THE IMPACT OF THE INFORMATIONAL AND COMMUNICATION TECHNOLOGY ON THE REALIZATION AND PROTECTION OF HUMAN RIGHTS[1]

Maja NASTIĆ

Associate Professor, Faculty of Law, University of Niš

E-mail: maja@prafak.ni.ac.rs

Abstract

The application of information and communication technology (ICT) gradually takes over every aspect of contemporary society. The article's main goal is to observe how ICT reflects on human rights, realization and protection. First, we consider the changes that digital technologies develop in the constitutional systems and speak about digital constitutionalism. Then, we indicate the influence of the ICT on the human rights catalogue.

The impact of ICT is discussed from two perspectives; one refers to the new dimension of existing human rights, and the other relates to the emergence of new rights, so-called digital rights. We consider the right to access the Internet, the right to confidentiality and integrity of information systems, the right to informational self-determination and the right to be forgotten. These rights are developing in the constitutional direction. In this sense, we can talk about the gradual ''digitalization'' of the Constitution.

Since the digital age brings rapid changes, the legal system is not capable of following it. Therefore, we recognize the crucial role of constitutional courts in filling the gaps between normative and actual state.

***Key words**: Human Rights, ICT, digital rights, Constitution, Constitutional Court*

[1] This article is a result of research financing by the Ministry of Education, Science and Technology Development Republic of Serbia (contracting number 451-03-9/2021-14/200120)

Introduction

The revolutionary progress of information and communication technology (ICT), which began in the 60s of the last century, and is still in full swing, inevitably reflects on all spheres of the society in which we live. The application of ICT gradually takes over every aspect of human existence in the contemporary world. ICT unavoidable affects human rights and the legal framework for their protection. Therefore, the focal point of this article is to deal with the impact that modern technologies have on the existing concept of realization and protection of human rights to determine the extent to which the legal system can adapt to the changes brought by the digital age. We will try to answer whether the existing list of human right is elastic enough to absorb all the changes that happen in the modern world? Is it necessary to recognize the new rights generated by the application of new technology? To what extent is it necessary to transform existing human rights protection systems?

Information and communications technology (ICT) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications that have led to the application of electronic technologies for the information processing and communication, as well as platforms, built on such technologies (Khandagale, 2016). In this context, we will pay special attention to the Internet, as a global network that connects more than two billion people. The Internet is a medium that is accessible to everyone today. It has a major role in gathering information, downloading various content, and expressing views, exchanging ideas and communicating in general. The Internet is not just an information platform, nor an ordinary channel of communication; it is the centre of social communications: almost all areas of our lives are reflected in cyberspace: economy, politics, marketing, education, family, financial transactions, but also criminal activities, terrorism (Jevtović, Aracki, 2014, p. 320). The application of new technologies significantly shapes our everyday life, affects our habits, and in the conditions caused by the coronavirus, pandemic communication that takes place digitally is especially emphasized.

These technologies deeply permeate the current legal environment, and their impact is obvious on human rights. New ways of searching (data mining) and data warehousing, 'cloud computing' and the 'internet of things' are current buzzwords that are imposed as challenges to the realization of human rights (Jori, 2016, p.166). However, unlike other technologies, ICT is characterized by ambivalent action. On the one hand, applying these technologies can strengthen human rights and enable their effective realization. On the other hand, it exposes human rights to unprecedented risks. This is particularly affected by the fact that the law cannot follow the development level that characterizes new technologies. Many of these issues remain outside the reach of the legal system. The application of ICT significantly facilitates communication between people by offering new ways of transmitting data,

which were not known before. At the same time, freedom of expression may be prevented, due to the application of new technologies, by blocking content, filtering or, in the most dramatic sense, by cutting off access to these technologies. Scientific and technological innovations can lead to pollution, which is directly maintained, realising the right to a healthy environment and the right to health. But people can use new technologies to, e.g. reduced gas emission, prevented pollution of rivers and the like, which achieves benefits with the mentioned rights. Therefore, the critical challenge of human rights protection in the digital age is finding and maintaining the appropriate balance between the advantages and disadvantages that the application of technology brings, i.e. how to ensure that technological development moves within a framework that provides the well-being of human society. The essence would be to find *modus vivendi* in which the positive effects will be maximally emphasised and the adverse effects reduced to a minimum.

The application of new technologies is reflected in the realisation of human rights at the national level and defined by the Constitution. In this sense, the primary question that arises and to which we will try to answer is: To what extent do constitutional design and constitutional architecture change under the influence of ICT? What are the basic challenges that national law must face?

In the first part of the paper, we will analyze digital constitutionalism, which emerges in the conditions of globalization and ICT application. In the second part, we will talk about human rights in the digital age. We analyze the right to access the Internet, the right to confidentiality and integrity of information systems and the right to be forgotten.

1. Digital constitutionalism

The impact of new technologies on human rights at the international level was first expressed during the 1968 International Conference on Human Rights in Tehran (Coccoli, 2017. p 225). It resulted in the adoption of UN Resolution 2450 (XXIII) on 19 December 1968[2]. More recently, we mention the Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet[3], which affirms that the same rights people have offline must also be protected online, particularly freedom of expression. It also recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms. The Resolution on the right to privacy in the digital age[4] emphasising that 'in the digital age, technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to

[2] Human Rigths and Sceintific and Technological Developments (1968) UNGA 65: A/RES/2450 (XXIII)

[3] Resolution adopted by the Human Rights Council 26/13 The promotion, protection and enjoyment of human rights on the Internet

[4] Resolution adopted by the Human Rights Council on 26 September 2019

privacy, to freedom of expression and freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques'.

