# Guarantees of the Constitutional Right to Privacy in the Digital Environment: The Legislation of the Eu, Eu Member States, Russia and China

**Alsu Machmutovna Khurmatullina[1], Rimma Rashitovna Amirova[2], Aisylu Machmutovna Khurmatullina[3]**

*[1]Kazan Federal University*
*Senior Lecturer of the Department of Constitutional and Administrative Law*
*Law Faculty of KFU, akm551@mail.ru*

*[2]Kazan Federal University*
*Associate Professor of Constitutional and Administrative Law*
*Law Faculty of KFU, arimma60@mail.ru*

*[3]Kazan Federal University*
*Assistant of the Department of Internal medicine diseases, Safian333@mail.ru*

## Abstract

The European Union, like any other international organization, originated from an intergovernmental agreement in which the contracting governments have given up some of their sovereign powers and authorities in favor of a supra-governmental institution in order to achieve common goals. The unique feature of this structure is that it has not given up on the citizens of these governments beyond the mutual rights and duties between the member states and has in fact organized a self-sufficient legal order and regime. This feature has caused the institution in charge of interpreting the founding documents of the Union, namely, the European Court of Justice, to infer the general principles of the direct effect and supremacy of European Community rights, which can be considered a form of constitutionalism. The article is devoted to identifying the features of the transformation of one of the most important constitutional and legal institutions for a person – the human right to privacy in a digital society, which is based on the digital environment. The subject of the study is the legislation of the European Union, the member States of the European Union, Russia and China in the field of regulating the right to privacy, the implementation of which is being modified under the influence of emerging complex institutions in the digital society, including various forms of human interaction with robotics. The issue related to the implementation of human rights in the information society is considered. The article analyzes the data privacy guarantees of individuals operating within the European Union. The authors also consider the features of implementing Big Data technologies that allow us to structure social reality in a new way in the context of the transformation of the right to privacy. The optimal ways to improve the national and international legal regulation of the legal status of a person and citizen in the context of new technological opportunities of mankind are proposed.

**Keywords***:* Law, human rights, right to privacy, digital environment, personal data, confidentiality, state, guarantees.

## Introduction

With the digital environment, there is a problem of preserving the human right to privacy in its traditional sense. According to K. Davidson, the most important parameters of this environment are multi-dimensionality and openness [2, p. 708]. The Internet space requires the development of its own specific algorithm for building relationships and interaction of a person with a technological device and software. However, at present, the subjects of the digital society are forced to play by the rules that are built by the owners or administrators of an Internet resource, where there is no place for the principle of personal inviolability and privacy.

The analysis of social relations on the web reveals the "digital inequality" that calls into question the value of the person himself, his rights and freedoms, which was developed by the efforts of the entire world community in the post-war period.

According to the law, doing some unauthorized activities in cyber space is a crime. As you know, there are different types of crimes in cyberspace and criminal actions can be carried out in this virtual network in many ways. Here we introduce some of the crimes that occur in cyberspace. According to Article 14 of the Computer Crimes Law and Paragraph 2 of Article 6 of the Press Law, publishing, distributing and trading vulgar and obscene content against public modesty in cyberspace is considered a crime, and the perpetrator must undergo legal punishment. Likewise, defamation is another offense that, if done, will result in punishment.

The police warned people who defame and spread lies against each other in cyberspace and social networks that according to Article 17 of the Computer Crimes Law, by proving their criminal act, they should be accountable to the law and responsible for their criminal act. In addition to the mentioned cases, inciting, encouraging, persuading, threatening or inviting corruption and prostitution and committing crimes against chastity or sexual perversions are punishable according to paragraph b, article 15 of the Computer Crimes Law and article 639 of the Islamic Penal Code. Article 6, paragraph 2 of the press law talks about the spread of obscenity and obscenities, and this is also one of the criminal cases in the cyberspace, in addition to the instrumental use of people (both men and women) in images and content, humiliating and insulting women. Advertising illegitimate and illegal rituals and luxuries is also considered a crime. If disruption of national unity and creating differences between social strata occurs in the cyber space, especially through raising racial issues, the perpetrator is guilty and must be held accountable for his criminal act.

