboundary nature
- difficult user identification
- speed of distribution of information
- net neutrality principle – any information is important, regardless of the source
In the context of online communication, the capabilities of traditional influential (power) structures are limited by many other online sources of power as well as by the fundamental properties of the web – interactivity and unfiltered communication (despite its negative manifestations). Such interaction can be seen as strategic partnership or rivalry, cooperation, and competition. Thus, the problem of ensuring guarantees for the realization of rights is actualized, which is usually solved at the state level but when using information and communication technologies, the problem is exacerbated due to the limited possibilities for the impact of state institutions and legal means on technological processes on the Internet.

It is often simpler and easier to realize rights and freedoms via the Internet but at the same time one must consider the downside, the risks involved. Providing more and more new opportunities in the fields of education, health care, obtaining public services, etc., the Internet at the same time makes life more vulnerable in terms of, for example, interference with people's privacy, phishing, spreading fake news, stirring up conflicts of different levels, destabilization of the political situation in certain regions and entire countries, cybercrime, etc. Experts warn that with the use of appropriate technology in the field of civil law relations, there is theoretically the likelihood of a so-called "51% attack", when a group of network participants concentrate in their hands 51% of computing power and will thus be able to act in their interests, confirming only beneficial transactions for themselves (Wong et al., 2011). Therefore, one must pay attention to the existing possibilities of regulatory impact on the development of Internet communications and relations from the perspective of protecting the subjects' legitimate rights and interests.

The UN General Assembly Resolution dated 18 Dec. 2013 No. 68/167 "The Right to Privacy in the Digital Age" notes that the rapid pace of technological development enables people in all regions of the world to benefit from new information and communication technologies, while at the same time increasing the ability of governments, companies, and individuals to track, intercept and collect information that may violate or undermine human rights (especially the right to privacy). It is emphasized that the need to ensure public safety may justify the collection and protection of some confidential information but states must ensure that their international human rights obligations are fully respected (Wong et al., 2021).

According to the principle confirmed by the UN General Assembly, rights protected offline must be protected online. Thus, civil rights guaranteed by law are by default extrapolated to the digital environment, which implies their implementation within the existing legal
content and boundaries. However, it is necessary to note the existing restrictions on freedom in the digital environment (Figure 3).

<table>
<thead>
<tr>
<th>Types of restrictions on the freedom of expression in the digital environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restriction of freedom of expression for socially significant purposes</td>
</tr>
<tr>
<td>Economic restrictions (Internet access implies the presence of certain devices and the obligation to pay for services, which is not affordable for everyone)</td>
</tr>
<tr>
<td>Restriction of political freedoms (for example, both China and Turkey largely regulate access to certain Internet resources, including those that are posted online and can be accessed by users)</td>
</tr>
</tbody>
</table>

Figure 3 Types of restrictions on the freedom of expression in the digital environment

At the same time, the properties of the virtual environment may sufficiently require a reconsideration of the existing legal approaches to assessing the content and permissible limits of interference in the law that determine the legal capacity of an individual in the digital environment. In this regard, it is possible to identify the issue of the emerging risks legally regulating the actions of subjects in the online environment, the technical capabilities of which are almost unlimited in the transfer, storage, and use of information.

Discussion

The technogenic factor is crucial for the emergence and development of digital human rights, so the spread of digital technologies can tangibly affect human rights. The scenarios can be different. The global threat to freedom is among the pessimistic expectations, which arises in connection with the approach to the social state, which is called "electronic society", where "the border between "mine" and "not mine" is blurred". There is reason to think that in such a society, individual freedom will be increasingly limited "in the interests of the person himself/herself" (Emrah Karakilic 2019). It seems that the system of human rights will change depending on the conditions for their implementation. Digital rights arise with the advent of digital technologies.
The Internet has already become a new medium, but not just that. Since access to the Internet is a necessary prerequisite for using all the features of online, it can now be considered as an essential aspect of human freedom, proclaimed by article 1 of the Universal Declaration of Human Rights, since blocking a person's access to the Internet constitutes a serious interference with his/her freedom. Moreover, researchers see a problem not only when the use of the Internet for political criticism is faced with repression (as in China, North Africa, and the Middle East), but also when disconnection from the Internet occurs as a sanction for repeated copyright infringement (France and the United Kingdom).