Under the auspices of the Council of Europe, several recommendations and strategies were adopted. We highlight Recommendation CM/Rec (2014)6 to member states on a guide on human rights for Internet users[5]. The member states are obliged to ensure to everyone in their jurisdiction the human rights and fundamental freedoms contained in the ECHR. This obligation also applies to the use of the Internet. It is public service; people, communities, public authorities and individuals rely on the Internet in their activities and have a legitimate expectation that these services will be available. States are expected to provide Internet users with access to effective remedies when their rights are restricted or violated. They should also encourage civil society to support disseminating and implementing the guide as an effective act for Internet users.

In the Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society[6], it was stated that the ICT was increasingly becoming an integral part of the democratic process offering a wider range of possibilities in exercising human rights.

The aspiration to establish an internet constitution is also present in the national context. In the last few years, national parliaments worldwide have been increasingly 'developing sophisticated normative approaches to Internet-related issues' (Santaniello et al., 2018, p. 321). In Brazil, for instance, the Marco Civil was adopted in 2014, which is considered a kind of digital Constitution (Bisson, Bochet, 2017, p. 18). Italy adopted the Declaration on Internet Right in 2015, stating that rights recognized in international human rights, the Charter of Fundamental Rights adopted in the EU and national constitutions have to be protected and applied on the Internet. The Declaration recognizes 'new' rights: the right to information self-determination, right to online identity, the right to online anonymity, the right not to be subject to decisions based on automatic processing of personal data and the right to be forgotten by search engines (Yilma, 2017, p. 124)

Bearing in mind that modern constitutionalism seeks to ensure human rights protection, it must adapt to the changes brought about by the modern age. Digital technologies generate the following changes in the constitutional ecosystem: 1. Increase the ability of individuals to exercise their fundamental rights, 2. Increase the risk of threats to fundamental rights, and 3. Emphasises the special role of private actors (Celeste, 2018). Digital technology expands the possibilities of information transfer, which, from the constitutional point of view, affects the rights based on the exchange of information, such as freedom of expression, freedom of assembly, religious freedom, etc. By applying new

[5] Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a Gude to human rights for Internet users (adopted on 16 April 2014)

[6] CM (2005)56 (adopted on 13 May 2005)

technologies, news about human rights violations can very easily and very quickly reach a vast number of subjects, which at the same time can raise awareness of the importance of respect for human rights. However, digital technologies also generate new sources of threats to fundamental rights such as blocking or restricting the transfer of information, monitoring and controlling the content of transmitted data, and illegitimate personal data use. The application of new technologies, in the foreground, emphasises the role of private companies that produce and manage these technologies and thus gain the power to influence the realisation of the fundamental rights of individuals. Indeed, this role of private actors is not new, but it gained particular importance in these circumstances. These circumstances require an extension of the original concept of constitutionalism in which private actors role' will be recognised.

Globalisation and the emergence of a transnational phenomenon, primarily the Internet, challenge state sovereignty and lead to new governance models. These models recognise the role of the non-state actors engaged in horizontal, decentralised relations, representing an alternative to hierarchical forms of government. This situation further poses a double challenge to constitutionalism. The rise of transnational governance models is blurring the line between public and private and between inside and outside the state. On the one hand, the private actors' involvement in public functions is the controversial trend to transnational business behaviour that poses a potential threat to human rights realisation. On the other hand, the permeability of territorial sovereignty weakens the state's authority as well as the core principles of liberal democracy such as self-governance, representation and popular sovereignty (McGrew, 1997, p.12).

The reactions of the existing constitutional systems to the challenges that arise due to the ICT application lead to the emergence of the so-called digital constitutionalism. Digital constitutionalism is used to denote the role that digital technology plays as 'the main catalyst of change in the constitutional environment' (Celeste, 2018). Digital constitutionalism is a set of ideas, values and principles that guide the normative framework to meet the challenges of applying new technologies. Digital constitutionalism is 'a common term to connect a constellation of initiatives that have sought to articulate a set of political rights, governance, norms, and limitations on the exercise of power on the Internet' (Redeker, Gill, Gasser, 2018, p. 303). Digital constitutionalism is also used as an umbrella term for linking a set of documents that seek to establish a charter of rights on the Internet. However, this Internet charter of human rights is not a constitution in the classical sense. It is rather a mechanism that sets the limits of state power towards its citizens.

The new constitutional discourse is not static but markedly progressive. Digital constitutionalism share core values and goals with modern constitutionalism but focuses on a specific context concerning the application of digital technology. In this sense, digital constitutionalism can be defined as

an ideology aimed at establishing and ensuring a normative framework of protecting fundamental rights and balancing existing powers in the digital environment (Celeste, 2018). Namely, the digital context includes a new role of private actors, which in unique circumstances, and the existing public actors, i.e. the state, can influence human rights protection. Private companies appear in the role of network intermediaries, enabling access and use of digital technologies and their products. The Internet space is mastered by powerful private companies such as Google and Facebook, which dictate further development with their additional investments. But, such action of companies poses a significant challenge to state sovereignty. It is clear that in cyberspace, the state is not nearly as powerful as in the existing physical-territorial framework. Besides, the corporations' activities go beyond the space of one state and acquire a global character. Therefore, the goal of digital constitutionalism is to limit the power of both categories of actors.

