Transformation of the right to privacy in the context of the development of digital technologies

Evgeniy Batyrovich Sultanov[1], Georgy Borisovich Romanovsky[2], Rifat Rasimovich Kil'deev[3]

[1]Kazan Federal University, Candidate of Law, Law Faculty of KFU, Author ID: 505639, ORCID 0000-0003-2997-6878, Sultanov2007@yandex.ru
[2]Penza State University Doctor of Law, Professor, Institute of Law of PSU, Author ID: 422344, ORCID 0000-0003-0546-2557, vlad93@sura.ru
[3]Penza State University, post-graduate student, Institute of Law of PSU, ORCID - 0000-0002-0408-6986, rifkildeev13.08@mail.ru

[*]Corresponding Author:

Abstract

The article examines the transformation of the right to privacy in the context of globalization of the Internet space and the rapid development of digital technologies. The emergence of a new concept of digital rights led to the search for an optimal model of individual autonomy, resulting in the right to data protection, most clearly articulated in the Charter of Fundamental Rights of the European Union. It is shown that the declaration of the right to data protection is associated with at least the following factors: 1) communication with the ability to control information about themselves; 2) the evolution of the right to inviolability of private life, the changing in the development of various technologies, pushing the boundaries of the law, or changing approaches to its protection; 3) the emergence of new values and informational self – determination (autonomy of information); 4) the circulation of information flows in accordance with the technological processing rules affecting the contents of the specific powers of each citizen in the digital space. The author also highlightsa the trend of Internet sovereignty driven by security requirements, as exemplified by the "Golden Shield" built in the People's Republic of China.

Keywords: the right to privacy, the right to data protection, cybersecurity, transformation, secrecy, digital rights.

1. INTRODUCTION

The right to privacy has a relatively recent historyю of origin. Traditionally, it is believed that its discoverers are S. D. Warren and L. D. Brandeis (Warren Samuel D., Brandeis Louis D. The Right to Privacy) (1890). Since then, the right has been enshrined in most constitutions of countries around the world, developed in judicial and law enforcement practice. Based on the American experience, it is impossible not to mention the landmarke decisions of the US Supreme Court, which formalized the content of law and its modern understanding. Among the first – dated June 7, 1965 in the case "Griswold against Connecticut, in which, thanks to W. O. Douglas, the Judgee, the main author of the judgment, the right to privacy was derived from IV Amendments to the US Constitution as an integral part of the right to personal integrity. Then a specific argument was used about the creation of "penumbra" to form a new law, emanations (McKay Robert B. The Right of Privacy: Emanations and Intimations) to protect privacy zones.

In Russian constitutional practice, the right to inviolability of private life is enshrined in article 23. Thus, was the break with the Soviet tradition, which included the right to protection of private life, where the concept of "identity" and its sign is "private" – had a narrow understanding, not including the autonomy of significant social groups (minors, incapacitated persons prosecuted, etc. (Malein, 1981)). But even in the modern doctrine, various approaches have been formed. Thus, M. N. Maleina focuses on autonomy and personality (Maleina, 2001). O. E. Kutafin defined an independent institution of inviolability in constitutional and public law, which included the inviolability of private life (Kutafin, 2004).

At the same time, both the Russian and foreign understanding of this right was formed outside the expansion of digital technologies. Now we can observe the transformation of human rights, and hence the right to privacy, under the influence of the Internet, the development of social networks as a new means of communication, and

the transfer of many aspects of public activities to the virtual space. Given the fact that almost every citizen is interested in disclosing their own secrets (at least to gain access to services provided by public authorities), and the state is increasingly trying to put the individual under total control (often under the guise of public safety requirements), it is necessary to identify new trends in understanding the right to privacy.

2. METHODS

The study used the methods of comparative law, description, interpretation, theoretical and formal logic, as well as private scientific methods: legal-dogmatic and the method of interpretation of legal norms.

3. RESULTS AND DISCUSSION

3.1. Privacy in the digital rights system

The development of digital technologies and the change in the principles of building communications have led to difficulties in defining the boundaries of private life. The need to disclose many aspects of it when receiving the necessary services, exercising rights and freedoms, as well as the desire of citizens themselves to push these boundaries due to the openness of many aspects of their intimate sphere, led to the emergence of a significant amount of personal data, the processing of which is possible in automatic mode, minimizing the impact on its results from a particular person or organization.

