Cuestiones Constitucionales
Revista Mexicana de Derecho Constitucional
Núm. 46, Enero-Junio 2022
ISSN (versión electrónica): 2448-4881

Digital human rights: risks, challenges, and threats of global socio-political transformations*

*Цифровые права человека: риски, вызовы и угрозы глобальных социально-политических преобразований***

Recepción: 17 de agosto de 2021
Aceptación: 18 de noviembre de 2021

Sergey VOLODENKOV***
Sergey FEDORCHENKO****

ABSTRACT: *This interdisciplinary work identifies and analyzes the risks, threats, and challenges associated with preserving and implementing human rights in global socio-political transformations. The article pays attention to introducing artificial intelligence technologies and neural network algorithms into crucial spheres of social life. The authors analyze the potential for the formation of digital control regimes over population, the risks of implementing digital isolation projects, and the hybridization*

АННОТАЦИЯ: Данная междисциплинарная работа посвящена определению и анализу рисков, угроз и вызовов, связанных с сохранением и реализацией прав человека в условиях глобальных социально-политических преобразований. В статье уделяется особое внимание внедрению технологий искусственного интеллекта и алгоритмов нейронных сетей в важнейшие сферы общественной жизни. Авторы анализируют возможности формирования цифровых режимов кон-

* This research has been supported by the Interdisciplinary Scientific and Educational School of Lomonosov Moscow State University "Preservation of the World Cultural and Historical Heritage".

** Исследование выполнено в рамках Программы развития Междисциплинарной научно-образовательной школы Московского государственного университета имени М. В. Ломоносова "Сохранение мирового культурно-исторического наследия".

*** Professor, Faculty of Political Science, Lomonosov Moscow State University, Doctor in Political Science–Lomonosov Moscow State University, Russia. E-mail: *s.v.cyber@gmail.com*; ORCID: *https://orcid.org/0000-0003-2928-6068*.

**** Professor, Faculty of History, Political Science and Law, Moscow Region State University, PhD in Political Science–Moscow Region State University, Russia. E-mail: *s.n.fedorchenko@mail.ru*; ORCID: *https://orcid.org/0000-0001-6563-044X*.

of political regimes that involve the merging of government institutions with technological corporations that possess digital technologies. The authors show that integrating artificial intelligence and neural network algorithms forms a significant manipulative and propagandistic potential of influencing citizens' consciousness and the digital society value-semantic foundations.

троля над населением, риски реализации проектов цифровой изоляции и гибридизации политических режимов, предполагающих слияние государственных институтов с технологическими корпорациями, владеющими цифровыми технологиями. Авторы показывают, что интеграция алгоритмов искусственного интеллекта и нейронных сетей формирует значительный манипулятивный и пропагандистский потенциал воздействия на сознание граждан и ценностно-смысловые основы цифрового общества.

Keywords: *digital rights, socio-political transformations, digitalization, artificial intelligence, neural network algorithms, digital society.*

Ключевые слова: цифровые права, социально-политические трансформации, цифровизация, искусственный интеллект, нейросетевые алгоритмы, цифровое общество.

I. INTRODUCTION

Human rights are an essential foundation for protecting the freedoms and dignity of individuals. For hundreds of years, people have been forced to fight for their rights, defending them in many spheres of socio-economic and political life. The development of economic areas, productive forces, mass media, educational policy, and increased literacy among the population of different countries provoked a change in the balance of social forces, leading to the emergence and activity of new political movements and parties that took a course towards achieving equality. Equality before the

law, the right to personal inviolability, correspondence, freedom of movement, freedom of speech and press, freedom of assembly have entered the political agenda of most countries.

The development of the economic sphere and productive forces has led through scientific and technological progress to contemporary digitalization processes. Significant contradictions characterize this development. On the one hand, the rapid development of the Internet as a space of digital communications initially meant an increase in the potential for democratization of contemporary states, an expansion of opportunities for the realization of personal rights, including the right of citizens to receive information, freedom of communication and expression of their opinions. Digital communication provides ample opportunities for interaction between people in various spheres of the state and society functioning. It is no coincidence that many scientists and experts note the high possibilities of creating new forms of democracy based on contemporary information and communication technologies: monitoring democracy, a democracy of direct action, expert democracy, a democracy of joint action. The spread of the Internet in various parts of our world, its transition from the paradigm of the professional, expert Web 1.0 Network to the paradigm of the non-professional, pluralistic Web 2.0 Network has contributed to the emergence of confident hope for building a more just society and a state with elements of digital democracy, where the authorities will listen to the problems of citizens.

However, on the other hand, with the technological development and digitalization of key spheres of life of contemporary states and societies, it became clear that in addition to the possibilities for the realization of personal rights, contemporary technologies can be used in the opposite direction — to restrict the rights and freedoms of people, to form new models of political regimes based on digital control and surveillance of citizens, to block opportunities for accessible communication. The development of the economy has led to the phenomenon of digital corporations and platform capitalism, striving for monopoly control over granting the right to digital communication to citizens.

This contradiction, first, has led the scientific community to the academic discourse on special digital rights, which need to be protected by appropriate institutions. Second, this controversy has fueled the demand for new movements fighting to secure citizens' digital rights.

Professor of Complutense University of Madrid J. Bustamante recalls that rights have evolved over generations (Bustamante, 2007). The rights

of the first generation (the right to human dignity, immunity, procedural guarantees, political rights) received their impetus from the liberal constitutional tradition. The second-generation rights came from the humanistic and socialist tradition, more related to the socio-economic rights provided by the state (the right to access health care, education, work). Third-generation rights resulted from the activism of groups that opposed discrimination against ethnic, cultural, religious, and other minorities. In turn, digital rights are becoming fourth-generation rights. Bustamante rightly notes that these rights have become necessary, as the exclusion from the digital environment is now tantamount to exclusion from society.

The Internet has acquired the status of an independent ontological space of social and political communications, which has its own rules of the game and forms an independent digital reality. In this regard, new types of personal rights have arisen — digital rights.

It is no coincidence that the Chairman of the Constitutional Court of the Russian Federation Valery Zorkin, in his work, draws particular attention to the fact that the digitalization of social life has led to the emergence of previously unknown special digital rights: "A new law is emerging that regulates relations in the context of the world in numbers and artificial intelligence". Simultaneously, Zorkin understands digital rights 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 to the Internet. Also, the right to freely communicate and express opinions on the Web and the right to the inviolability of the private information sphere, including the right to confidentiality, anonymity (impersonality) of his already digitized personal information (Zorkin, 2018).

Thus, we find ourselves in a new situation where it is necessary to simultaneously support both traditional and new digital rights of citizens.

Professor of University of Pablo de Olavide I.-V. Lucena-Cid emphasizes that the implementation of the principles of "digital management" within the framework of the open government model did not provide for special measures that would consider the transformation of an "analog citizen" into a "digital citizen". The researcher considers that if the Internet has become a universal public good, an effective tool for implementing democratic practices, transforming the social and political order, then access to it should be guaranteed to citizens (Lucena, 2014). Lucena-Cid refers to the right to access the Internet as freedom of choice of software,

quality of service, equality and neutrality of the Internet, and a guarantee of digital inclusion.

In fairness, we should note that not all researchers believe that having access to the Internet guarantees the full development of democratic institutions. In his studies, the Australian political scientist J. Keane draws attention to the fact that communication abundance is not tantamount to democratization. In his opinion, the owner of new media is an essential factor in the communication environment (Keane, 2015: 206). Indeed, as the analysis of the existing practice of political activism of Internet users demonstrates, the development of the Internet does not always favor the democratization of politics (Bykov, Hall, 2011).

Moreover, a researcher from the Mexican Autonomous University of Aguascalientes, A. C. Galindo Núñez, captures specific discourses emerging in the digital space (blackmail, hatred, cyber-bullying) that undermine the very idea of digital rights and freedoms (Galindo, 2019).

Thus, for contemporary science, there is an important research problem of identifying and studying fundamental digital rights, as well as the obstacles that exist for the implementation of digital rights today. In this regard, the article was structured as follows: first, the authors consider the features of the formation of digital rights of a citizen in the context of global technological transformations, and also identify key risks, threats, and challenges in ensuring the protection of digital rights of citizens; further, the authors consider in detail the problems and obstacles associated with ensuring the implementation of such rights as the right to access the Internet, the right to privacy in the digital space, the right to communicate, freedom of speech, and access to information in the context of digitalization, the right to communicate with their own kind. A separate section of the article is devoted to each of these rights. In conclusion, the authors draw the main conclusions based on the study results and give a number of recommendations designed to arrest the risks in the field of legal regulation of digital human rights.