Digital constitutionalism is a kind of effort to respond to the challenges of the modern age and reduce private companies activities to a framework that nation-states can control to ensure adequate human rights protection. On the other hand, the application of technology (e.g. accessories to optical cables through which the flow of digital information occurs) can control telecommunications and Internet traffic. States can easily monitor mobile phones' movement, intercept calls or text messages, control information available on the Internet, or filter the content. It is known that China has one of the most sophisticated and widespread information control systems and filtering mechanism called the 'Great Firewall' (Coccoli, 2017, p. 229). This system blocks site searchers when the words 'democracy' and 'human rights' are used as key terms. Social networks like Facebook and Twitter are entirely censored and cannot be accessed, but domestic authorities control other social networks. The reasons for such censorship are the reasons for national security.

2. Human rights and the digital age

In the previous section, we analyzed the impact of digital technologies on the constitutions and constitutional systems. In this section, our focus will be on the changes taking place in the human rights catalogue. We can speak of at least a double effect of new technologies on human rights. Firstly, the existing human rights gain a new dimension in the context of applying new technologies, and there is a need for their reinterpretation. Secondly, we can see the emergence of new so-called digital rights. Technological innovations of the digital age significantly affect the realization of traditional rights, including a wide range of personal and political, socio-economic and cultural rights. The influence of new technologies on personal rights is especially pronounced in exercising the right to privacy, the protection of personal data, freedom of expression, inviolability of the apartment, the secrecy of communications, and the right to security, the presumption of innocence. The mentioned rights are the most endangered as a result of the poor handling of information technologies.

Freedom of expression is a right that has undergone significant transformations due to the action of new technologies, which have opened completely new types of communication. Namely, the application of the Internet and other new technologies enables the simple expression of opinions and expression of views available to millions of people in a split second. One of the basic questions that arise is how to regulate freedom of expression in the new circumstance. It is necessary to re-formulate this right or stick to legally neutral formulations.

The right to privacy has gone through notable reshaping and is one of the rights that are especially sensitive to the changes applying of new technologies. The right to privacy, its basic scope and content defined in the case Marcx vs. Belgium. Here, the ECtHR clarify the meaning and purport of the words ''respect for private and family life''. The ECtHR stressed for the first time, that in addition to the primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life. The right to privacy in the 'classical sense' refers to the certain space in the physical sense within the framework when the individual can develop freely, and he/she has the right to be left alone.

The digital age generates new sources that threaten privacy, but technology can be used to enhance and protect privacy. Namely, the application of the encryption system should contribute to that. Also, each of us must be aware that the content we create online can be accessed worldwide and compromise our privacy. The most drastic form of invasion of privacy through the use of electronic communications refers to the theft of a person's identity in order to gain material, or other befits (so-called Phishing) (Prlja, Reljanović, 2012, p. 96). This is often a consequence of the careless leaking of sensitive personal data in the internet environment (identity number, card credit number etc.). Therefore, today the right to privacy can be viewed from the angle of spatial, informational and communicative privacy. Spatial privacy refers to the home and other space in which the person lives (including workspace). Information privacy refers to the attachment, management and use of personal data. Communication privacy refers to personal records, correspondence, or any other form of communication. Under the influence of information technologies, the protection of privacy data took a new form: e-privacy, which is related to communication that is achieved via the Internet in any way (Boban, 2012, p. 587). The right to digital privacy extends to the online space and includes the confidentiality of communications and correspondence. This confirms the jurisprudence of the European Court of Human Rights, which under auspices of the right to private family life (article 8) includes e-mail at work, and video calls, internet chat, and some cases, metadata.

The inviolability of home in the conditions of application of modern technologies gained a new dimension. The home search does not have to be physically carried out in the home. Still, the search of the apartment, i.e. devices in the apartment such as computers, laptops and other electronic devices, can

be carried out 'remotely'. However, it should be equated the search undertaken by the judiciary in the network system with a physical search, and in that sense, it should respect appropriate procedural guarantees. When we talk about procedural guarantees, it should be noted that the presumption of innocence is at risk due to the existing practice of data collection for supervisory purposes and without the existence of prior doubt. The presumption of innocence suffers negatively from the application of modern surveillance systems. Namely, the accused will have to prove that the evidence obtained by applying modern technologies cannot be considered sufficient for him/her to be found guilty. This has been confirmed in the jurisprudence of the European Court of Human Rights. In the case of *S. and Marper vs the United Kingdom*, the Court has recognized that the preservation of any collected through modern surveillance technologies (fingerprints, audio recordings, video recordings, DNA profiles) may potentially damage right to the presumption of innocence even at a later stage in the trial (Coccoli, 2017, p. 233). On the other hand, states have an obligation to protect their citizens from criminal activities or crimes committed on the Internet or by using the Internet, especially when it comes to illegal access, falsification or other manipulation of digital identity, computers and data in it.

The Internet enables a new form of communication between citizens and their representatives. It significantly shapes traditional political rights, such as the right to civic initiative and the right to vote. The Internet significantly influences political participation by enabling new forms of political communication between citizens and their representatives and new opportunities for civic engagement. The Internet enables the participation of citizens in various online political debates, discussion forums, and the signing of an online petition, which can initiate the adoption of legal acts. Thus, the Internet becomes an important tool that enables citizens to build and strengthen democratic society. ICT is capable of mobilizing the population and strengthening civil society. Therefore, it is important to recognize this 'power' of the Internet at the state level and convey it into appropriate strategies for e-democracy, e-participation, e-activism. The impact of the Internet and social networks, in particular, has an important role in the stage of nomination and election campaign and is one of the most important forms of communication between candidates and voters. The application of new technologies changes the nature of freedom of the press, making it interactive in the circumstances of mass use of social networks.