The right to freedom of expression and the right to access information, guaranteed by article 10 of the Convention, lead today to the formalization of the right to access the Internet. In world practice, this happens in three ways: the recognition of the Internet as a universal and public service (Estonia, Spain), the consolidation of the right to access the Internet as a constitutional right (Greece, Portugal), and the recognition of this right by the highest courts (France, Costa Rica). Therewith, the right to access the Internet should distinguish at least (1) the right to connect to the Internet, in which the Internet is considered as a service, and (2) the right to access information on the Internet, including the right not to be disconnected from the Internet, i.e. the prohibition of illegal blocking of sites. In general, the right to information via the Internet implies the right to access the Internet, the right not to be disconnected, the right to freely search for information, the right to use the Internet safely, and the right to be protected from unwanted information. However, on the Internet, as well as offline, it is important to distinguish between allowing people to express everything they think, and thoughts that they cannot express freely. This is the rule without which a democratic society could not exist.

It is now difficult to talk about the global right to communicate without digital communication. A person who does not have access to the Internet today cannot take part in political life, and therefore cannot be an active citizen. Therefore, digital communication is used to legitimize the right of modern people to access the Internet. Article 8 of the Convention "The right to respect for private and family life" gave birth to the right to the protection of personal data. Its active development in the digital era has led to the emergence of the right to oblivion (the right of an individual to demand from a search engine operator to stop issuing information about the index of a website page on the Internet, allowing access to certain information about a given individual).

The main source of digital rights is the right to respect for privacy, but digital technologies have also influenced other fundamental rights. For example, freedom of expression, which is the basis of the right to access the Internet, has faced new ways of combating illegal content, which is implemented by the state with the participation of private actors. Freedom
of entrepreneurship has been enriched by the right to digital existence (the right to a domain name, the right to provide services via the Internet, the right to use digital tools — advertising, cryptography, electronic contracts, and now smart contracts). The right to reputation in modern conditions becomes the right to digital identity. Thus, digital human rights include the right to access the Internet, the right to be forgotten, and the right to be protected from unwanted information, which has already been legislated in various countries. The next step is the recognition of other rights. In the field of ensuring human rights on the Internet, the modern state (democratic and encouraging technological development) is designed to solve three problems:

- Not to hinder or restrict the exercise of human rights via the Internet (for example, not to censor).
- To protect the legitimate use of information and communication technologies from cyber-attacks by third parties.
- To guarantee and facilitate the legitimate use of information and communication technologies (access to the Internet for low-income people). The use of new digital technologies, including blockchain technologies, to ensure the turnover of property and transactions, has raised complex issues for legal systems that will cause a wave of discussion (Mimi Tatlow-Golden Amandine Garde 2020).

A feature of the information society, the formation of which is declared at the official level, is not only the active use of information and telecommunication technologies but also the involvement of large volumes of personal information in commercial circulation, which also casts doubt on the adequacy of implementing the right to privacy in the context of rapidly developing information technologies, the legal consequences of which are often unknown even to the developers (Sung, 2020).