Modern data processing speeds, as well as their qualitative transformation into a new category – big data, the globality of social networks and the transfer of communications to the virtual world - lead to blurring the lines between the natural barrier that everyone builds to protect their privacy from arbitrary interference. In these circumstances, traditional forms and methods of protecting a person's private life do not give the necessary effect, do not provide a reliable level of human rights guarantees.

All this has given rise to a new concept of digital rights, which has a different understanding, and therefore reflects different aspects. First, digital rights are understood as a set of powers that determine the freedom of access to the Internet space, various social networks, and other forms of communication based on virtual communication. In this part, it is customary to highlight the freedom of dissemination of information, freedom of speech, freedom of search, etc. The right to privacy acts as a certain barrier that does not allow unlimited expansion of the limits of freedom.

The second approach represents a negative element-requirements for the digital space, within which privacy is the principle of its construction. The main focus is shifted to the human rights sphere of individual autonomy and the inadmissibility of harming the individual through new forms of communication. Indeed, the stated aspect is becoming increasingly relevant. A citizen, sending a significant amount of personal data to the external environment, feels his own defenselessness. It is enough to refer to the statistics of fraudulent activities and cybercrime to make sure of this. In addition, many States are concerned about the spread of violence on the Internet, when personal data is a means of activating aggression. The phenomenon of cyberbullying has become widespread (in addition, its targets are increasingly minors whose psyche is less protected from manifestations of unmotivated violence).

With both approaches, ideas are expressed about the formation of a new generation-digital human rights, which include the rightato access the Internet and social networks, the right to electronic communication, the right to be forgotten, the right to comment, etc. Attempts are being made to initiate changes to basic laws (including national Constitutions). For example, article 5A, paragraph 2, of the Greek Constitution provides not only for the right of everyone to participate in the information society, but also for the obligation of the State to facilitate access to, and the production, exchange and dissemination of, information transmitted electronically.

The existence of new constitutional rights that are put forward not only in Russian legal science, related to the era of "digital civilization", raises a number of relevant substantive problems, including:

- regulatory consolidation of "digital rights", both at the constitutional and other sectoral levels;
- identification of the content and structure of new rights, as well as the content and structure of basic human rights that were formed earlier, but are undergoing global changes under the influence of digital technologies;
- analysis of technological conditionality (often direct dependence) of legal categories;

- the genesis of face identification (the appearance of "nicknames", IP addresses, logins, avatars, identifiers, as well as the replacement of familiar documents with digital counterparts, in particular, the replacement of passports with smart cards);
- determination of the jurisdiction of information intermediaries (and hence their responsibility), which is enhanced by the growth of cloud technologies (when territorial location is difficult due to the break in the technological chain – "user-provider (which itself can be divided within the chain) - subjects of the cloud structure";
- the impact of the volume, speed, accessibility, simplicity and global nature of information circulation on the qualitative characteristics of "digital rights";
- the gap between the network architecture (defined in most cases by the giants of the technology industry) and legal regulation, which tends to form digital sovereignty.

3.2. Complete freedom or sovereignty of the Internet: differences in legal regulation

In the modern world, we can observe the existence of two mutually exclusive trends-the defense of complete freedom of the Internet space and its sovereignty, based on fragmentation with the help of strict national rules. A striking example of Internet sovereignty is the policy of the People's Republic of China, designated by it as the "Golden Shield". Foreign sources use a different ironic name – "Great Firewall of China" (Zhang Lena, 2006), where the literal translation of "Firewall" – "fire wall" – has a different meaning: traffic filtering based on established requirements (Taneja & Xiao Wu, 2014).

Cyberspace sovereignty is understood as "a naturale extension and expressione of a country's national sovereignty in cyberspace" (https://baike.baidu.com). In Chinese literature, there is a reference to thea statement of Xi Jinping, General Secretary of the Central Committee of the Communist Party of China, on extending the international principle of sovereign equality, enshrined in the UN Charter, to cyberspace. The content of this element of the principle will be the rights of the State to choose the path of the Internet, the governance model, public policy on the Internet and equal participation in the governance of international cyberspace.