Keeping in mind that e-government is being developed in new circumstances, enabling citizens to exercise their rights concerning various administrative bodies through the network, more and more talk about the so-called digital citizenship. It is also manifested as the right of citizens to have full access to data and services of public administrations, in a simpler way and without physical access to administrative bodies (Romano, Fioravanti, 2017, p. 58). Today, e-government enables access to registry books, payment of taxes, issuance of personal documents and other public documents, access to public

libraries and other databases in science and culture, contributing to significant time savings and easier realization of rights. An important advantage of e-government is its availability during 24 hours. The principle of single touchpoint makes it available to internet users with one access to all necessary services and administrative information (Dimitrijević, 2011, p. 219).

New technologies largely shape the business environment and significantly affect the exercise of the right to work and related rights, consumer rights, and copyright and intellectual property rights. The application of new technologies has repeatedly affected the sphere of labour relations. The need for many jobs, especially those performed by low-skilled workers, has ceased; traditional jobs have taken on a modern look in the new surroundings, and a whole range of new jobs and occupations have emerged. Also, teleworking and working from home is very present in the new circumstances, and the emergence of 'digital workers' and 'digital professions' is present (Reljanović, 2020, p. 765). The corpus of rights enriches the 'classic' labour law relationship that employees enjoy in the new conditions, which is important when employers have opportunities for more intensive control of employees. It is essential to point out the existence of the so-called 'disciplinary immunity' that employees enjoy in terms of facts from their private lives (Kovačević, 2014, p. 344).

The right to education in applying new technologies has acquired a new dimension which refers to online access to education and cultural, scientific and other similar contents. However, the Internet requires a new type of literacy from its users, the so-called digital literacy. This skill refers to using a wide range of internet tools, enabling access to digital education and knowledge to realize rights and freedoms on the Internet.

2.1. Digital rights

Modern technologies shape the existing catalogue of human rights in the sense that some new rights are adopted, such as the right to access the Internet, the right to be forgotten, the right to informational self-determination, the right to confidentiality and the integrity of telecommunication systems. We will refer to these rights as digital rights. Unlike traditional constitutional rights, characterized by stability and immutability, digital rights are flexible in nature. As technologies are constantly evolving and are incessantly changing, this is inevitably reflected in the so-called digital rights. However, here we want to emphasize that the mentioned new rights arise based on existing, established rights. Thus, e.g. the right to access the internet can be seen as a form of freedom of expression, and the right to be forgotten rests on the right to privacy. However, our starting point is that applying new technologies is a kind of 'evolution' of human rights. These rights are gradually developing, and that further development will lead to their gradual independence.

Keeping in mind that changes in the digital sphere occur with much greater intensity than the legal order can follow, constitutional courts often play

a key role in defining new rights. The courts are in a position not to hold on to technology to develop more sophisticated mechanisms to prevent harmful actions and not to wait for the legislator to decide how to distribute the burden of liability. This is not always a sign of judicial activism; it is a sign of the inescapable need to address contemporary issues (Polliciono, Romeo, 2016, p. 250); the reason for that may be found in the fact that countries are reluctant to change their constitutions due to the complex revision procedure. Even when they do, the motivation for the change is not technological development.

2.1.1. The right to access the Internet

The Internet is an indispensable part of our everyday life, and a large number of activities that we perform are realized on the Internet or through it. So far, there has been a lot of talk about the changes that the Internet is causing when realising and protecting human rights. But now we want to analyse whether access to the Internet can be defined as a right, and if so, what are its nature and its place in the legal system. In support of understanding the necessity of the right to access the Internet, arguments can be made that led to the emergence of freedom of the press. The appearance of the printing press was one of the greatest technological advances in the history of humankind, when it comes, above all, to freedom of speech, freedom of expression and freedom of information. It contributed to a revolutionary understanding of the concept of the freedom of expression and led to the recognition of a special right-the right to freedom of the press (Chawla, 2017, p. 58). Radio followed the press, television followed the radio, and then came the Internet, which took precedence and unites all media into one. The Internet is becoming a medium that plays a key role in achieving freedom of speech and the right to information; it is an important tool in political debate and encourages economic and cultural development.

The right to have access to the Internet satisfies the condition for it to be at least a moral human right (Sartor, 2010). This right refers to freedom or opportunity that is of great importance to each individual, such as participating in a network that unites humanity and provides unique opportunities for information, communication and participation. Obviously, such an opportunity did not exist before the Internet. Nowadays, the Internet has spread to the entire planet, and when the costs of installation and software have dropped, access to the Internet can be provided to the general population. Sartor further analyzes whether one can take a step. This right can be seen as a legal right-*de lege lata* that should already influence institutional decision-making rather than only a right *de lege ferenda*. Best put forwards two arguments supporting the claim that there is a right to have access to the Internet. First, the Internet has shown to be an important tool for achieving democracy goals. Second, since the Internet requires a symmetrical right to information, it qualifies to be recognized as a human right (Best, 2004). The right to access to the Internet has to be considered as a social right, or better, as an individual claim to a state's

performance, like services such as education, health and welfare (Frosini, 2013 p. 230)

The United Nations Human Rights Committee stated that any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information-dissemination system, including systems to support such communication, such as Internet service providers or search engines should be content-specific. Generic bans are not consistent with paragraph 3 Article 19 of the ICCPR. It is also inconsistent with this paragraph to prohibit a site or an information-dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[7]

One of the most important documents dealing with the right to access the Internet is the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[8]. This report researches key tendencies and challenges to the right of all individuals to look for and obtain impart information of all kinds through the Internet. Two components of the right to access the Internet are recognized; one relates to access to online content without restrictions, except in cases permitted by international human rights law. The second component refers to the availability of the necessary infrastructure and ICT. However, access to the Internet is seen in a broader context, as an important ,,tool'' that influences the exercise of human rights, but not as an independent human right.