The use of digital technologies has provided new and almost limitless opportunities for the state to exercise its functions, which inevitably jeopardizes the privacy of citizens, including when it manifests itself in public. Thus, "the systematic collection of information by secret services constitutes an interference with private life, even if this information is obtained in public places and if it contains information exclusively about the professional or public activities of a person. The same actions carried out through the use of GPS technologies, and the storage of data on the location of a person and his/her movements also constitute an invasion of privacy" (Graham Sherriff Daisy Benson Gary S. Atwood, 2019). In this respect, the courts are called upon to find a balance between private and public interests. The well-known ruling of the European Court of Human Rights in the case of Big Brother Watch and Others v. the United Kingdom, in particular, the Court's claim that mass
surveillance by perse does not violate the Convention, was controversial. The European Court has found that the decision to impose a mass interception regime to identify unknown threats to national security falls within the wide margin of appreciation afforded to the state in choosing how best to ensure that the legitimate aim of protecting security is achieved. The court emphasized that the new technologies are used by "terrorists and criminals", which helps them "avoid detection on the Internet". In the Court's view, the mass interception regime has a proactive function and is therefore effective (para. 314 et seq.) (Big Brother Watch and Others v the United Kingdom. Applications nos. 58170/13, 62322/14 and 24960/15. Judgment of 13 September 2018). The decisions of the European Court of Justice also do not prohibit the use of metadata interception as a preventive measure, but only if this interception is not mass, but targeted. The position of the European Court of Justice regarding the observance of human rights in the conduct of mass surveillance operations, as reflected in the decisions on the cases. The Centrum for Rattvisa and Big Brother Watch demonstrates a rejection of the progressive approach that has already begun to crystallize. The European Court of Justice has lowered the bar of the requirements imposed on states to protect the right to privacy, and this position may be fatal. Everything shall be analyzed in context. It is no secret that the terrorist attacks that took place in France had a significant impact on both the public consciousness and the position of the courts. European states have responded by adopting rather tough legislation. In France, at the end of 2015, the law on surveillance measures for international electronic communications was adopted, which allows intercepting all messages sent abroad or received from abroad, and storing the content of messages for one year, and metadata for six years. In Germany, on December 23, 2016, the law on the interception of foreign communications by the Federal Intelligence Service was adopted, which regulates the surveillance of foreign citizens. The changes were made to the Polish police law and some other acts regulating the use of secret surveillance in the same year. The legislative changes were approved in a referendum in Switzerland, significantly expanding the possibilities for establishing mass surveillance. In Egypt, in the summer of 2018, the Law on Combating Cybercrime was adopted to ensure national security, which tightens government control over the Internet. The Information Technology Act was passed in India in 2007. Partial censorship was introduced. The reason was the terrorist attacks in Mumbai, so the restrictions affected primarily political and extremist resources. Some sites are also blocked in Pakistan. The reason for this is usually ethnoseparatist materials.

Thus, it can be stated that at the mass level, the protection of privacy is weakening under the onslaught of digital technologies. As for the individual level, the trend seems to be reversed — the right to the protection of personal data is being given increasing attention.
in connection with the use of digital technologies. The world is talking about a new, third phase of personal data protection. In general, "issues of personal data intersect with almost all new areas of legal thought, up to the discourse associated with the "magic circle", i.e. the question of the "communicative boundaries of the action of law", passing along the line of fictional and real, play and non-play, serious and frivolous" (Jose Ramon Saura Domingo Ribeiro-Soriano Daniel Palacios-Marqués 2021). As a rule, the conflict of the right to the protection of personal data with other fundamental rights is resolved in favor of the former. There is an extensive judicial practice in this area. Let us turn to just one example, related to the competition of the right to the protection of personal data with the freedom of religion.

In one case, the European Court of Justice was asked whether members of the community of Jehovah's Witnesses comply with the rules for processing personal data in their activities when visiting homes and apartments (CJEU. Grand Chamber. Cases C-25/17. Proceedings brought by Tieto suoja-tuu tet tu. Request for a preliminary ruling from the Korkein hallinto-oikeus. Judgment of 10 July 2018). They write down, if possible, the names, addresses, and religious beliefs of the people they meet, and whether they want preachers to come to them. These records containing personal data are made and collected without notifying their subjects. Earlier, the European Court of Justice developed two criteria to determine whether private activities fall under the regulation of the European rules for the processing of personal data. Firstly, activities that make personal data available to an unlimited number of people can no longer be considered private (CJEU. Case C-101/01. Criminal proceedings against Bodil Lindqvist. Reference for a preliminary ruling: Göta hovrätt — Sweden. Judgment of 6 November 2003). It is in some way located in the public space. Secondly, activities that are directed outside the private sphere are subject to the requirements for the processing of personal data (paragraph 42) (CJEU. Fourth Chamber. Case C-212/13. František Ryneš v Úřad pro ochranu osobních údajů. Request for a preliminary ruling from the Nejvyšší správní soud. Judgment of 11 December 2014).