One of the topics that has become a serious challenge regarding cyberspace today is the discussion of the rules governing cyberspace. The legal issues that are raised in cyberspace are new to a large extent and have no history in the legal system, and therefore not only there is no predictable answer about it, but sometimes an answer for it cannot be imagined in a short time, and the same thing. It can create more challenges. One of the areas where more consistent laws need to be formulated is the issue of virtual businesses. It is the design and use of domestically produced software that requires a foundation and efficient rules, because some of the problems and inadequacies that plague people in practice in the virtual space and are more apparent in the discussion of filtering are due to the defects in the preparation and formulation of rules. It is dynamic and adapts to the needs of society.

Over the past few years, Big Data technologies have become one of the new sources of knowledge about a person and society: preferences, needs, individual and collective strategies, and lifestyles of millions of people are identified and classified. Data protection and the problem of privacy is becoming one of the urgent problems of the beginning of the XXI century [10, p. 39]. An example of a solution to this problem can be interim measures in EU law, which has strict rules for the processing of personal data. At the same time, in most cases, the judicial authorities have to fill in legislative gaps, which, in turn, delays the moment when a citizen exercises his right, and each time the court has to decide the issue on an individual basis.

Features of the implementation of the right to privacy are currently associated with the development of the digital environment, which should be understood as an artificially created information environment, the value of which is the presence of huge databases, information repositories and the ability to quickly search for it. As K. Hayne notes: digital data act as a communication tool [1, p. 270].

Here we can distinguish two trends that can be observed at the present time. The first trend is the establishment of additional guarantees for the exercise of citizens' right to privacy, one of which is the tightening of requirements for these citizens. This trend is mainly evident in European countries. The second trend is the lack of guarantees for the exercise of citizens' right to privacy, which allows the state to control the actions of its citizens in this way. An example is China's experience in implementing an individual rating system based on the assessment of personal behavior of citizens.

## Methods

The study methodology is expressed by systematic, structural-functional, structural-logical, historical, as well as dialectical methods of scientific knowledge, collection and analysis of scientific and practical material. A review article is a type of article that reviews the background of a scientific topic. In review articles, the results presented in scientific writings about a specific topic are summarized and evaluated. This type of article may examine anything, it is designed to summarize, analyze and evaluate information that has already been published. In such articles, experimental and new findings are rarely reported. Review articles have a well-defined narrative, are usually critical, and should provide theoretical and emerging interpretations. The important role of review articles is to guide original scientific writings. For this reason, it is essential that the citations provided are accurate and complete.

## Results and discussion

The principles that govern members of the Organization for Economic Cooperation and Development (most of the European Union States) can be used as an example of establishing legal principles that serve as a guide in regulating confidentiality (data protection) in the digital environment. Both the public and private sectors in these countries are in charge of providing the following: 1) restrictions on data collection; 2) assurance of data quality; 3) purpose specification of data at time of collection; 4) limitation of data use to specified purpose; 5) assurance of security safeguards; 6) openness about practice, policies, and developments regarding the data; 7) specified set of rights for the individuals from whom data is collected; 8) accountability of the data controller. The General Data Protection Regulation (GDPR), which contains stricter равила аит data protection rules, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations of the United States serve

as the foundation for the regulatory framework. Let's concentrate on a few provisions of the General Data Protection Regulation (GDPR) of the European Union. The decree was passed on April 27, 2016, was approved two years later, went into effect on May 25, 2018, and is applicable to all EU member states as well as foreign businesses doing business there, giving it a truly global impact. The GDPR's protections are present in U.S. law, albeit in weaker, less rigid forms. S. both in agreements with businesses reached by the Federal Trade Commission and in privacy laws. Prior to it, the European Union adopted Directive 95/46 EC in 1995[4] titled "On The law defined the role of a data protection officer (data protection officer), listed the rights and obligations of the following subjects, and agreed to guarantee the protection of your personal information from third parties online, including "cross-border transfer of data, pseudonymization, "installed "right to be forgotten," and genetic data, biometric data, and health data. For instance, according to Article 13 of the GDPR the data subject has a broad range of rights that are set. In the event of a person's objection, data processing is only allowed when it is necessary to carry out a task in the public interest, which takes precedence over the interests, rights, and freedoms of the data subject and must be demonstrated by the controller (Article 21 GDPR). However, restrictions on rights are also possible, and the regulation outlines two prerequisites for doing so: 1) the adoption of a law; and 2) the adoption of the law for one of the purposes listed in paragraphs a through j of Article 23 (among them: preserving public safety, national security, and other purposes). Take the legislation of Germany, one of the member states of the European Union.