European Union adopted Directive 2009/136/EC, which entered into force in 2011, introduced a positive obligation of European countries to ensure that all reasonable requirements for access to the Internet connection from fixed locations should be enabled with functional Internet access. Subsequently, the European Commission launched the action plan Digital Agenda for Europe.

The importance of the Internet has been recognized in the jurisprudence of the ECtHR, also. In the case Ahmet Yidrim v. Turkey[9], the Court reiterates that the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The Internet has become one of the principal means by which individuals exercise their right to freedom of expression and information.

Within the concept of the right to access the Internet, one should distinguish it negative and positive dimension. The negative dimension implies an obligation not to intervene with Internet access. This dimension includes the obligation of the state not to interfere with the right of citizens to access the

[7] General Comment No. 34 on Article 19 of the ICCPR, adopted at its 102nd session (11-29 July 2011)

[8] Report of the Special Rapporeur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27

[9] Appl.no 3111/10

Internet, except in exceptional cases that exclude unreasonable, inappropriate and illegal restrictions. A similar concept is already present in the freedom of speech, freedom of opinion and freedom of expression. The positive dimension is provided through the obligation to provide Internet access to all citizens. However, we cannot understand the right to access the Internet as an obligation of the state to provide its citizens with a laptop and wireless connection. Still, we cannot deny how important the Internet is as a tool for promoting and protecting human rights by disseminating information.

Estonia is the first country that recognized the right to access the Internet. The Telecommunications Act passed in February 2000 declared this right as necessary for life in 21 st centuries (Tully, 2014, p. 178). Today, Estonia has a strong infrastructure network and easily accessible wireless coverage. Education, voting, taxation, administration are sectors that have been significantly transferred to the online environment. Greece is the first country to recognize in its constitution the right of all people to participate in the information society. This was made possible after the revision of the Constitution from 2001 when Article 5a was added. At the same time, the obligation of the state to facilitate access to electronic and transmitted information, as well as production, exchange and distribution has been established. This means that both dimensions of the right to access the Internet have been recognized (Chawla, 2017, p. 66). Finish legislation from 2009 recognized the right of citizens to have access to the Internet (minimum bandwidth of 1 megabyte per second) (Frosini, 2012, p. 231). The law came into force on July 1, 2010, and defined the right to access the Internet for over 5 million citizens. Spain has recognized the positive dimension of the right to access the Internet since 2011 through the Law on Sustainable Economy. On 28 July 2015, the Declaration of Internet Rights was published in Italy. The declaration aims to establish a precise responsibility that reflects the reality of the new legal regime and to develop the constitutional rule that is the basis for the Internet. The Declaration seeks to recognize the basic principles of the validity of human rights in the digital world by pointing out their unique characteristics. The Declaration endorses rights such as the right to protection of personal data, the right to information self-determination, the right to inviolability of computer systems and computer domains, the right not to be the subject of personal data, the right to online identity, the right to online anonymity, and the right to be forgotten (Yilma, 2017, p. 124).

The Constitutional Council of France considered the right to access the Internet in the context of the rights protected by Article 11 of the Declaration of the Rights of Man and the Citizens. The mentioned article protects the free expression of thoughts and opinions as one of the most precious human rights. Every citizen is free to speak, write and print freely unless these freedoms are abused in cases provided by law. In Decision no. 580 (2009), French Constitutional Council affirmed that access to the Internet is considered a human right by declaring that freedom of expression implies freedom to access public online communication services (Coccoli, 2017, p. 243). Such a decision

of the Constitutional Council is of great importance both nationally and internationally. For the first time, the constitutional principle of freedom of expression has been extended to include access to the Internet as a part of freedom of speech.

The Constitutional Court of Poland considers that the protection of constitutional rights and freedoms in the context of using the Internet and other electronic means is different from protecting common forms of communication. The Internet is a complex phenomenon, and therefore, it should protect the activities of individuals resulting from its use in various ways. Expressing opinions and disseminating information using the Internet and other electronic devices are the same as traditional media, as defined in Art. 54 of the Constitution of Poland. In general, the Constitutional Court of Poland stands firmly on technical neutrality of constitutional protection (Kowalik Bańczyk, 2016, p.191). This principle implies that it should protect all individual rights and freedoms regardless of the technical means used to violate them.

2.2.2. The right to confidentiality and integrity of information systems

This right reflected the Constitutional Court's active role in adapting the legal system to the challenges of applying ICT. It was created in the jurisprudence of the Federal Constitutional Court. Assuming that existing rights are not sufficient to protect citizens from threats to their personalities in the modern world, the Federal Constitutional Court has created the right to confidentiality and integrity of information systems and the right to information self-determination. These rights are not recognized in the Basic Law (Grundgesetz) and result from judicial activism.