II. Digital rights in the context of technological transformations: problem statement

The intensive development of artificial intelligence technologies and algorithms for self-learning neural networks further actualizes the issues related

to whose interests digital communications will be used, as well as with what the global digital space and its national segments will become in the near future in terms of ensuring implementation rights and freedoms of citizens. It is no coincidence that the UN General Assembly Resolution No. 68/167 "The Right to Privacy in the Digital Age" notes that the rapid pace of technological development allows people in all regions of the world to use new information and communication technologies. However, simultaneously, it increases the ability of governments, companies, and individuals to track, intercept and collect information that can violate or infringe on human rights (especially the right to privacy) (UN. General Assembly, 2014).

It is no coincidence that international organizations have recently become more active in the field of adapting the legal framework to the peculiarities of algorithmic systems. It is necessary to note the work of the European Council. For example, as legal instruments developed within the framework of its activities, a manual on face recognition has appeared, recommendations for eliminating the influence of algorithmic systems on human rights.[1]

Moreover, we must state that digitalization and the introduction of "smart" digital technologies have generated several effects, to which it is crucial to draw the attention of contemporary scientists and specialists in the field of protecting personal rights (Popova *et al*., 2021). The formation of the digital space of social and political communications has given a new sound to the issues of the implementation of traditional personal rights and freedoms that have been formed in democratic regimes over the centuries.

However, speaking about the protection and implementation of personal rights in the digital space, we should note that the main driver of digitalization is not states but large technology companies pursuing their own interests, the main of which is profit maximization. Already today, we are witnessing the formation of new concepts related to the activities of technology companies in the digital environment — "platform capitalism" by N. Srnicek (Srnicek, 2020: 53), "surveillance capitalism" by S. Zuboff (Zuboff, 2019), "media imperialism" by O. Boyd-Barrett (Boyd, 2018). According to N. Srnicek, digital platforms that provide citizens with communication arenas for communication and exchange of opinions are interested in increasing the number of users. This strategy for digi-

[1] Council of Europe's Work in progress. Available at: *https://www.coe.int/en/web/artificial-intelligence/work-in-progress* (accessed on: december 20, 2021).

tal platform owners poses considerable risks to digital rights compliance, namely, merging the revenue function with the oversight function. The accumulating data of citizens (their digital footprints) are collected and analyzed to identify consumer behavior patterns, the study of which is highly beneficial for platform owners (Srnicek, 2020). The Internet architecture favors the formation of systems that seek to identify users and certify their activity (Martínez, Flores, 2016: 24-25). It is no coincidence that M. Castells wrote about the emergence of Networking Power — the power of organizations and entities over network systems (Castells, 2011). Thus, the right to the inviolability of a citizen's private information sphere is made dependent on the interests and cyber policy of digital corporations.

Here there is a risk — a higher priority of the economic interests of tech giants compared to the interests of citizens in the field of protecting their rights. Monetizing the communication activity of citizens in the digital space, making a profit from tracking the digital activity of Internet users, and the formation of big data arrays, based on an aggregation of digital traces, seem to us to be largely incompatible with the issues of observance of citizens' rights, including the right to privacy. After all, as T. Dunning wrote back in the 19th century, capital becomes bold if there is sufficient profit. Provide 10%, and the capital agrees to any application; at 20% he becomes lively, at 50% he is positively ready to break his head; at 100%, he tramples with his feet all human laws; with 300% profit, there is no such crime that the capitalist would not risk, even if only on pain of the gallows (Dunning, 2015: 35-36).

These fears are being confirmed today, according to Sh. Zuboff:

> During the past two decades, surveillance capitalists have had a pretty free run, with hardly any interference from laws and regulations. Democracy has slept while surveillance capitalists amassed unprecedented concentrations of knowledge and power. These dangerous asymmetries are institutionalized in their monopolies of data science, their dominance of machine intelligence, which is surveillance capitalism's "means of production", their ecosystems of suppliers and customers, their lucrative prediction markets, their ability to shape the behavior of individuals and populations, their ownership and control of our channels for social participation, and their vast capital reserves. We enter the 21st century marked by this stark inequality in the division of learning: they know more about us than we know about ourselves or than we know about them. These new forms of social inequality are inherently anti-democratic (Naughton, 2019).

It is evident that today tech giants act not only as drivers of technological development but also become new subjects of social and political life, influencing the formats, opportunities, and limitations of information and communication interaction of people in the digital space. In fact, today, not only the means of production — the technological platforms of social networks and the blogosphere — but even the results of production activities in the social media space (publications, news feeds, friends lists, etc.) are under the control of technology companies.

At any time, any user can lose access to their accounts, content, and own social circle, even if it numbers in the millions of users. This state of affairs is clearly reflected in the situation with former US President D. Trump, whose accounts in leading social media were blocked, and he lost access to his audience. The very right to communication is beginning to be privatized by digital corporations with a transnational character.

Thus, if in traditional states the main regulatory and supervisory functions are carried out directly by the state, which regulates the activities of citizens in the legal space and ensures the protection of their rights, then in the contemporary digital space, such functions are carried out mainly by technology companies that own key communication platforms.

Will tech giants also be careful about respecting citizens' rights and protecting the public interest? The answer to this question seems to us to be one of the key ones for determining digital personal rights development vectors. Indeed, in the event of abuse by technology corporations, the potential of digital deprivation of a citizen, digital erasure of individual, digital restrictions on unwanted persons at the sole discretion of decision-makers at the corporate level becomes real. What digital rights, in this case, can we really talk about? Against this background, the urgent task is to ensure digital literacy of the citizen, associated with the assimilation of democratic and technical competencies. For example, the Council of Europe Committee of Ministers on Digital Citizenship Education recommendations focus on information literacy, critical thinking, participatory skills, ethics, and empathy.[2]

Another challenge in the field of protecting personal rights in the digital space is, in our opinion, the intensive introduction of artificial intelligence

[2] Recommendation CM/Rec(2019)10 of the Committee of Ministers to Member States on Developing and Promoting Digital Citizenship Education. Available at: *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168098de08* (accessed on: december 20, 2021).

technologies and algorithms for self-learning neural networks in the key processes of the functioning of the state and society. First, we mean the potential for forming a hybrid subjectness within the framework of which the mass user will be forced to communicate not with living people but with virtual personalities operating based on using "smart" technologies. After all, it is much cheaper to use artificial personalities instead of real people in the processes of providing services, the interaction between authorities and citizens, making court decisions.

Here we see significant risks, threats, and challenges associated with the hybridization of digital information and communication space. The high realism of artificial simulacra formed based on the use of neural network algorithms already today poses a problem of increasing manipulative potential in the processes of using deep fakes. The potential for simulating and simulating socio-political reality may turn out to be high enough to plunge billions of people into a distorted, fictional reality, divorced from objective reality.

For this reason, in 2019, as a result of the concerns of the Council of Europe, the Declaration of the Committee of Ministers on the manipulative possibilities of algorithmic processes was passed.[3] On the one hand, the document highlights the threats to the right of people to form their own opinions, regardless of algorithmic systems. On the other hand, it is proposed to minimize these threats by initiating public debate and discussion of these problems, disseminating critical digital literacy skills among citizens, conducting additional research, and providing voters with equal access to political information. The Venice Commission of the Council of Europe in 2020 has increased its focus on the correct use of digital technology in politics, proposing to maintain electoral integrity through a mechanism to periodically review regulations and rules related to internet intermediaries and political advertising.[4]

[3] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. Available at: *https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b* (accessed on: december 20, 2021).

[4] CDL-AD(2020)037-e. Study-Principles for a fundamental rights-compliant use of digital technologies in electoral processes, approved by the Council for Democratic Elections at its 70th meeting (online, 10 December 2020) and adopted by the Venice Commission at its 125th Plenary Session (online, 11-12 December 2020). Available at: *https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)037-e* (accessed on: december 20, 2021).

