THE DIGITAL IMPACT ON THE CONSTITUTIONAL HUMAN RIGHTS

Abstract

The article analyzes the controversial issues of protecting the constitutional rights of citizens to information, to privacy, as well as to preserve the secrecy of correspondence, telephone conversations, and other messages in the digital era. The study identifies major legal risks of using the advanced information processing methods in the new digital reality: first, the risk of unintentional deanonymization of personal data; secondly, the risk of generating falsified information. We propose solutions, such as introducing an information audit system and a two-component information reading system. They can help to overcome the legal risks of data deanonymization and information falsification. We conclude that digital technologies have a significant impact on the content and methods of protecting some constitutional rights of citizens.

Author

Pechatnova Yulia Vadimovna

Masters student, Law Institute of Altai State University
(Barnaul, Russia)

The digital revolution marks the final transition from the industrial to the post-industrial type of society, in which information has acquired the role of the full-fledged asset. At the same time, in the light of digitalization, the conflict has already emerged between the requirements of legislation in the field of information protection and the transparency of the Internet. As the result, the problem of full-fledged legal regulation of the public data on the Internet is revealed.

Such constitutional human rights as the ability to fully protect the right to privacy and the right to privacy of correspondence, telephone conversations and other communications is the most difficult and controversial in the digital age. The purpose of this work is identification of the main legal risks in the development and mass distribution of digital technologies, as well as search for possible ways to overcome their negative impact on the observance of the constitutional rights of citizens.

The research methodology is based on general scientific methods of analysis and synthesis, as well as special scientific formal legal and comparative legal methods. The relevance of the research lies in the absence of appropriate legal regulation of information circulation in the context of the rapid development of digital technologies.

Digital technologies open up tremendous opportunities for creating advanced methods for collecting, processing and storing information. Such programs, called Big Data in the business environment, can generate results that are not envisioned by the developer, but are possible due to the introduction of the ability to analyze and compare unlimited amount of data into the program. The rapid development

of Big Data is due to the significant economic advantage obtained from the use of new technologies. For example, in the field of banking, there is an increase in the activity of the industry of information brokers, who, through Big Data technologies, accumulate and analyze in the interests of lenders information about potential borrowers, which, among other things, include personal data [1].

In most cases, the use of personal data means their intended use. Considering the fact that Big Data is the reusable digital asset, legislative consolidation of its intended use hinders business development. Therefore, due to the fact that Big Data is gradually being transferred to the commercial area, personal data as the part of Big Data periodically becomes the currency for paying for Internet services, asset of companies, marketing maneuver, commercial product provided by information brokers to interested companies.

The introduction of Big Data into the market turnover is becoming an irreversible process. At the same time, significant changes in the field of information circulation affect the relationship between the exchange of personal data and the protection of privacy in such a way that the latter requires additional measures to be taken to protect them.

As the measure to protect personal data, it is proposed to transfer user data into the sphere of civil circulation, and avoid situations when personal data is sold for commercial benefit. At the same time, the differentiation of user data and personal data, the introduction of some into circulation and the strengthening of measures to protect others from circulation are not possible. The key risk is the possibility of data deanonymization by artificial intelligence, which has the ability to establish the personal data of a specific person during the joint analysis of several anonymized user databases [3].

Thus, two main factors: the increase in the productivity and availability of computing power of artificial intelligence, as well as the huge array of personal information available on the Internet, make it technically possible to deanonymize even carefully anonymized data. In this regard, the opinion of Marshall McLuen is interesting, who believes that the Internet and privacy are incompatible concepts. Therefore, the ubiquitous spread of digital technologies will turn history back and humanity will again find itself residents of "one global village" in which privacy will be done away with [2]. Thus, Big Data is incompatible with the concept of informed, specific and conscientious consent as the main basis for legitimizing the processing of personal data.

Moreover, the technological capabilities of Big Data indicate that anonymization of personal data is gradually ceasing to be the guarantee of their anonymity. Moreover, the capabilities of artificial intelligence are not limited by the ability of scan information, posted by users on the Internet. For example, the ability of artificial intelligence to generate mixed realities blurs the boundaries of the "truth" and challenges the perception of Internet users, who find themselves in the fake reality. At the same time, the technical possibility of exposing misinformation becomes more complicated every year, since artificial intelligence technologies allow creating falsified information practically indistinguishable from reality, backed up by synthetic fake photographs, audio and video recordings.

In these conditions, the government can ensure the safety of only those citizens and organizations that voluntarily agree to soften standards to the extent, which is necessary to comply with the requirements of international and national security. At the same time, restrictions should be formulated with the maximum degree of accuracy and reflect the answers to the questions when, how and by whom these exemptions from the legal regime can be used.

It seems that the attention of the legislator should be focused on the following legal risks. First, artificial intelligence can achieve unintended results that lead to

violations of the legal regime for the protection of personal data and the secrecy of correspondence, telephone conversations and other messages. Secondly, artificial intelligence is able to generate falsified information that constructs an alternative reality and serves as the powerful propaganda weapon.

The legal risk of artificial intelligence gaining access to the unlimited amount of data can be prevented by conducting the periodic information audit of the system and removing unnecessary user data, including the personal data of those persons who do not meet certain criteria. The legal risk of generating falsified information should be prevented by introducing the two-component system that includes personal inviolable data and personal machine-readable data. Thus, information should be collected by the monitoring system and immediately translated into the coded machine-readable form. Thus, only the machine gets access to any information by reading the programming code, while the read information is not verified in the human-readable form. Consequently, platform operators will be significantly limited in their ability to deliberately falsify data.

Thus, the development of digital technologies has the significant impact on the constitutional rights of citizens, which require either the revision of existing concepts or the adoption of additional measures to protect them.

References

1. Voinikanis E.A., Semenova E.V., Tyulyaev G.S. Artificial intelligence and law: challenges and possibilities of self-learning algorithms [Iskusstvennyj intellekt i pravo: vyzovy i vozmozhnosti samoobuchayushchihsya algoritmov] / E.A. Voinikanis, E.V. Semenova, G.S. Tyulyaev // Civil law. Civil Procedure [Grazhdanskoe pravo. Grazhdanskij process], 2018. — № 4. — P. 137–148. (in Russ.)

2. McLuhan, M. Understanding media: external expansion of a person [Ponimanie media: vneshnee rasshirenie cheloveka] — M.: Zhukovsky: "CANON-press-Ts", "Kuchkovo Pole", 2003. — 464 p. (in Russ.)

3. Saveliev A.I. Problems of the application of legislation on personal data in the era of "Big Data" [Problemy primeneniya zakonodatel'stva o personal'nyh dannyh v epohu «Bol'shih dannyh» (Big Date)] / A.I. Savelyev // Law. Journal of the Higher School of Economics [Pravo. ZHurnal Vysshej shkoly ekonomiki], 2015. — P. 43–66. (in Russ.)