The Court brought a key decision on 27 February 2008, when it ruled on the constitutionality of a law authorizing the secret services of North Rhine-Westfalia to monitor and conduct an online investigation. In fact, the law allowed the secret services to carry out covert interception via the Internet and secret surveillance of the Internet and to access all its information technology systems secretly. The Constitutional Court found that the disputed provisions of the law were not under the Constitutions. But the rationale for this decision was what made a huge step forward in protecting rights in the digital environment. It was expected that the Court would extend its comprehensive search and seizure of the practice applicable to physical premises to the online environment. But the Court of Karlsruhe went a step further and found that existing rights were not enough to protect citizens' constitutional rights from all the potential loss of freedom that remote computer search could cause, and therefore created a new basic right: the right to confidentiality and integrity of information technology systems (Abel, Schaffer, 2009, p.111).

The right to confidentiality and integrity of information technologies protects personal and private lives from state access to information technology devices as a whole, not limited to individual communication events or stored data. The Court does not provide a list of systems covered by this right, aware

that it is changing rapidly under the influence of technological development. Therefore, the Court is trying to create neutral rules in order to maintain the new law in the future. The protective scope of the right to confidentiality and integrity of information technology systems applies to systems that, by themselves or interconnected, may contain personal data about a given person to the extent that access to the system facilitates insight into significant parts of lives and provides an image that reveals her personality. Such systems are, e.g. personal computers, laptops, mobile phones, electronic calendars. The Federal Constitutional Court considers that it is sufficient for the system to store personal data, not for that capacity to be used in a particular case.

However, the right to confidentiality and integrity of information technologies is not absolute and can be limited for preventive purposes and criminal prosecution. Any measure restricting this fundamental right must be appropriate to the violation, especially if carried out without the suspect's knowledge. The Federal Constitutional Court believes that a measure of restraining is proportionate if there is sufficient evidence that the basic value of a higher rank should be protected. Any such measure must be examined and validated by judges on a case-by-case basis to guarantee objective and independent pre-trial review and must be based on constitutional ground. This measure should not violate the core of private life, which, among other things, includes communication and information about inner feelings and deep connections.

2.2.3. The right to informational self-determination

The right to informational self-determination is another right that arose in the jurisprudence of the Federal Constitutional Court of Germany. This right is derived from the right to free development of personality (Art 2.1) and the general right to dignity (Art.1.1) and was first formulated on the occasion of the Census Act (Volkszählungsgesetz) in a decision passed on 15 December 1983. The right of informational self-determination, understood by the Court as 'the authority of the individual to decide himself, based on the idea of self-determination, when and within what limits information about his private life should be communicated to others' (Rouvroy, Poullet, 2009, p. 45).

This was one of the first and most famous articulations of a right to informational self-determination. According to the Court, this right arose from the fact that the states have more opportunities to collect process and use private data. That electronic data processing has been developed to such an extent that it can obtain a detailed picture of an individual's personality. The court stated that this especially concerns personal data that a person can neither reveal nor prevent. However, the Court considers that the right to information self-determination does not take into account the fact that individuals rely on information systems and develop their personality and thus entrust sensitive data to the system or inevitably provide such data simply by using the system. According to the Court, the right to informational self-determination traditionally deals with processing structured sets of personal data. Still, third-

party access to IT systems can lead to disseminating large-scale and potentially sensitive information about an individual, even without further data processing operations (Jori, 2016, p. 174). The stated right may be endangered even before a concrete attack on legal goods. Electronic data processing allows individual data to be suitable for unlimited storage and can be re-loaded at any time, as they can be combined with other data collections, creating a wide variety of possibilities for combing and using.[10] The scope of protection of the right to information self-determination is not limited to information that is sensitive in nature; they also have insignificant informative content, but which, according to their purpose and existing possibilities of processing and merging, can have a relevant effect on the privacy and freedom of behaviour of the affected person.[11]

The right to informational self-determination is not guaranteed without any restrictions. The Federal Constitutional Court considers that an individual does not have a right in the sense of absolute, unlimited rule over his data. The individual is formed within a social community and is instructed in communication. He/she has to accept the limitations of the right to information self-determination in the overriding interest of the community. Such restrictions must be introduced by law (enshrined in the Constitution) and in a way that takes into account the principle of proportionality.

2.2.3. The right to be forgotten

The right to be forgotten arose as a response to the rapid development of technology. It is a kind of counterbalance to the practically unlimited memory capacities of the Internet (Midorović, 2019, p. 283). In the world of ICT, when one piece of data reaches the digital airways, it isn't easy to delete it completely. The right to be forgotten is based on the tendency of citizens not to suffer the consequences of using data in the past (Andonović, Prlja, 2020, p. 103). The citizens have the right to have their data deleted or forgotten when they are no longer needed. Therefore, we should speak about the right of 'digital oblivion' to delete information and data registered on the Internet and social networks.

The right to be forgotten was formalized in the case-law of the European Court of Justice in *Google Spain*.[12] In this case, it was raised the questions about the obligations of search engine operators to protect the personal data of interested parties who do not want certain information to be found or be indexed and made available indefinitely to Internet users. The right to be forgotten is understood as the right that specific information about a given

[10] Decision of the FCC BVerfGE 65,1

[11] Decision of the FCC BverfGE 2074/05 1BvR 1254/07

[12] Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain Sl, Google Inc V. Agencia Espaῆola de Protección de Datos (AEPD), Mario Costeja González (C-131/12)

person is no longer available to the general public by being included in such a list of results. It is the right of an individual to have information concerning him to be deleted, limited or terminated, which are considered harmful or contrary to its interests. This right prevails over the economic interests of search engine operators. Unless there are specific reasons to support the view that there is a dominant public interest in accessing that information in the context of such a search, the person whose rights are at issue may request those links be removed from the list of results.