Currently, UNESCO is also initiating discussions on AI. The 2019 UNESCO document emphasizes that organizations and individual countries should not tackle AI alone but should definitely build close partnerships. The report draws attention to the fact that AI problems cannot be given only to representatives of the expert community; all interested groups (families, teachers, students, universities, schools, politicians, industry) must be involved in the discussion.[5]

Additionally, the concept of algocracy, which explains the role of "smart" algorithms in contemporary social relations, has acquired great importance for studying threats to digital rights (Aneesh, 2006). It is unclear whose interests will be pursued by neural network algorithms, actively implemented today in digital communications. What will be the value and semantic guidelines of artificial neural network personalities if they are admitted to the processes of interaction with real people in the vital spheres of the functioning of society? Will the neural network support the principles of justice that are critical for the existence of human society for centuries? Or the primary criterion for decision-making and communication with people will be the expediency inherent in the algorithm (reducing costs and costs, increasing controllability, the efficiency of decision-making)? Additionally, the question arises about what criteria will be guided by a self-learning neural network, whose functioning is based not on the use of human experience but solely on data analysis and autonomous self-learning? After all, there are social biases in all artificial intelligence systems, and artificial intelligence, and machine learning — "it is just the Wild West, no matter how skilled you think your data science team is" (Vincent, 2021).

In this regard, a clear example is a system based on artificial intelligence technologies for creating thumbnails of images uploaded by users on Twitter. As the results of the analysis of the operation of this system found out, when creating a preview, the algorithm prefers thin, young, with light or warm skin tone, with a smooth skin texture and stereotypically feminine facial features. Additionally, the system turned out to be biased against people with white or grey hair (age discrimination) and finally "prefers" English to Arabic in images. The researchers note that the prejudices of

[5] Artificial Intelligence for Sustainable Development: Synthesis Report, Mobile Learning Week 2019. UNESCO. Available at: *https://unesdoc.unesco.org/ark:/48223/pf0000370308* (accessed on: december 20, 2021).

neural network algorithms reinforce prejudices in society, literally "cutting out" from the life of those who differ from the "norm" in weight, age, skin color, language used to communicate. These "prejudices" are more common than one might think.

It is no coincidence that researchers and specialists pay much attention to the social and moral aspects of introducing "smart" technologies in most technologically developed countries. For example, the European Regulation on the Protection of Personal Data (Regulation…, 2016) is gradually expanding the assessment of the impact of digital technology assessment on human rights in general, including social and ethical aspects (HRESIA-Human Rights, Ethical and Social Impact Assessment) (Mantelero, 2018).

Thus, a particular concern is caused by the axiological aspect of introducing artificial intelligence technologies and algorithms for self-learning neural networks in the processes of information and communication interaction in the traditional spheres of social and socio-political life. Today, the situation with how human rights will be interpreted in a meaning and value sense by artificial intelligence and neural networks in the case of their decision-making in the social sphere looks uncertain.

In a special study on the ethics of artificial intelligence under the auspices of UNESCO (2019), much attention is paid to the risks of disinformation, "fake news", the use of content moderation to incite "hate speech", the polarization of opinions through algorithms (paragraphs 70-73). UNESCO is updating the problem of the role of algorithms in violating gender equality, issues of bias in systems for hiring (the example of Amazon is considered separately, paragraphs 90-93).

Therefore, the document proposes recommendations (paragraphs 106-107): AI systems should assume inclusiveness (involve many parties in the discussion of emerging problems), human control, transparency, explainability, democratic principles, consideration of human rights and ethical principles by developers, accountability of governments on the use of AI systems for security, police, and intelligence.6 Such recommendations, of course, already need to be taken into account by contemporary states and digital corporations.

As a result, based on reports and research in 2021, the UNESCO General Conference passed a special recommendation on the ethical issues of

[6] Preliminary Study on the Ethics of Artificial Intelligence. UNESCO. Available at: *https://unesdoc.unesco.org/ark:/48223/pf0000367823* (accessed on: december 20, 2021).

artificial intelligence. The document reflects the following recommendations: legal education in the context of the proliferation of AI technologies, respect for privacy (therefore, before the implementation of AI systems, it is important to assess them for compliance with this principle), respect and encouragement by all AI actors of freedom of expression, accessibility of information regarding curation, moderation and automated content generation (p. 112-115). States are instructed to ensure the functioning of human-machine interactions, taking into account the observance of human rights (para. 126). At the end of the document, the issue of monitoring and methodology for evaluating AI systems by UNESCO is raised (paragraphs 131-134).[7] The UNESCO project was supported unanimously by representatives of 55 states.

The recommendations accompanying the Montreal Declaration Responsible AI note that it is important to pay attention to the problem of automatic decision-making systems that have severe consequences for humans, as well as tracking and recording systems should be developed that can help developers to the source of the algorithm and identify responsibility when a problem occurs.[8]

The Asilomar AI Principles,[9] signed by scientists from many countries, also cite the following components as recommendations: adherence to the principles of system security for humans, human values, judicial transparency, developer responsibility, personal confidentiality, and the priority of human control over systems. There is a call to abandon the arms race in a new type of weapon. The existential risks of self-improving AI systems are emphasized.

Finally, accelerated digitalization in the context of the COVID-19 pandemic deserves special attention. The rapid introduction of digital technologies in the field of mass information and communication interactions in a forced mode has significant differences from digitalization, which

[7] Report of the Social and Human Sciences Commission (SHS). UNESCO. Available at: *https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14* (accessed on: december 20, 2021).

[8] Montréal Declaration Responsible AI. Overview of International Recommendations for AI Ethics. Part 2. Available at: *https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_003a48f375c444a99e79a5786436a070.pdf* (accessed on: december 20, 2021).

[9] Asilomar AI Principles. Available at: *https://futureoflife.org/2017/08/11/ai-principles/* (accessed on: december 20, 2021).

occurs in an evolutionary format. Even though human thinking remains broadly analogous, the rapid immersion of billions of people in the digital space over the past year and a half has its consequences. For example, some experts say that traditional "analog" communication is becoming an unaffordable luxury available only to elite members (Bowles, 2019). If at the previous stages of technological development the smart devices possession and digital technologies using acted as a kind of marker of success and status, now digital communications, digital education, digital consumption of services are becoming the prerogative of the mass consumption sector. An ordinary person is often deprived of the opportunity and right to traditional communication.

Thus, we can state a wide range of threats and challenges associated with the contemporary digitalization of traditional spheres of life of the state and society and the introduction of "smart" technologies of artificial intelligence and neural networks in them. Obviously, this spectrum includes significantly more problem points in addition to those described in this work. Therefore, it seems essential today to draw the attention of scientists, specialists, and experts to the potential risks in ensuring human rights that accompany the processes of global technological transformations in the contemporary world.

III. The right to access the Internet: does communication abundance lead to digital democracy?

As we have already noted, digitalization, as a concomitant phenomenon of the development of platform capitalism, does not bring only advantages but also creates risks, challenges, and threats to human rights. The right to communication is beginning to be privatized by digital corporations of a transnational nature. Digital rights are widely violated by various actors, depending on digital corporations, and facing government censorship. Various digital divide causes hamper the digital right to access the Internet among social groups.

At the same time, there is both an internal and international digital divide. Additionally, using Russia's example, individual researchers found that the digital divide is more pronounced between non-users and Internet users than between Internet users themselves.

Of course, the digital inequality depends on such reasons as the poor development of the IT economy sectors, the lack of investment (including government) in the development of the country's communications, social inequality in a particular country (which is manifested in the fact that only wealthy groups of the population have access to the Internet). Also, the reasons may be insufficient information and technological development of certain country regions due to natural-geographical, climatic factors. Disparities in the development of information technology communications affect the picture of similar inequalities between countries in the development of e-government.

Access to the Internet is by far the most basic digital right. Without it, implementing other rights in the digital plane is impossible. J. Keane writes that only in countries with "communication abundance" such phenomena as "unelected representatives" and "cross-border public" have emerged (Keane, 2015: 206). By "unelected representatives", Keane means the authoritative defenders of public interests and values, whose activities lie outside the plane of the legitimate electoral field. These can be bloggers, well-known writers, leading video blogs, and commenting on the situation with the censorship of the Web and digital rights. Whereas under the "cross-border public" Keane considers a subpolitical phenomenon of a global audience, to which media conglomerates (CNN), digital corporations (Facebook), political regimes can appeal (for example, American President Barack Obama once turned to "global citizens"[10]) against other corporations and political regimes. It is clear that such largely artificial cross-border constructs are not harmless and in conflict with the paradigm of sovereignty. We must not forget about the risk that the discourse on digital rights in the cross-border plane can lead to destructive consequences, fraught with the delegitimization of regimes and the loss of their sovereignty.