Starting from the principle of sovereignty of cyberspace, the legal framework of the Golden Shield consists of a whole set of regulations that impose requirements not only on telecom operators, but also on поставщикомsoftware suppliers, manufacturers of mobile phones and computers. This образомcovers the entire technological chain-from the production and pre-installation of programs and applications to access to the World Wide Web. In addition, China has a cyber space monitoring system that tracks the appearance of illegal content (Yanga & Liub, 2014).

A special feature of cyberspace regulationa In China, there is a bias towards by-laws, the right to issue which are vested in various departments: Ministry of Public Security, National Bureau of State Secrets, Ministry of Defense (Quinn, 2017). In addition, an interdepartmental body has been created – the Central Leading Group on Cybersecurity and Informatization-aimed at overcoming contradictions that arise in the adopted bylaws (Quinn, 2017).

The sovereignty of the Internet in the scientific literature is called the process of its fragmentation, which results in "cyberpaternalism" (Bellaby, 2018). Accordingly, the state border regime hasenot only a territorial extension, but also a digital turnover framework, and therefore ports for managing the flow of data from the country's storage facilities, which is ensured by strict localization of data. In part, this was a response to the expansion of tech giants, who initially promoted the idea of an open space, where jurisdiction is defined by the place of domain management. Currently, most countries define the Internet as a sphere of cooperation between all participants in relations (the state, users, telecom operators, providers, content owners, etc.), where the main goal is to create a comfortable cybersecurity zone.

Strengthening State regulation in the Internet - the German Law on Improving Social Media Enforcement aims to do the same (Netzwerkdurchsetzungsgesetz, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerke (https://www.gesetze-im-internet.de), abbreviated NetzDG). It should be pointed out in particular that the Act still does not have the same level of support in German society (Adamski, 2018; Feldmann, 2017; Hagen et al., 2017).

The Federal Act dated July 1, 2021 236-FZ "On the activities of foreign persons in the information and telecommunication network "Internet" on the territory of the Russian Federation" was adopted in the Russian Federation. Its purpose (as detailed in the Explanatory Note to the draft Law) is to create a legal basis for

"establishing the official presence of foreign companies engaged in information technology activities that affect the interests of Russian citizens".
From the documents accompanying the procedure for submitting the draft to the State Duma of Russia, it is clear that the Law is aimed at regulating the activities of such key companies as Google, Facebook, and Twitter.

3.3. The concept of the right to data protection

The changes in the digital environment have made the right to data protection, a new autonomous category of the right to privacy, which was initiated by the Charter of Fundamental Rights of the European Union (article 8).

The structure of Article 8 of the Charter is indicative. Part 1 provides for the general right of everyone "to the protection of personal data relating to them". Part 2 establishes guarantees of compliance with the law:
– data processing should be performed without manipulation.
- processing is allowed only for certain purposes.
- availability of the consent of the interested person, or the presence of other legitimate grounds provided for by law;
- everyone has the right to access the data collected in relation to them;
- the right to correct errors in the data.

Part 3 of Article 8 of the Charter stipulates the need to create an independent body authorized to monitor compliance with the established guarantees. This obligation is fulfilled by many European countries, where the institution of an ombudsman in the digital space has been established. For example, Poland has introduced the position of Inspector General for Personal Data Protection, whose activities are positively evaluated by various researchers (Błotny, 2017). In Switzerland, a Federal Data Protection and Transparency Officer position has been created in the government system (https://www.edoeb.admin.ch). In the Netherlands, there is a Data Protection Authority (https://www.autoriteitpersoonsgegevens.nl), which provides opinions on draft regulations affecting citizens' information rights, prepares annual reports on complaints from citizens about violations of their privacy (https://www.autoriteitpersoonsgegevens.nl), as well as annual reports on leaks of information about citizens (Meldplicht datalekken: facts & figures. Overzicht feiten en cijfers 2020).