With the adoption of the General Regulation on Data Protection (GDPR), the right to erasure was expanded and regulated in more details than was the case with the previously valid Regulation. The data subject has the right to have the controller without undue delay allow him to delete personal data relating to him, and the controller has an obligation to delete personal data without undue delay if the exhaustive conditions are met. The right to be forgotten refers to the ability of individuals to erase, limit, delink, delete, or correct personal information on the Internet that is misleading, embarrassing, irrelevant, or anachronistic (Kelly, David, 2017, p.1). The right to be forgotten should ensure that people, not algorithms, are the ones who determine what information about them will be available online or when their name is entered into a search engine. It should bear in mind that the algorithms used by search engines have been perfected in recent years, that users can find the required data at lightning speed and get a complete picture of what or about whom they want to know in a few seconds. Today, it is almost impossible to delete content from the Internet, which cannot be the essence of the right to be forgotten. But it's a goal to make it harder to find that information. The right to be forgotten shifts this search for information from modern technological barriers to another dimension where these processes take place much more slowly. Today's users do not have the patience to search and search for information for a long time, and thus certain personal data is protected. The new European version of the right to be forgotten is based on the legal theory of intermediary liability, which views search engines as data controller, who has a responsibility to manage content online. This shift the concept of responsibility from the state to the private sector.

The right to be forgotten is recognized in the Serbian legislation. Detailed provisions are contained in the Law on Personal Data Protection[13]. According to the Law, the subject has a right to have his/her personal data deleted by the controller in the following cases: 1. Personal data are no longer necessary to achieve this purpose for which they were collected; 2. The data subject has revoked the consent on the basis of which the processing processed and there is no other legal ground for processing; personal data have been unlawfully processed; the personal data have to be erased for compliance with the legal obligation, or the personal data have been collected about the offer of information society services (article 30). If the controller has publicly disclosed

[13] Official Gazette of RS, No. 87/2018

personal data, his obligation to delete also refers to taking all measure, to inform other controllers that the data subject has submitted a request to delete all copies of his data. The Law also precisely regulates the case when processing is necessary and when deleting cannot be requested.

3. Concluding remarks

New technologies have enormous implications for the realization and protection of human rights. There is a close link between ICT, democracy and human rights and they all influence each other. The impact of new technologies hass reflected both constitutions and human rights. In a broader sense, this impact relies on modifications in constitutional architecture, which is known as digital constitutionalism. It should answer these challenges in the digital era and establish a balance in the constitutional system.

The impact of the ICT on human rights is observed from two perspectives; one refers to the new dimension of existing human rights, and the other relates to the emergence of new rights, the so-called digital rights. We recognize those rights: the right to informational self-determination, the right to access the Internet, the right to confidentiality and integrity of information systems and the right to be forgotten. All traditional rights enshrined in national constitutions and international conventions remain fully valid. However it is should be taken into account new forms of human rights, so-called digital rights and adjust the human rights protection system. Due to the fact that changes in the digital space are very intensive, the legal system is not capable to follow them at the same speed. Therefore, the constitutional courts have an active role in adjusting the legal system to the challenges that bring the ICT. The jurisprudence of the German Constitutional Court and the French Constitutional Council are the best examples.

The influence of modern technologies on human rights and their protection is complex due to its ambivalent action. On the one hand, the application of ICT can strengthen human rights and enable their effective implementation. On the other hand, human rights are exposed to risks without precedents. Therefore, the key challenge in protecting human rights in the digital era is to find a proper balance between the advantages and disadvantages that ICT brings and to ensure the technological development moves within the framework that confirms the welfare of human society.

Aware that this topic is very broad, we tried to point out the basic trend concerning the impact of the ICT on human rights. Therefore, the conclusions are given in the general sense. There is no single pattern and each country should find its way to meet the challenges of digital technologies. Normative adjustment is certainly necessary, but the role of the constitutional court is also important.

However, it is expected that this insight in the human rights trends could be useful for creating adequate legal framework in the Balkan states.

BIBLIOGRAPHY

Abel, W. Schafer, B. (2009). The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems-a case report on BverfG, NJW, 2008, 822. *Scripted*. 6 (1), 106-123.

Best, M.L. (2004). Can the internet be a human right. *Human Rights & Human Welfare*. 4. (1). 23-31.

Boban, M. (2012). Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu (The right to privacy and the right to access information in the modern infomation society) *Zbornik radova Pravnog fakulteta u Splitu*. 49.3 575-598. (translation of abstrct in English)

Dimitrijević, P. (2011). Pravo informacione tehnologije. Internet Law. (Information technology law (Information technology law. Internet Law) Niš. Pravni fakultet. (translation by M. Nastić)

Frosini, T.E. (2013). Access to Internet as a Fundamental Right. *Italian Journal of Public Law*. 5 (2). 226-234.

Jevtović, Z., Aracki, Z. (2014). Moć glasina i dezinformacija u kreiranju moralne panike na onlajn društvenim mrežama (The power of rumors and disinformation in creation of moral panic on online networks). In D. Todorović, D. Petrović & D. Prlja (Eds.). Internet i društvo. Niš, Beograd: Srpsko sociološko društvo, Univerzitet u Nišu.Institut za uporedno pravo.319-336. (translation of abstrct in English)

Jóri, A. (2016). Protection of fundamental rights and the internet: a comparative appraisal of German and Central European constitutional case law. In O. Policino, G. Romeo G. (eds.). The Internet and Constitutional law. London, New York: Routledge, Taylor & Francis Group. 166-176.