Thus, J. Keane notes that communication abundance does not automatically lead to democracy (especially digital democracy). Optimal implementation of the "right to access the Internet" requires a long-term government policy to overcome the threats of digital inequality, the existence of a

[10] "11 Times President Obama Spoke to Global Citizens in his Farewell Address". *Global Citizen*. Available at: *https://www.globalcitizen.org/en/content/11-global-citizen-values-obama-embraced-in-his-far/* (accessed on: december 20, 2021); "12 Times President Obama Called on Global Citizens in the State of the Union". *Global Citizen.* Available at: *https://www.globalcitizen.org/en/content/12-times-president-obama-called-on-global-citizens/* (accessed on: december 20, 2021).

developed digital infrastructure (not only dependent on corporations), and regular digital education.

If a person in contemporary digital conditions treats his rights as something unshakable and stable, he will simply lose them (McQuire, 2018: 35-37). Therefore, it seems crucial to develop such socio-economic infrastructures and digital practices of democracy that will stop serious risks of digital inequality in the future.

As counterarguments, it is still important to refer to real attempts to adapt the legal system in the context of digitalization in order to preserve and develop democratic institutions. Such attempts are being made at the level of international organizations.

For example, the work of the Ad Hoc Committee on Artificial Intelligence (CAHAI) at the Council of Europe (established in 2019) should be noted. Since its inception, CAHAI has analyzed the challenges and opportunities of the legal framework for the creation and implementation of AI, taking into account the established European standards in the field of democracy, human rights, and the rule of law. The committee pays special attention to the protection of people with disabilities, gender mainstreaming, and creating cohesive communities.[11] However, in its recent joint statement, CAHAI regrets that many states aim to weaken potential safeguards to protect citizens affected by AI systems. Instead, states seek to narrow the scope of any legal framework. CAHAI urges the Council of Europe to ensure the openness and inclusiveness of the AI legal framework for civil society representatives.[12]

At the same time, back in 2020, PACE, in its recommendation to the Committee of Ministers of the Council of Europe, emphasized that private companies that develop and apply AI only turn to self-regulation policies in the absence of a legal basis. The Committee of Ministers agreed with PACE's thesis on the emerging link between AI and the future of democracy, taking note of the results of CAHAI's work.[13]

---

[11] *Ad Hoc* Committee on Artificial Intelligence-CAHAI. Available at: *https://www.coe.int/en/web/artificial-intelligence/cahai-1* (accessed on: december 20, 2021).

[12] Joint Statement on the *Ad Hoc* Committee on Artificial Intelligence (CAHAI) in the Council of Europe. Available at: *https://algorithmwatch.org/en/joint-statement-cahai/* (accessed on: december 20, 2021).

[13] Need for Democratic Governance of Artificial Intelligence. Reply to Recommendation. Doc. 15346. 26 July 2021. Available at: *https://pace.coe.int/en/files/29384/html* (accessed on: december 20, 2021).

In this regard, we should not forget about the emerging phenomenon of "mediocracy" (Smorchkov *et al*., 2020), when large news conglomerates, being in fact, influential digital platforms and active customers of digital technologies, begin to establish a format of political news coverage convenient for their purposes and the order of political competition. Unfortunately, "mediocracy" does not always favor the development of democracy but rather provokes populism.

IV. Digital privacy *vs*. Digital panopticon

Today, ensuring and protecting citizens' right to privacy in the digital space is a significant concern. Many experts note that at the mass level, privacy protection is weakening under the onslaught of digital technologies (Florimond, 2016: 388-392). This situation is associated with several factors at once, which we will try to analyze.

First, we are talking about the rapid development and implementation into the actual practice of Big Data technologies, allowing, based on the collection and processing of "digital traces" of network users, to perform a practical analysis of the personality of each individual in various parameters, including psychological, value, behavioral and many others. Psychological characteristics, behavioral preferences, sexual orientation, religion, and many other aspects of personal life are no longer private information belonging exclusively to a person. All these data become available for study and use for owners of big data arrays and their customers.

So, back in 2013, M. Kosinski proved that the analysis of 68 Facebook likes enough to determine the subject skin color (with a 95% probability), his homosexuality (88% of the probability), and adherence to the Democratic or Republican Party of the United States (85% of the probability). The data even made it possible to determine whether the subject's parents divorced before his majority or not (Kosinski *et al*., 2013). According to Kosinski, people do not understand that the information we are happy to share is enough for a good algorithm to reveal the personality characteristics that we might not want to disclose, like political views, religion, IQ, sexual orientation, and the like. Simultaneously, we cannot live in this world without leaving behind a significant number of digital traces (Hutchinson, 2015).

In his latest work, M. Kosinski convincingly demonstrates that neural network algorithms, based on face recognition technologies, can determine citizens' political preferences with a high degree of probability (Kosinski, 2021).

The entire contemporary digital space (or rather, the totality of users located in it) can be described and structured at the level of technologically created and accumulated data arrays available to global corporations like Google, YouTube, Apple, Facebook, Twitter, Amazon. Microsoft, Instagram.

As a result, today, contemporary society is faced with the problem of maintaining personal privacy and privacy on a global scale. This problem is accompanied by a technological transition to a post-private future, within which the phenomenon of post-privacy only complements the already existing phenomenon of post-truth. It creates a closed digital framework for the existence of an individual, in which a closed cycle of obtaining personal information about an individual and collecting private information about the individual characteristics of a citizen is carried out. Such information allows to exercise control, apply personal sanctions concerning unwanted individuals.

At the same time, such a digital fixation of the psycho-type and various individual characteristics of a person based on his digital behavior does not require consent. It can be performed in a hidden mode, for example, to form new social norms, values, meanings, ideas, and expectations in the interests of the actors who control Big Data. We can describe Big Data as digital data sets from various spheres of society's life combined into a single system, which allows describing and structuring in real-time mode the necessary group of people and every citizen who has shown any unwanted activity in the digital environment. For this reason, in 2015, PACE proposed a number of recommendations to ensure privacy protection: to agree on an "intelligence code" (among the EU member states), strengthen cooperation with other countries, and study Internet security problems.[14]

The equally important problem is that Big Data, in fact, are private resources that can be sold or transferred to almost any actor to achieve their own interests. In our opinion, the hidden collection of personal information and its uncontrolled distribution is a serious threat to the individual

[14] Mass Surveillance. Recommendation 2067 (2015). Available at: *https://pace.coe.int/en/files/21694/html* (accessed on: december 20, 2021).

in the contemporary world. Imagine that Big Data arrays have become available to a dictator or representatives of an international terrorist organization. Obviously, in this case, there are risks of losing the privacy of personal life and an immediate threat to the lives of many people. Big Data is steadily becoming a digital resource for efficient control over citizens. Additionally, digital data about users can be stored indefinitely, resulting in a severe threat to the realization of the citizen's right to be forgotten. Scientists note that the right to be forgotten has become a matter of paramount importance due to the digital space's lack of spatial and temporal boundaries (Moreno, 2020).

Today, the technological capabilities of forming a fully controlled digital space have increased significantly. The behavior of citizens in the digital space, their user reactions to publications, information preferences become an integral part of digital data arrays that can be used effectively to exercise total control over any person.

Personal devices of users (computer, tablet, smartphone) begin performing not an instrumental function of obtaining information by the user but become a source of data for the formation of digital profiles, while, in most cases, without requiring any consent from the user for this. Personal "smart" devices are becoming tools for tracking, monitoring, and generating information about the user, his activities, and preferences. On his own initiative, a citizen acquires and uses devices that can later perform the function of control over him.

As B. Barber wrote, "There is no tyranny more dangerous than an invisible and benign tyranny, one in which subjects are complicit in their victimization, and in which enslavement is a product of circumstance rather than intention. Technology need not inevitably corrupt democracy, but its potential for benign dominion cannot be ignored" (Barber, 1998: 582).

In fact, the private information sphere no longer belongs only to the citizen. Today, a person is immersed by technology corporations in such nonalternative conditions that he cannot refuse to disclose his personal data. In practice, digital corporations use pretty inflexible techniques, reducing a person's choice to transfer his personal data to the corporation or to a complete refusal of a particular service (McQuire, 2018: 39, 131). Digital corporations, having acquired their socio-political subjectness and tending to monopoly, can pose a threat from the perspective of building a digital Panopticon — all-pervading control over human life through digital technologies (Diamond, 2019).

Simultaneously, artificial intelligence technologies and neural network algorithms are increasingly being used to analyze digital user traces. This circumstance further increases the efficiency, operativeness, and completeness of automatic control over people. In fact, today, we are witnessing the formation of hidden modes of "smart" digital Panopticon in technologically developed states.

In other words, we are talking about the formation and further use of such arrays of digital information, which, with an appropriate technological application, can provide an impact on almost any aspect of citizens' lives.