In the foreign scientific literature, this approach is recognized as progressive and provides maximum protection against possible abuse when working with personal data (Lynskey, 2014). In addition, it is specifically emphasizedëthat the right to data protection has acquired a cross-sectoral character and has acquired links with other rights: the right to freedom of expression, the right to security (Politou et al., 2018), the right to international exchange (Politou et al., 2018). Indeed, there has been a concentration of many aspects in the issue of data protection that have recently gained maximum relevance. Let's list just a few of them:

- globalization of the information space;
- special importance of cybersecurity and;
- monetization of information resources.

4. SUMMARY

Technical features of the transmission and processing of electronic files often break the link with their owner and data subject, which reduces the possibility of using only the right to privacy in matters of effective protection. That is why the need for the emergence of a new human right – the right to data protection, which needs its constitutional consolidation and industry-specific specification-is actively being introduced in the domestic and foreign legal literature.

5. CONCLUSIONS

The emergence of the right to data protection is associated with at least the following factors:
– its connection with the ability to control information about oneself (with the definition of corresponding obligations to other subjects of law);
- the evolution of the right to privacy, which is changing in the context of the development of various technologies that push the boundaries of the right itself, or change approaches to its protection;
- the emergence of a new value – information self-determination (information autonomy), due to the turnover of a significant number of data subject to automated processing;
- circulation of information flows in accordance with technological processing rules that affect the content of specific rights of each citizen in the digital space.

The right to data protection is not absolute, but it must be correlated with related fundamental rights, including the right to privacy, the right to freedom of speech, the right to receive information, and the right to security. The right to data protection has acquired a cross-sectoral character, with a special focus on international exchange (cross-border information exchange). The openness of information about state citizens affects the concept of state sovereignty, which causes opposition in some countries that seek to introduce additional restrictions and build additional national borders in cyberspace.

ACKNOWLEDGEMENTS

This paper has been supported by the Kazan Federal University Strategic Academic Leadership Program.

REFERENCES

1. Warren Samuel D., Brandeis Louis D. The Right to Privacy // Harvard Law Review. 1890. Vol. IV. № 5. Pr. 193-220 / https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy
2. McKay Robert B. The Right of Privacy: Emanations and Intimations // Michigan Law Review. 1965. Vol. 64. № 2. Pp. 259-282 / https://repository.law.umich.edu/cgi/viewcontent.cgi?article=5464&context=mlr
3. N. S. Malein, Civil Law and individual rights in the USSR. Moscow, 1981, 216 p.
4. Maleina M. N. Personal non-property rights of citizens: concept, implementation, protection. Moscow, 2001. P.153.
5. O. E. Kutafin, Inviolability in the Constitutional law of the Russian Federation. Moscow: Layer Publ., 2004, 407 p.
6. C. Liang, Red Light Green Light: Has China Achieved its Goals through the 2000 Internet Regulations? // Vanderbilt Journal of Transnational Law. 2001. Vol. 34. № 5. Pp. 7–22.
7. Zhang Lena L. Behind the 'Great Firewall': Decoding China's Internet Media Policies from the Inside // Convergence: The International Journal of Research into New Media Technologies. 2006. Vol. 12. № 3. Pp. 271-291 / https://journals.sagepub.com/doi/abs/10.1177/1354856506067201
8. Taneja H., Xiao Wu A. Does the Great Firewall Really Isolate the Chinese? Integrating Access Blockage with Cultural Factors to Explain Web User Behavior // The Information Society. 2014. Vol. 30. No. 5. Pp. 297-309 / https://www.tandfonline.com/doi/abs/10.1080/01972243.2014.944728://www.tandfonline.com/doi/abs/10.1080/01972243.2014.944728
9. 中华人民共和国网络安全法 / https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin
10. Yanga Q., Liub Y. What's on the other side of the great firewall? Chinese Web users' motivations for bypassing the Internet censorship // Computers in Human Behavior. 2014. Vol. 37. Pp. 249-257 / https://www.sciencedirect.com/science/article/abs/pii/S0747563214002775
11. M. A. Filaleev, N. A. Sitdikova, E. E. Nechai, Digitalization as a factor of transformation of state institutions in the PRC. 2021. Vol. 11. No. 7. P.2137-2143.
12. Quinn J. A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law // SMU Science and Technology Law Review. 2017. Vol. 20. No. 2. p. 428.
13. Bellaby R.W. Going dark: anonymizing technology in cyberspace // Ethics and Information Technology. 2018. Vol. 20. Rr. 189–204 / https://link.springer.com/article/10.1007/s10676-018-9458-4
14. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) / https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html
15. Adamski H. Hassreden (Hate Speech) im Internet. Zum Streit um das Netzwerkdurchsetzungsgesetz (NetzDG) // Gesellschaft. Wirtschaft. Politik. 2018. № 1. S. 135-142.
16. Feldmann T. Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung // Kommunikation &Recht. 2017. № 5. S. 292-297 / http://www.feldblog.de/wp-content/uploads/2017/04/KuR_05_17_Beitrag_Feldmann.pdf
17. Hagen L.M., Au A.-M., Wieland M. Polarisierung im Social Web und der intervenierende Effekt von Bildung: eine Untersuchung zu den Folgen algorithmischer Medien am Beispiel der Zustimmung zu Merkels «Wir schaffen das! » // Kommunikation@Gesellschaft. 2017. № 18. S. 1-20 /