Concerning religious instruction activities at home, the application of these criteria is not obvious. On the one hand, the doorbell is a private contact, and the records made are not collected in a centralized dossier. On the other hand, since the purpose of this activity is to attract people to a spiritual community in which they do not belong, it is directed outside, beyond the private sphere. According to this criterion, the records of Jehovah's Witnesses still differ from the usual address book for home use. In addition, some of the collected data is transmitted to parishes, where it becomes available to an unlimited number of people (paragraph 45). Accordingly, the religious community, in solidarity with its members, falls under the status of those responsible for the processing of personal data (paragraph 75). In addition, home instruction is the main activity of this religious community. In this regard, the Court rejected the argument that the application of the rules on personal data interferes
with the exercise of religious freedom since the rights of third parties should not be violated. Recall that in general, there are two approaches to understanding personal data. In Europe, the issue of human rights and the Internet is discussed almost exclusively in the context of personal data, their regulation is still strictly protective. Here, the protection of personal data is a fundamental human right. Therewith, there is no individual ownership of their data, but only the right to control their processing, i.e. this subjective right is always associated with the activities of third parties (Cor Verdouw Bedir Tekinerdogan Sjaak Wolfert, 2021). At the same time, the Anglo-Saxon approach recognizes the economic value of personal data. Experts are trying to find out the industry affiliation of relations regarding personal data. They are looking for an answer to the question of whether the agreement on the use of personal data falls within the scope of civil law (Samer Faraj Wadih Renno Anand Bhardwaj 2021). Even state authorities sometimes refer to civil law, because it is more developed and therefore easier to apply. This is why civil law attracts many people. The "weakness" of public law turns lawyers to civil law. It is proposed to apply it to relations regarding personal data. "The very idea of applying the provisions of civil law to liability in the field of personal data cannot be unduly challenging in conditions when, for lack of other guidelines, state bodies themselves – so far selectively – turn to civil law" (Nathaniel D. Line, Tarik Dogru, 2020). If the state abandons the idea of public-legal protection of the personal data of citizens, do we not risk completely commercializing this area? Will citizens be able to profitably "dispose" of their data? In reality, the right to personal data is violated in all countries. In 2018, PrivacyInternational published a report on the practice of the police in the UK, which secretly downloaded all the content of the phones of not only criminals and suspects but also witnesses. The police do this with the help of special XRY software from MSAB, and it is already used by about 97% of police departments. In Canada, border police claim they have the right to check phones without a court order. It also uses products from MSAB and Cellebrite, which allow accessing the phone content even without knowing passwords or other authentication factors (Eric Van Der Horn Sankaran Mahadeva 2021).

Thus, fundamental rights (including personal ones) exercised in the digital communication space are undergoing significant changes. However, the urgent question is what these changes are – whether the changes signify only an indefinite expansion or, conversely, a narrowing of the scope of rights compared to their current assessment (including at the legal level) or indicate a change in the essence of fundamental law, the emergence of a new meaning of the law. The very statement of the problem of insufficient fundamental rights protection in the new conditions of digitalization at the highest level indicates the impossibility of recognizing their complete similarity to known rights and the need for a new interpretation.
A completely new mass phenomenon has emerged in the world – digital identification. Citizens go through this procedure when putting their finger on the phone, making any transactions, when our messengers do something – this is all an attempt to use digital means to determine whether a particular person is performing these actions or not. The question arises whether it is necessary to identify everyone in a continuous and end-to-end manner, or whether it is necessary to introduce some kind of restrictions. How to find a balance between private and public interests? This is a serious problem. Now commercial interests are at the forefront of many processes, it is extremely beneficial for commercial companies to identify everyone and everything, including through the use of big data technologies and artificial intelligence.

The UN resolution on the right to privacy in the digital age calls on all states to respect and protect the right to privacy in the context of digital communication. Civil law establishes the principle of the inadmissibility of arbitrary interference by anyone in private affairs without consent (Svantesson, 2018). In the environment of the Internet and network communication, the boundaries of private life are indefinite, as well as the question of implementing the condition for accessing personal information by obtaining consent. The principle of non-interference in private affairs, while retaining its formal meaning, can be easily violated in digital communications. It is also noteworthy that a significant idea of the development of a virtual reality zone is the realization of the right to anonymous communication and self-expression, that is, it is assumed that the Internet is designed to provide freedom of anonymous communication and, accordingly, the scope of the right to privacy in such a space should be wider.