At the same time, a possible evolution of disciplinary power from the panopticon regime towards the panspectron regime — voluntary social observation of users one after another, seems to us a hazardous challenge for digital privacy rights (Dudina, 2018). We see the threat to human rights in this aspect on several levels at once. First, such self-observation is encouraged and stimulated by the very logic of digital monopoly platforms aimed at increasing traffic and profits. Second, this panspectron mode is flexibly combined with the regular intrusion of subjects controlling digital communications into a person's private sphere.

The main actors are global technology corporations, government agencies, and special services within this practice. Depending on the design of relations between these actors (antagonistic, cooperative, competitive), various scenarios for forming digital control regimes may arise. Notably, in the appendix to the recommendation of the Committee of Ministers of the Council of Europe, it is clearly stated (paragraph 1.1.3) that not corporations, but "states bear the main responsibility for protecting human rights and fundamental freedoms in the digital environment…".[15]

However, as current practice shows, in many countries of the world, there is a gradual merging of state institutions of power, technological corporations, and special services, as a result of which the effect of hybridization arises, and it becomes more and more likely to implement a "hybrid" scenario of merging state institutions and tech giants into a single system of state-political management. This scenario seems to be one of the most probable to realize the interests of government institutions and large techno-corporations (but not society).

[15] Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries. Available at: *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14* (accessed on: december 20, 2021).

Several factors determine the potential of state-corporate symbiosis at once:

— Traditional political regimes already have the legality and legitimacy necessary for managing society, which makes it possible to "technologize" the existing state management systems in a soft regime without transition periods and socio-political upheavals inherent in states in which the regime change is taking place.
— Due to the technological potential of corporations in the general management system, state institutions of power are also able to significantly increase their own managerial potential, which, ultimately, is a necessary condition for ensuring effective management of complex social systems.
— Global technological infrastructure owned by large corporations can be quickly integrated into a new type of digital public-political management system, together with all multi-billion audiences of global digital platforms. Moreover, the existing Big Data arrays in combination with contemporary artificial intelligence technologies and self-learning neural network algorithms make it possible to successfully form, in addition to national ones, also supranational systems of "smart" management and control in the socio-political sphere.

Obviously, the legal regulation of the collection, use, and distribution of Big Data is becoming the most crucial factor determining whether a citizen's right to privacy will be preserved in a digital society. However, as the analysis of contemporary lawmaking practice demonstrates, it has a predominantly reactive nature and is often subject to the influence of tech giants on representatives of the legislative branches of government of national states. It is no coincidence that a representative of the Harvard University Sh. Zuboff singles out the model of surveillance capitalism as one of the most relevant models of contemporary development, based on the state-corporate regime of joint digital control and monetization of citizens' digital activity. As the researcher notes, surveillance capitalism is a mutant form of our economic system that sifts through the human experience found in our search data in order to get marketable predictions of what we will do/read/buy/believe next. Most people understand the term "surveillance" but do not notice the word following it. The social media business

model is not really a mutant version of capitalism: it is just capitalism that is doing it - finding and exploiting resources from which to profit.

> Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to service improvement, the rest is declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as "machine intelligence", and fabricated into prediction products that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call behavioral futures markets. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behavior (Zuboff, 2019).

And now "surveillance capitalism moves from a focus on individual users to a focus on populations, like cities, and eventually on society as a whole" (Naughton, 2019).

In this regard, we are forced to state that the right to privacy in the digital space today is largely conditional and requires more severe protection from democratic institutions of power that seek not to control their own population and make a profit but to effective and democratic social development.

V. The right to communicate, freedom of speech, and access to information in the context of digitalization

On the one hand, it should be borne in mind that human thinking itself still has an analog nature, and digital transformations can affect it but not change it. It is also impossible to ignore significant groups of the population, which still do not have the competence of their practical use. Such groups do not have the opportunity to exercise their digital rights due to the presence of a competence gap with other, technologically more advanced population groups.[16]

Digital literacy is important for children too. For example, the Council of Europe's Committee of Ministers' recommendations (para. 96) advise

[16] These are not necessarily people living in regions where digital infrastructure is poorly developed.

states to encourage companies to develop and implement child-friendly standards, codes of conduct, and industry policies.[17]

On the other hand, current trends demonstrate that digitalization is pervasive and aimed at a mass audience. Forced digitalization amid the COVID-19 pandemic is no exception. In the near future, in our opinion, the main emphasis will be placed on the development of systems of digital control over citizens, the transfer of traditional spheres (education, medicine, services, etc.) to digital formats of mass consumption, the formation of digital arenas that replace traditional spaces of public interaction.

As a result, we expect that traditional offline relationships between people will increasingly become the prerogative of a selected audience (representatives of the political and economic elite) and a kind of luxury. The situation today is developing in such a way that if earlier digital communications were an opportunity for the elite (the presence of a mobile phone in the mid-1990s, the ability to use e-mail, the presence of smart gadgets and computers, video communication, etc.), today the avoidance of digital communications, which have become cheap, massive and in many respects inevitable, is a status symbol, a marker of the chosenness of a person who has the ability to communicate in traditional formats. Traditional live human contact is gradually becoming an elite luxury item. How comfortable it is for someone to interact with people in traditional analog reality can become a new marker of social class. It seems to us that this trend will primarily become long-term, and digitalization in the context of a pandemic has only strengthened it.

Forced pandemic digitalization, in our opinion, has led to the fact that in a contemporary culture of growing isolation, the social fabric of society is rapidly deteriorating. People acquire competencies for digital consumption, digital communication technologies develop, resulting in socialization processes increasingly shifting into the digital space. However, in this space, there are only impersonal avatars and accounts, through which it is no longer direct but mediated communication between people, which is an influential factor in the transformation of a traditional society into a digital society of a new type.

[17] Recommendation of the Committee of Ministers to Member States on Guidelines to Respect, Protect and fulfil the Rights of the Child in the Digital Environment-CM/Rec(2018)7. Available at: *https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a* (accessed on: december 20, 2021).

The intermediate stage of the transition from a traditional to a digital society is highly likely to have a hybrid character, within which offline and online tools of social interaction will be combined. At the same time, the latter will steadily displace the former.

However, the digitalization of public communications creates another extremely significant challenge associated with the vast possibilities for technological limitation of the right to communicate of an unwanted citizen.

The possibilities of digital isolation and deprivation of any individual in the conditions of his total immersion in the digital socio-technical reality on the part of the actors controlling the digital communication channels can become quite serious. The forced digitalization of public communications has led us today to the fact that, being deprived of their accounts in social media and digital accounts on state service portals and in financial organizations, an individual is isolated from society, unable to receive financial, legal, social services. A person disappears from the digital and, most importantly, social space, being almost wholly deprived and limited in the right to communicate and receive information. In fact, we can say "no digital profile-no person". This thesis is especially relevant in the context of the privatization of citizens' digital social contacts by technological corporations.

Obviously, in such conditions, the possibilities of control and application of sanctions against any citizen become incomparably higher compared to traditional approaches to implementing restrictions. The person himself becomes maximally dependent on the will of those who own digital platforms and control communication channels. The formation of digital modes of society management only multiplies the possibilities for the large-scale exclusion of individuals and groups of citizens from the digital space of social and political life. We can predict with a high degree of probability in the near future the active formation and application of digital restrictions practices, the basis of which, paradoxically, is the high involvement of individuals in digital interactions in various spheres of their life. Moreover, hardware and software systems can automatically implement such restrictions based on artificial intelligence technologies and neural network algorithms.

It is no coincidence that today scientists are actively talking about rethinking the concept of disciplinary power by M. Foucault and discussing the emerging phenomenon of algocracy-algorithmized power. The most crucial feature of algorithmic power is not the "principle of the visibility

threat" but the "principle of the invisibility threat" (Bucher, 2012), when the digital platform (additionally, the political actor associated with it, the political regime) decides at its own discretion who will retain digital rights and who will not.

Recommendations in this area are offered not only by international organizations or governments but also by representatives of the academic community. For example, Kartik Hosanagar, a technology professor at the University of Pennsylvania, proposed an Algorithmic Bill of Rights that would protect humans from AI risks.

Based on his idea, Vox Future Perfect conducted a survey[18] of 10 experts dealing with AI problems and found out that such an Algorithmic Bill of Rights should include the principles of transparency, explanations (how algorithms affect humans), consent/disagreement to use AI systems, freedom from bias, feedback mechanism, data portability to another vendor, compensation for damages, algorithmic literacy, independent oversight, the right to reliable federal and global governance structures).