German legislation establishes special mechanisms aimed at reducing the risks of restricting a person's right to privacy:

1) Data processing is permitted if the person has explicitly (mostly in writing) given their consent to the collection, processing and use of the data (Section 4, paragraph 1, section 4A).
2) The automated processing procedure used must be approved by the Data Protection Authorities (section 4D), whose activities are limited to control and supervisory functions (at the industry level, the data protection authorities in broadcasting institutions are responsible for the computer processing of personal data)
4) Operation of the principle of economy and non-use of data: all data processing systems should aim to avoid using or use personal data as little as possible and, in particular, to use the possibilities of anonymity and pseudonymity. (Section 3A).
5) Extending the scope of the Federal Data Protection Law to legal entities. Although there is no provision for this in the law, some administrative courts have also applied the data protection laws to legal entities
6) Special protection of so-called special data types (Section 3 of ABS. 9 of the BDSG), namely data on ethnic origin, political opinion, religious or philosophical beliefs, trade union affiliation, health and sexual life. In accordance with section 4D of ABS. 5 of the BDSG, this data is subject to preliminary control. This means that data processing in institutions that collect, process or store this type of data must be verified before data processing begins. This is the responsibility of the Data Protection Officer, who must be hired by the relevant institution.
7) A wide range of rights of persons whose data is stored in state or non-public bodies):

- Right to information about what personal data is stored and where
- The right to information about the sources from which this data is received and why it is stored
- Right to correct false personal data
- Right to complain to the relevant data protection authority
- The right to delete or block records.

* the right to refuse to use their address data for advertising or for market research or public opinion in the body that stores the data, and to request that their data be blocked.

- Right to prohibit the transfer of personal data to third parties (section 6 (1) of the BDSG)

It should be noted that the first two rights cannot be exercised if the general public interest, the interest of the relevant non-public body in keeping commercial secrets, or the interest of third parties in non-disclosure outweighs. Refusal to receive information must be documented with the reasons given.

At the same time, in the conditions of the digital environment, the legislation of most states does not have a well-developed mechanism for guaranteeing rights implemented in the virtual space, which in turn can also be considered as a possibility of their restriction. For example, article 5A of the Greek Constitution recognizes the right to participate in the information society as an inalienable human right and declares it the duty of the State to promote it. Since July 1, 2010, Finland has guaranteed every citizen the right to access the Internet, but there are no specific guarantees for the exercise of the right to privacy on the Internet, and there is no possibility of holding the government accountable for the lack of these guarantees.

Consider the practice of implementing the right to be forgotten (Article 17 GDPR), which implies a limited right to data destruction, since conditions were provided for the possible further preservation of data in the presence of public interest or for research purposes [5]. As the judicial practice on the issue of violation of the right to be forgotten shows, this right is not absolute, its implementation depends on specific circumstances [6], in order to avoid contradiction with fundamental human rights, such as freedom of speech and the press. To exercise this

right, the relevant search engine must weigh the consequences of deleting information, i.e., on the one hand, public interest or other significance must be taken into account, and on the other, the harm caused by mentioning its name to the person requesting deletion [7].
Laws that provide for such rights as the right to access the Internet and the right to be forgotten are still not developed, and there are no clear standards and criteria that allow you to exercise personal rights, in particular, the right to privacy by deleting certain information.
The protection of other constitutional values may necessitate limitations on an individual's right to privacy and the rights of data subjects for purely objective reasons. As a result, human rights can be restricted by law in the interests of public health and safety, as stated in article 16 of the Italian Constitution. Article 55 of the Russian Federation's Constitution states that restrictions on civil and human rights and freedoms may only be made in order to safeguard others' rights, interests, and health as well as the security of the state. We can use the infringement of human rights brought on by the spread of COVID-19, a coronavirus infection, as an example. In order to adhere to constitutional requirements and guarantee the protection of others' health, Federal Law No. 68-FZ, dated December 21, 1994, "On the Protection of the Population and Territories from Natural and Man-made Emergencies," was amended, enabling the Government of Russia and state authorities of the constituent entities of Russia to adopt regulations aimed at ensuring the security and protection of One of these regulations was Decree of the Mayor of Moscow No. 43-UM, dated April 11, 2020, which mandated that residents issue digital passes in order to travel throughout the Moscow city limits using any mode of transportation. The following details were required from the citizen during registration: surname, first name, patronymic, passport series and number or other identity document details, contact phone number, state registration number of the vehicle they plan to travel in, name of the organization for which the digital pass is issued, and employer's taxpayer identification number. Citizens were subject to administrative liability in the form of a fine for these offenses.