https://www.ssoar.info/ssoar/bitstream/handle/document/51503/ssoar-ketg-2017-Hagen_et_al-Polarisierung_im_Social_Web.pdf?sequence=3&isAllowed=y&lnkname=ssoar-ketg-2017-Hagen_et_al-Polarisierung_im_Social_Web.pdf
18. Błotny M. Prawo do ochrony danych osobowych w Konstytucji RP na tle prawa Unii Europejskiej oraz orzeczenia Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/114 Schrems v. Data Protection Commissioner // Zeszyty Naukowe Prawa Konstytucyjnego. 2017. № 10. S. 12-25; Waglowski P. Ochrona dóbr osobistych i danych osobowych Warszawa: PARP. 13 s.; Węgrzyn J. Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym. Wrocław 2013. 274 s. / https://repozytorium.uni.wroc.pl/Content/41087/Prawo_konsumenta_do_informacji.pdf
19. Préposé fédéral à la protection des données et à la transparence (PFPDT) / https://www.edoeb.admin.ch/edoeb/fr/home.html
20. Autoriteit Persoonsgegevens / https://www.autoriteitpersoonsgegevens.nl/
21. Klachtenrapportage: facts & figures. Overzicht 2020 / https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_klachtenrapportage_2020.pdf
22. Meldplicht datalekken: facts & figures. Overzicht feiten en cijfers 2020 / https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf
23. Lynskey O. Deconstructing data protection: the «Added-value» of a right to data protection in the EU legal order // International and Comparative Law Quarterly. 2014. Vol. 63. No. 3. Pp 569-597.
24. Politou E., Alepis E., Patsakis C. Forgetting personal data and revoking consente under the GDPR: Challenges and proposed solutions // Journal of Cybersecurity. 2018. Vol. 4. № 1. Pp. 1-20 / https://www.researchgate.net/publication/323202685_Forgetting_personal_data_and_revoking_consent_under_the_GDPR_Challenges_and_Proposed_Solutions
25. McCarty-Snead S.S., Hilby A.T. Research Guide to European Data Protection Law // International Journal of Legal Information. 2014. Vol. 42. No. 2. Pp. 348-417.

Georgy Borisovich Romanovsky
Doctor of Law, Professor, Head of the Department «Criminal Law» of the Law Institute of Penza State University, Author of more than 450 scientific publications, Expert of the Russian Scientific Foundation. Main scientific interests: human rights, current problems of criminal law.
Evgeniy Batyrovich Sultanov
Candidate of Juridical Sciences, Associate Professor, Head of the Department «Constitutional and Administrative Law» of the Law Faculty of the Kazan (Volga) Federal University, author of a number of scientific publications, Member of the Commission on Amending the Constitution of the Russian Federation. Scientific interests: principles of the Constitution and principles of local self-government.
Rifat Rasimovich Kil'deev
Postgraduate student of the Department of State-Law Disciplines, Institute of Law, Penza State University. Author of 14 scientific papers. Main research interests: human rights, current issues of privacy.