In the current works of scientists, we can find many examples of discourse control and violation of the digital right to access information and communication by some undemocratic political regimes. Various examples of the work of firewalls, phishing of usernames on social networks, complex configuration of the Internet gateway infrastructure, keyword bans, the functioning of special programs, systems that redirect users from politically unreliable sites to other resources are given (Keane, 2015: 259).

At the same time, contemporary cases of violation of digital rights indicate that the sources of the most severe risks are in many cases not political regimes but digital corporations. In January 2021, several social networks (Instagram, Facebook, YouTube, Twitter) blocked the accounts of the still current American President Donald Trump after his supporters briefly seized the Capitol. Moreover, the pressure was exerted on the Trump-backed right-wing network Parler. Amazon suspended web hosting, Apple and Google banned the Parler app. Similar actions followed from platforms such as Reddit, TikTok, Pinterest, Twitch, and Shopify. Although political misinformation about the American elections fell sharply after such drastic censorship measures (Floridi, 2021), a discus-

[18] "10 Things we should all Demand from Big Tech Right Now". Available at: *https://www.vox.com/the-highlight/2019/5/22/18273284/ai-algorithmic-bill-of-rights-accountability-transparency-consent-bias* (accessed on: december 20, 2021).

sion immediately erupted in society about whether digital corporations, already gaining their own sovereignty, have the right to deprive a person of the right to communicate. After all, private digital corporations, playing an important social and communication role, have shown who actually controls digital rights in practice.

Typically, the response to such digital constraints is the digital migration of users to other platforms and resources. The formation of entirely new digital resources, independent of digital monopolists, can also occur. When the Trump communities r/Incels and r/The_Donald faced sanctions on Reddit, they created new standalone sites incels.co and thedonald.win, urging users to switch to them. The special study showed ambiguous results (Ribeiro *et al*., 2020): if there were no special changes in the first new community, then digital migration in the second new community led to an increase in-group identification, which was recorded on the example of an increase in the "toxicity" of discourse. In any case, such digital migration was an attempt by the community to save its independence from digital monopolies in the face of the state institutions' indifference.

As a result, in our opinion, the protection of a citizen's right (already digital right) to the freedom of communication and expression, along with the protection of the right to access information, acquires a special meaning and special relevance in current conditions of digitalization. Indeed, it is not easy to talk about global ius communications (right to communicate) without digital communication. A person who does not have access to the Internet today cannot participate in social and political life, which means he cannot be an active citizen (Thumfart, 2017: 200).

VI. Hybrid subjectness and human right to communicate with their own kind

Additionally to the classical personal rights to privacy, freedom of speech, and access to information, it seems important to us to analyze the prospects for developing artificial intelligence technologies and self-learning neural networks in terms of forming new digital human rights.

So, in our opinion, one of the central rights, the maintenance of which will become a challenge to social development in the conditions of the formation of a new digital socio-technical reality, be the right to communicate with one's own kind.

This thesis is substantiated by the fact that contemporary society can pass the point of no return in the conditions of global technological turbulence associated with the multidirectional but at the same time extremely intensive introduction of smart technologies into the current socio-political practice. We mean a critical increase in the importance of artificial intelligence technologies and neural network algorithms in the processes of information and communication interaction occurring in key areas of the life of the state and society (Volodenkov, 2020). Today, it is difficult to imagine the communication of a contemporary person without the use of smartphones. In the same way, humanity may face a high dependence of its existence and social interaction on "smart" digital technologies in the foreseeable future.

Here, we are faced with the question — in whose interests and on what value foundation important decisions will be made, on which the fate of hundreds of millions of people depends.

Additionally, a separate issue is the problem of the decisions' subjectness made by artificial intelligence and neural network algorithms. Who, ultimately, is the subject of decision-making? The developer, the user, the smart system itself?

To date, the answer to this question is not obvious. For example, neural networks have learned to create music, paintings, literary works. So, in 2017, the musical project "Neurona" was presented — an album created by a neural network based on the analysis of musical compositions by Kurt Cobain. In 2018, using a neural network, a piece of music, "Digital Sunrise", was written, later performed by the orchestra under the direction of Y. Bashmet. In 2017, the painting "Portrait of Edmond de Belamy", created by a neural network algorithm, was sold at Christie's auction. In 2021, the ruGPT-3 neural network, trained by Russian Sberbank AI specialists, independently wrote a C ++ and Java computer program. It is the first software, registered in Russia, written by artificial intelligence. In turn, in Australia, the artificial intelligence system Dabus (A Device for the Autonomous Bootstrapping of Unified Sentience) was registered as an inventor under Australian patent law in 2021. Australian Federal Judge Jonathan Beach ruled that "an artificial intelligence system or device can be recognized as an inventor by law. This is in line with the realities of contemporary technology, as well as the law, and promotes innovation" (Taylor, 2021). The Dabus also received its first patent in South Africa this July. As Professor Adrian Hilton, Director of the Institute for People-Centred AI at the University of Surrey, noted the

following: "This is a truly historic case that recognizes the need to change how we attribute invention. We are moving from an age in which invention was the preserve of people to an era where machines are capable of realizing the inventive step, unleashing the potential of AI-generated inventions for the benefit of society" ("DABUS Gets Its…", 2021).[19]

The problem we have identified requires a specific solution. To begin with, it is important to identify which actors are most intense in attempts to develop legal norms related to AI. It should be emphasized that international organizations carry out important work in this area. It is confirmed by the base of normative documents collected by the Secretariat of the Council of Europe.

The possibilities for visualizing this base show that the most active actors in the initiatives to create normative documents in the field of AI are precisely international organizations (Council of Europe, European Union, UNESCO, and OECD).[20] In this regard, they are ahead of governments and private sector initiatives. For example, in 2018 at the UN General Assembly, the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye highlighted not only the positive aspects of AI but also commented on the risks of such systems.[21]

The rapporteur made specific recommendations to the states. Since the volume of the article does not allow commenting on the entire report, we will highlight the theses that, in our opinion, deserve the most significant interest in terms of recommendations:

— When purchasing and deploying AI systems, states are encouraged to act based on human rights principles, to conduct public consultations.
— Regulate the field of data protection, require enterprises to operate effective mechanisms of external accountability.

[19] However, it should be noted that at the same time, in some countries, opposite court decisions were adopted, in which artificial intelligence systems were not recognized as patent owners.

[20] AI initiatives available at: *https://www.coe.int/en/web/artificial-intelligence/national-initiatives* (accessed on: december 20, 2021).

[21] Report on Artificial Intelligence Technologies and Implications for Freedom of Expression and the Information Environment. Available at: *https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx* (accessed on: december 20, 2021).

— Practice industry regulation of AI applications, where necessary, regulation should be developed with the involvement of representatives of civil society.
— Create political and legislative conditions conducive to forming a pluralistic information environment and ensure competitiveness in the AI segment.

In a separate set of AI-focused company recommendations, speaker David Kaye urged them to:

— Reflect ethical principles in technical guidelines and corporate policies.
— Clearly indicate how and where AI technologies are practiced in services, platforms, and applications, publish data on the facts of content deletion.
— Prevent discrimination based on AI, monitor discriminatory practices.
— Conduct public consultations during the development and deployment of new AI systems, interact with human rights defenders, representatives of civil society, and publish the results of such assessments.
— Provide an independent audit of AI systems.
— Implement systems for responding to user complaints about the violation of their rights by AI systems.

Most of the recommendations are explicitly intended for companies, not states. It is not surprising since contemporary corporations engaged in IT technologies and the implementation of AI developments, in particular, are becoming an important condition for citizens' communication.

As we can see, artificial intelligence systems and neural network algorithms are gradually beginning to claim the legal right to be a subject in various fields.

In this regard, the introduction of neural network technologies and programs based on artificial intelligence into the field of public communications is of particular interest. Artificial algorithms are becoming more realistic, replacing real people in information and communication interaction processes with a higher degree of success. Based on Big Data arrays available for analysis, which make it possible to thoroughly study

the individual personality traits of the communication partner, possessing a high level of realism, communicating with people independently in an autonomous mode, artificial personalities begin to more and more claim, if not for subjectness, then for pseudo-personality in social interactions with humans.

In fact, it will be very problematic for a simple user to distinguish a real person from an artificial personality in the near future. For an ordinary person, an artificial personality based on artificial intelligence or a neural network algorithm will seem quite natural, which forms a high manipulative and propagandistic potential of information and communication impact on the part of "smart" software and hardware systems.