## Summary

The foundation of human rights, including the right to privacy, is changing as a result of the development of digital technologies. The legislation on the protection of personal data, which establishes broad rights of data subjects, including "right to be forgotten," is one of the safeguards for the exercise of this right. It should be kept in mind, though, that the legislation that has been passed in this area does not permit us to guarantee the full implementation of either the right to privacy or the rights of data subjects. First off, the need to safeguard other constitutional values based on public interests makes it possible to limit the scope of rights exercised. We can use the acquisition of a digital pass bearing a personal data message as an illustration. In the context of the Covid-19 outbreak, this pass would allow one to exercise their right to freedom of movement. Second, there is no clear mechanism in the laws for enforcing certain rights of data subjects (such as the right to be forgotten), and there is also no clear mechanism for prosecuting those who transgress these rights. In this regard, the law should establish a specific mechanism for implementing the right; for instance, the law on personal data, which establishes the right to be forgotten, should contain concrete criteria that must be met before data can be deleted (for instance, the data cannot be used to publish investigative journalism or literary works on a website). We also believe it is necessary to create a specific body that will be in charge of carrying out this mechanism.

## Conclusion

In the modern world, we can observe a reality where there is an "all-seeing eye" that is aware of a significant part of a person's life, evaluates his actions, rewards good for good deeds and punishes for mistakes. Based on digital technologies, the so – called "social credit system" or to be more precise, "social trust system" is actively scales in China. With the help of various structures: the tax authority, the court, the municipality, corporations in conjunction with digital technologies, the state assigns citizens an individual rating, through which the state tracks and evaluates Chinese citizens in real time. It should be noted that the trust rating of individuals is linked to the internal passport [8]. Through such control, the state evaluates not only the legality of actions and actions performed by citizens, but also instills moral guidelines in behavior. At the same time, the country is actively developing various studies in the field of genetic engineering, which in turn affects the scope of human rights and freedoms, in particular, the right to personal integrity, the right to personal and family secrets, and others. As noted in the literature, "China is a special socio-cultural space in which the concept of human rights, freedoms and duties differs from the classical European system of values" [9, p. 158].

## Acknowledgements

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

## Bibliography

[1] C. Hine, Databases as Scientific Instruments and Their Role in the Ordering of Scientific Work // Social Studies of Science. 2006. Vol. 36, № 2. P. 269–298.
[2] C. Davidson, Humanities 2.0: Promise, Perils, Predictions // Publications of the Modern Language Association of America (PMLA). 2008. P. 707–717.
[3] Universal Declaration of Human Rights adopted by the UN General Assembly on 10.12.1948 // Russian newspaper. 10.12.1998.
[4] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal of the European Communities. 23.11.1995. No L 281/31
[5] European Parliament legislative resolution dated March 12, 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation // OJ C 229, 31.7.2012, p. 90.
[6] European Commission, Factsheet on the «Right to Be Forgotten» ruling (C-131/12) // Orlowski Andrew, The Register Google de-listing of BBC article 'broke UK and Euro public interest laws' — So WHY do it?
[7] Andrew Orlowski, The Register Google de-listing of BBC article 'broke UK and Euro public interest laws' — So WHY do it? // // The Register. Jul.2014.
[8] L. A. Kovacic, Big Brother 2.0: How China is Building a Digital Dictatorship. URL: http://carnegie.ru/ commentary/71546 (accessed: 21.10.2017).
[9] M. O. Orlov, Multi-dimensionality of the digital environment in the risk society, Saratov University Bulletin, New Series, Series of Philosophy. Psychology. Pedagogy. 2019. Vol. 19, issue 2. pp. 155-161.
[10] Lane J., Stodden V., Bender S., Nissenbaum H. Privacy, Big Data and the Public Good: Frameworks for Engagement. Cambridge University Press, 2014. 344 p.