Khandagale V.S. (2016). Information Communication Technologies and Human Rights in 21st Century. Human Rights Education and Indian Scenario Retrieved 20 April 2021 from https://www.researchgate.net/publication/303895075_Information_Communication_Technologies_and_Human_Rights_in_21st_Century#fullTextFileContentreasearch gate

Kelly, M. David, S. (2017). The right to be forgottem. *University of Illinois Law Review*. 1. 1-64.

Kovačević, Lj (2014). Internet i privatni život zaposlenih: granice poslodavčevih nadzornih, disciplinskih i normativnih ovlašćenja (Internet and private lives of employees: the boundaries of employers' supervisory, disciplinary and normative prerogratives) In: Todorović, D. Petrović & D. Prlja (Eds.). Internet i društvo. Niš, Beograd: Srpsko sociološko društvo, Univerzitet u Nišu. Institut za uporedno pravo. 337-352 (translation of abstract in English)

Kowalik- Bańczyk,K. (2016). Constitutional adjudication on internet issues in Poland. In O. Pollicino,G. Romeo, G. (eds.) The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe. (pp.176-192). London, New York: Routledge, Taylor & Francis Group

Midorović, S. (2019). Pravo na brisanje podataka o ličnosti dostupnih na internetu. (The right to erasure of personal data available on the Internet) (*Zbornik radova Pravnog fakulteta u Nišu.* 84, 281-306. (translation of english summary)

McGrew, A, (1997) Globalisation and territorial democracy: An introduction. In A. McGrew (ed.) The Transformation of Democracy. London: Polity Press. 1-24.

Pollicino. O. Romeo, G. (2016). The Internet and constitutional Law. The protection of fundmanetal rights and constitutional adjudication in Europe. Routledge.

Prlja, D. Reljanović, D. (2012). *Internet pravo (Intrnet Law)*. Beograd: Institut za uporedno pravo. (translation by M. Nastić)

Romano, F. Fioravanti, C. (2017). Alati digitalnog građanstva: projekat Paesi Regije Toscana. In L.Luatti (ed.). *Ljudska prava u doba digitalnog građanstva.* III susret ljudskih prava: 58-62.

Rouvroy, A. Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy and Democracy. In S. Gutwirth.S. et al (eds.). *Reinventing Data Protection*? Springer.

Redeker, D. Gill, L. & Gasser U. (2018). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazzette.* 80.4. p. 302-319. doi/10.1177/1748048518757121

Reljanović (2020). Informacione tehnologije i izazovi u reformi radnog prava. (Information Technologies and Challenges of the Labour Law Reform) *Zbornik radova Pravnog fakulteta u Novom Sadu*. 2., 763-779. (translation of abstract in English)

Sartor, G. (2010). Human rights in the information society. Retrieved 20 March 2021 from

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724

Tully, S. (2014). A Human Right to Access the Internet-Problems and Prospects. *Human Rights Law Review.* 14 (2). 175-196.

Celeste, E. (2018). Digital Constitutionalism: Mapping the Constitututional Response to Digital Technology's Challenges. HIIG Discussion Paper

Series No. 2018-02. Retrieved 25 March 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219905

Chawla, K. (2017). Right to Internet Access- A Constitutional Argument. *Indian Journal of Constitutional Law.* 57, 57-88

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

Yilma, K. M. (2017). Digital privacy and virtues of multilateral digital constitutionalism-preliminary thoughts. *International Journal of Law and Information Technology.* 25, 115-138.

International documents*

Directive 2009/136/EC Retrieved 10 June 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136

General Comment No. 34 on Article 19 of the ICCPR, adopted at its 102nd session (11-29 July 2011) Retrieved 09 June 2021 from General Comment No. 34 on Article 19 of the ICCPR, adopted at its 102nd session (11-29 July 2011)

Human Rigths and Scientific and Technological Developments (1968) UNGA 65: A/RES/2450 (XXIII) Retrieved 22 April 2021 from http://www.worldlii.org/int/other/UNGA/1968/65.pdf

Resolution adopted by the Human Rights Council 26/13 The promotion, protection and enjoyment of human rights on the Internet Retrieved 24 April 2021 from https://www.right-docs.org/doc/a-hrc-res-26-13/

Resolution adopted by the Human Rights Council on 26 September 2019 42/3 Retrieved 2 April 2021 from https://undocs.org/A/HRC/RES/42/3

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 Retrieved 02.03.2021. from https://www.right-docs.org/doc/a-hrc-17-27

Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a Gude to human rights for Internet users (adopted on 16 April 2014) Retrieved 28 March 2021 from https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168044d5b31

Case law*

Decision of the FCC BVerfGE 65,1 Retrieved 25 April 2021 from https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200505_2bvr085915en.html

Decision of the FCC BverfGE 2074/05 1BvR 1254/07 Retrieved 25 April 2021from https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/03/rs20080311_1bvr207405.html

Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain Sl, Google Inc V. Agencia Espaῆola de Protección de Datos (AEPD), Mario Costeja González (C-131/12) Retrieved 20 April from

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Case of *S. and Marper vs the United Kingdom* (appl.no 30562/04 and 30566/04) Retrieved 28 March 2021 from https://rm.coe.int/168067d216

Case of Marckx v. Belgium Retrieved 09 June 2021 from https://www.womenslinkworldwide.org/files/2896/gjo-echr-marckx-en-pdf.pdf[14]

*Translation of all government and legislative material is from the official translation webistes as referenced in the bibliography.)