As Sean Gourley rightly noted,

> …artificial intelligence and learning algorithms will make it almost impossible to tell robots from humans — and actual news from fake. We will see the emergence of more automated computational propaganda — bots using sophisticated artificial intelligence frameworks, removing the need to have humans operate the profiles. Algorithms will not only read the news but write it. These stories will be nearly indistinguishable from those written by humans. They will be algorithmically tailored to each individual and employed to change their political beliefs or to manipulate their actions (Gourley, 2015).

Here the following question arises: if the processes of information and communication interaction of real people occur in the formats of persuasion and exchange of opinions (which is guaranteed by the corresponding law), then in what formats will the interaction between a living person and an artificial person take place? How can we eliminate the manipulative component of the communicative act of a "smart" artificial personality who knows everything about a partner based on the analysis of his digital traces? In whose interests will the communication of a machine with a person be carried out?

In this situation, the emergence of the Artificial Intelligence Act proposed by the European Commission is quite natural. This document takes a "risk-based approach", classifying AI technologies by risk and introducing a legal mechanism to regulate these risks. A good solution is to divide all AI systems into four categories: low and minimal risk, limited risk, high risk, and unacceptable risk. The systems with the highest risk, according to this document, must obey additional rules. Before their direct

implementation, it will be necessary to register them in the EU database. The document focuses on assessing AI systems used for the biometric identification of people.[22] This European document might well become an example for adopting similar acts in other states.

An equally important aspect of this problem is the possibility of a person choosing an actual communication partner. If in ordinary life a citizen has a choice — to contact the authority in person or through the appropriate digital portal, to talk to a live bank operator, or to use the help of an artificial assistant, then what choice will be given to a person in conditions of the simulation of real personalities by artificial intelligence? If a person does not even realize that a communication partner is an artificial person, what choice can we talk about? Also, the right to communicate with an actual partner becomes problematic in its conscious realization possibilities.

We can assume that in the context of the intensive introduction of cyber simulators of real people into public communications, which only simulate actual citizens with the help of digital accounts, society will face the problem of hybrid subjectness. It can be described as the simultaneous existence in the communication space of real people and artificial personalities operating based on artificial intelligence technologies and neural network algorithms. Simultaneously, communication will be performed in mixed formats: "real person-real person", "real person-artificial person", and even "artificial person-artificial person".

This topic is of particular relevance in the context of the initiatives of large technology corporations to create the Metaverse, which will be a collection of common three-dimensional spaces and digitally improved physical spaces that are extensions of the Internet.

In such conditions of hybrid communicative subjectness, the exercise of the right to communicate with their own kind will be challenging, and the active participation of artificial personalities in publication, commentary, and dialogue activities will only exacerbate the situation in the digital space. Suppose a situation in which, due to certain circumstances, only communication with artificial persons is available to a citizen (or he does not even know that other people are absent in his communication act). Will the possibility of communication with an artificial person mean that the

[22] Artificial Intelligence Act. Available at: *https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf* (accessed on: december 20, 2021).

citizen is still retained his right to freedom of communication and the right to express his opinion?

At the same time, what will be the legal responsibility of an artificial personality for bullying, trolling, publication of offensive posts, as well as materials of a radical and extremist nature? This question is not exclusively hypothetical since an analysis of current practice has been demonstrating examples of how bots with elements of emotional intelligence broadcast questionable and ambiguous content in the digital space.

For example, the artificial personality Tay, created by Microsoft, as a result of its self-training in the processes of communication with real users, began to publish on Twitter extremist statements in support of Hitler and advocate the need to build a wall on the border between the United States and Mexico.

Obviously, with a critical mass of artificial personalities functioning in the digital space and carrying out information and communication interaction with real users, the potential of a manipulative and propagandistic influence on mass consciousness can be extremely high. It is fraught with severe socio-political consequences in the aspect of forming radical mass ideas and radical models of mass behavior. It is no coincidence that E. Morozov writes about this, suggesting that the development of Internet communications can lead to forming a "spinet" — a national Internet zone, where manipulations are practiced instead of the classic model of strict government censorship (Morozov, 2014: 160-161). At the same time, behind such manipulations may also be a transnational digital corporation or another political regime interested in weakening its economic or geopolitical adversary, not only the local political regime.

Clearly, such a scenario of the development of events can negatively impact both the value foundations of social development and the socio-political destabilization of state systems as a whole. After all, society can lose its leading role in forming values, meanings, goals it strives to achieve, and informationally active artificial personalities will come to replace real citizens in the digital space. Then we have high chances of encountering a situation in which neural networks and artificial intelligence will determine the moral and ethical principles of people's life, socially approved models of behavior, the value of personal rights and freedoms that seem to be unshakable today.

In this regard, we have identified hybrid subjectness in the digital communication space as one of the most significant threats to social de-

velopment and the preservation of human rights in the new socio-technical reality.

VII. Final remarks

A preliminary analysis[23] of the activities of international organizations in the field of AI legal regulation allows us to put forward a number of recommendations designed to mitigate risks in this area:

- It is important to create public situational centers-regular institutional platforms that promote an inclusive approach to discussing the discrimination problems caused by the activities of AI systems. Perhaps these regular platforms, where there would be representatives of the scientific community, public, youth organizations, should regularly work based on the UN system.
- These public situational centers, which have official status in all states, should receive the right to draw up a request to public authorities and corporations for the fact of discrimination by AI systems.
- Public authorities and companies involved in the development and use of AI are obliged to take into account the recommendations of these community centers and also allow regular consultations with them.
- The work of public situational centers must respect national legislation, take into account the peculiarities of local culture and public life, use the principles of mediation, the peaceful resolution of legal inconsistencies in case of possible contradictions between the national and international legal order.
- All activities of public situational centers should be aimed at the formation of a common and consistent legal order, the result of which should be the minimization of risks from discrimination from end-to-end digital technologies, AI, the Internet of things, concepts of a smart city, smart home.

[23] In our opinion, the topic of the activities of international organizations in the legal regulation of aspects of AI requires a separate scientific study, which is beyond the scope of this article.

— Cooperation of international organizations, states, digital corporations should be based on a "risk-based approach".
— All technologies related to digital communication, AI should be assessed for the potential for the preservation of human rights and freedoms, the development of democracy, cultural and ethnic diversity.
— States, corporations, international, and public organizations are required to work towards the adoption by all countries of the "Algorithmic Bill of Rights", which would become the main normative act regulating aspects of non-discriminatory human interaction with AI and other digital technologies and systems. Such a bill should include a clause stating that members of the public and the academic community should have systems that allow them to track the facts of the impact of algorithms on the socio-political sphere, identify the source of the algorithm and identify the subject responsible for the resulting discrimination or violation of rights.
— Any digital technologies, AI systems that are able to participate in automatic decision-making and thereby affect a person's life in one way or another, should leave the right of the main decision to the person, and not the AI system.
— Public situational centers, created on the basis of organizations like the UN, should regularly monitor the development and implementation of the latest digital technologies in order to prevent a fatal lag between the international and national legal frameworks from technological progress.

Summing up the work results, it should be noted that we have identified far from the entire range of potential risks, threats, and challenges associated with the global technological transformations and the digitalization of key spheres of life of the contemporary state and society.

Obviously, today, on their own any technology — only a tool that helps achieve the set goals. Digital technologies, including artificial intelligence technologies and algorithms for self-learning neural networks, also have a constructive potential for their application in the processes of social development, state and political governance, increasing the transparency of interaction between government institutions and civil society, and improving the quality of management decision-making in socially significant areas.

However, at the end of the last century, B. Barber pointed out that "if we measure power by the potential for monopoly and control over information and communication, it is evident that the new technology can become a dangerous facilitator of tyranny. Even in the absence of conscious government abuse, this potential can constrict our freedom, encroach on our privacy, and damage our political equality" (Barber, 1998: 581). That is why we focused our attention on the key risks, threats, and challenges of contemporary technological development.

We are confident that the scenario of the integration of "smart" technologies into the processes of social, political, and economic development is still determined exclusively by people, their interests, and goals.

However, what these interests and goals will be — the question remains open and highly urgent. What will be the choice between the desire for democratic social development and the desire to put contemporary society under digital control, between the desire to improve the people life quality with the help of new technologies and the desire to monetize the digital sphere, to maximize the profits derived from it — this will depend on many factors, the ability of society itself to take a responsible approach to the protection and implementation of personal rights.

Of course, this choice is a big challenge for state institutions of power, national political regimes, which will need to decide on one of the scenarios of national development — establishing regimes of total digital control over citizens, merging with technological corporations that have the necessary technologies or moving along a democratic path, ways to protect the rights of their own population in the digital age.