The Recommendation CM/Rec (2016) of the Committee of Ministers of the Council of Europe on Internet freedom specifies that the State does not prohibit, in law or practice, anonymity, pseudonymity, the confidentiality of private communications, or the usage of encryption technologies. However, there are practically no guarantees for this, and the result is the contrary – given the technical accessibility of obtaining data in a global context as well as the natural desire to transfer the regime of public law control to the exercise of rights online, the concept of "private life" practically loses its meaning in terms of obtaining the person's consent to provide their data. Moreover, this practice is developing (Moyakine & Tabachnik, 2021). According to the Internet Research Institute, work has been underway in various countries for quite a long time to develop and implement tools for identifying citizens, including with the prospect of their global use (Gerry & Moore, 2015). The National Strategy for Trusted Identities in Cyberspace (NSTIC) adopted by the United States government seems particularly relevant in this regard. The United States is not the only country where the question of identification is posed on a strategic national scale.
Other countries include Estonia, Brazil, Singapore, and South Korea. The state is interested in user identification both from the perspective of security and from the standpoint of optimizing the interaction of the state with citizens as well as citizens among themselves and with legal entities (Nam, 2016). Therefore, it is necessary to introduce a new principle of protecting digital rights – the secrecy of digital identification since one must be sure: what one does, one does voluntarily, these actions are not imposed on one by anyone (of course, there are exceptions within the framework of the law), and all information that arises as a result of decisions one makes behind a computer monitor, laptop or smartphone screen, is used precisely for the purposes for which one is identified and the secrecy of identification will be ensured, information will not circulate freely as is now happening.

When discussing the principles of protecting digital rights, one should consider the use of facial recognition technologies and the use of the resulting images of citizens and such images should also be reliably protected. Therefore, the principle of security of data obtained through facial recognition technologies needs to be enshrined in law as the principle is important.

Given the vulnerability of privacy in the digital environment, the right to be forgotten is among the basic rights that require legal guarantees. In the Internet space, in the context of self-regulation and easy access to data, specific approaches to the use of personal information, including correspondence, are being developed to meet the needs of commercial circulation and the development of Internet resources. There is a trend towards a change in the content of the sphere of private life towards openness, and this process is practically irreversible due to such properties of information as indestructibility, which makes the right to be forgotten conditional since it is extremely difficult to guarantee this right; nevertheless, the principle of erasure should be enshrined as a basic one.

A global problem is the elimination of digital inequality which is manifested not only in the lack of a basic opportunity for some citizens to use new technologies (Chik, 2010), but also in the different levels of digital literacy of the population, and exacerbates another very serious threat: citizens cannot resist telephone or Internet fraud not just because the people do not know how to behave in such a situation, but also because the people are not aware of the existence of such fraudulent practice.

Therefore, the basic principles of protecting digital rights are as follows (Figure 4).
The digital personal data legal protection model should consist of four components – the right to informational self-determination; the right to ensure the integrity and confidentiality of information technology systems (IT law); the right to privacy of correspondence, postage, and telecommunications; the right to privacy of digital identity.

People can and should manage the impact that digital technologies have on social relations, including human rights. The regulation of information and communication technologies largely takes place through "trial and error", and not as a result of a predictive assessment of possible social consequences. Meanwhile, it is human rights issues that can contribute to the development of a holistic view of the regulation of new technologies. Human rights can become "beacons" for the regulation of information and communication technologies, indicating what goals should be achieved and what harm should be prevented following the principle of proportionality. Thus, the "right to informational privacy" is subject to protection as long as its implementation does not lead to interference with other protected individual or collective rights (Diego Valentinetti Francisco Flores Muñoz 2021). The idea of the universality of human rights can be harmoniously linked to the neutrality and universality of digital technologies. The essence of a person and his/her basic needs in the era of digitalization, are unlikely to change, as well as the basic values associated with them. It is human rights that can become a "unifying target perspective" when determining the attitude to various technologies, which involves analyzing whether their use corresponds or does not correspond to fundamental human rights, such as dignity, privacy, equality, freedom (N. Vigouroux E. CampoA. Van den Bossch 2021).
Conclusion

The sphere of digital legal relations is transboundary and virtual, therefore, ensuring the protection of digital rights should be carried out considering the special features of this environment in which subjects cannot always be identified, and objects are characterized as simulations.

Digital rights are obligations and other rights, the content and the exercise of which are determined by their specific features according to the rules and functioning principles of the information and telecommunication system. The holder of a digital right can be a person who can exercise the right. Implementation, exercise, including transfer, bail, encumbrance of digital rights in other ways, or restriction of disposal of digital rights are possible only in the information system without contacting the third party.

The authors identify the basic principles of protecting digital rights: the digital equality principle; the digital self-determination principle; the anonymous communication principle; the principle of confidentiality of private communications; the principle of privacy in the digital environment; the principle of secrecy of digital identification; the principle of security of data obtained through facial recognition technologies; the principle of erasure of digitalized personal information.

Further studies should include an analysis of the negative and positive obligations of the state that correspond to the rights realized in the digital communication environment.

References