Today, it is not apparent to us which scenario will be chosen and implemented. However, in the context of global technological turbulence, it is significant for specialists in the field of law, social sciences, state and municipal administration to pay special attention to the processes of digitalization and the introduction of "smart" technologies, concentrating the focus of their research on the ways and possibilities of maintaining, preserving and protecting fundamental human rights. in the digital age.

VIII. References

Aneesh, A. (2006). *Virtual Migration: The Programming of Globalization.* Durham: Duke University Press.

BARBER, Benjamin (1998). "Three Scenarios for the Future of Technology and Strong Democracy". *Political Science Quarterly*. 113(4). Available at: *http://dx.doi.org/10.2307/2658245*.

BOWLES, Nellie (2019). "Human Contact Is Now a Luxury Good". *The New York Times*. Available at: *https://www.nytimes.com/2019/03/23/sunday-review/human-contact-luxury-screens.html* (accessed on: august 14, 2021).

BOYD-BARRETT, Oliver (2018). *Media Imperialism*. Kharkov: Humanitarian Center (In Russ.).

BUCHER, Taina (2012). "Want to Be on Top? Algorithmic Power and the Threat of Invisibility on Facebook". *New Media & Society*. 14(7). Available at: *http://dx.doi.org/10.1177/1461444812440159*.

BUSTAMANTE DONAS, Javier (2007). "Los nuevos derechos humanos: gobierno electrónico e informática comunitaria". *Enlace*. 4(2).

BYKOV, Ilya, Hall, Tad. (2011). "Digital Divide and the Internet-Users Political Preferences in Russia". *Polis. Political Studies*. 5 (In Russ.).

CASTELLS, Manuel (2011). "A Network Theory of Power". *International Journal of Communication*. 5.

"DABUS Gets Its First Patent in South Africa Under Formalities Examination" (2021). *IPWatchdog*. Available at: *https://www.ipwatchdog.com/2021/07/29/dabus-gets-first-patent-south-africa-formalities-examination/id=136116/* (accessed on: august 14, 2021).

DIAMOND, Larry (2019). "The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism". *Journal of Democracy*. 30(1). Available at: *http://dx.doi.org/10.1353/jod.2019.0001*.

DUDINA, Viktoriya (2018). "From Panopticon to Panspectron: Digital Data and Transformation of Surveillance Regimes". *Sotsiologicheskie Issledovaniya*. 11. Available at: *http://dx.doi.org/10.31857/S013216250002782-3* (In Russ.).

DUNNING, Thomas Joseph (2015). *Trades' Unions and Strikes: Their Philosophy and Intention*. Sagwan Press.

FLORIDI, Luciano (2021). "Trump, Parler, and Regulating the Infosphere as Our Commons". *Philosophy & Technology*. 34. Available at: *http://dx.doi.org/10.1007/s13347-021-00446-7*.

FLORIMOND, Guillaume (2016). *Droit et Internet. De la logique internationaliste à la logique réaliste*. Paris: Mare & Martin.

GALINDO NUÑEZ, Alma Celia (2019). "Derechos digitales: una aproximación a las prácticas discursivas en internet desde la etnografía virtual". *PAAKAT: Revista de Tecnología y Sociedad*. 9(16). Available at: *http://dx.doi.org/10.32870/Pk.a9n16.359*.

GOURLEY, Sean (2015). "Get Ready for the Robot Propaganda Machine". *WIRED.UK*. Available at: *http://www.wired.co.uk/article/robot-propaganda* (accessed on: august 14, 2021).

HUTCHINSON, Andrew (2015). "On What Facebook Knows-An Interview with the Man Behind Facebook's Personality Experiment". *Social Media Today*. Available at: *https://www.socialmediatoday.com/technology-data/adhutchinson/2015-10-01/what-facebook-knows-interview-man-behind-facebooks* (accessed on: august 14, 2021).

KEANE, John (2015). *Democracy and Media Decadence*. Moscow: HSE Publishing House (In Russ.).

KOSINSKI, Michal *et al*. (2013). "Private Traits and Attributes are Predictable from Digital Records of Human Behavior". *Proceedings of the National Academy of Sciences of the United States of America*. 110(15). Available at: *http://dx.doi.org/10.1073/pnas.1218772110*.

KOSINSKI, Michal (2021). "Facial Recognition Technology can Expose Political Orientation from Naturalistic Facial Images". *Scientific Reports*. 11(1). Available at: *http://dx.doi.org/10.1038/s41598-020-79310-1*.

LUCENA-CID, Isabel-Victoria (2014). "El derecho de acceso a Internet y el fortalecimiento de la democracia". *Revista Internacional de Pensamiento Político*, 9.

MANTELERO, Alessandro (2018). "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment". *Computer Law & Security Review*. 34(4). Available at: *http://dx.doi.org/10.1016/j.clsr.2018.05.017*.

MARTÍNEZ VELÁZQUEZ, Antonio, FLORES SOSA, José (2016). "En defensa del anonimato". *Internet en México: derechos humanos en el entorno digital*. México: Derechos Digitales.

MCQUIRE, Scott (2018). *Geomedia. Networked Cities and the Future of Public Space*. Moscow: Strelka Press (In Russ.).

MORENO BOBADILLA, Ángela (2020). "Forget Before Internet: The Origins of the Right to be Forgotten". *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*. 43. Available at: *http://dx.doi.org/10.22201/iij.24484881e.2020.43.15183*.

MOROZOV, Evgeniy (2014). *The Net Delusion. The Dark Side of Internet Freedom*. Moscow: AST, CORPUS (In Russ.).

NAUGHTON, John (2019). "The Goal is to Automate Us: Welcome to the Age of Surveillance Capitalism". *The Guardian*. Available at: *https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook* (accessed on: august 14, 2021).

POPOVA, Anna *et al*. (2021). "The System of Law and Artificial Intelligence in Modern Russia: Goals and Instruments of Digital Modernization". *Studies in Systems, Decision and Control*. Available at: *http://dx.doi.org/10.1007/978-3-030-56433-9_11*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (2016). *Official Journal of the European Union,* 119.

RIBEIRO, Manoel Horta *et al*. (2020). "Does Platform Migration Compromise Content Moderation? Evidence from r/The_Donald and r/Incels". *ArXiv*. Available at: *https://arxiv.org/abs/2010.10397* (accessed on: august 14, 2021).

SMORCHKOV, Andrey *et al*. (2020). "*Vox Populi-Vox Dei*: Elections in the Roman Republic and Modern Democracies (Comparative Analysis)". *The New Historical Bulletin*. 66.

SRNICEK, Nick (2020). *Platform Capitalism.* Moscow: HSE Publishing House (In Russ.).

TAYLOR, Josh (2021). "I'm Sorry Dave I'm Afraid I Invented that: Australian Court finds AI Systems can be Recognised under Patent Law". *The Guardian*. Available at: *https://www.theguardian.com/technology/2021/jul/30/im-sorry-dave-im-afraid-i-invented-that-australian-court-finds-ai-systems-can-be-recognised-under-patent-law* (accessed on: august 14, 2021).

THUMFART, Johannes (2017). "Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right, Just Cyber-Warfare". *At the Origins of Modernity. Studies in the History of Law and Justice*, 10. Available at: *http://dx.doi.org/10.1007/978-3-319-62998-8_11*.

UN. General Assembly (68th sess.: 2013-2014) (2014). The Right to Privacy in the Digital Age: United Nations Digital Library System. Available at: *https://digitallibrary.un.org/record/764407?ln=ru* (accessed on: august 14, 2021).

VINCENT, James (2021). "Twitter's Photo-Cropping Algorithm Prefers Young, Beautiful, and Light-Skinned Faces". *The Verge*. Available at: *https://www.theverge.com/2021/8/10/22617972/twitter-photo-cropping-algorithm-ai-bias-bug-bounty-results* (accessed on: august 14, 2021).

VOLODENKOV, Sergey (2020). "Digital Socio-Political Communication and its Transformation in the Technological Evolution of Artificial Intelligence and Neural Network Algorithms". Conference Proceedings: 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH). Available at: *http://dx.doi.org/10.1109/EMCTECH49634.2020.9261512*.

ZORKIN, Valery (2018). "Law in the Digital World". *RG.RU*. Available at: *https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html* (accessed on: august 14, 2021) (In Russ.).

ZUBOFF, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs. Available at: *http://dx.doi.org/10.1080/15228053.2020.1860404*.