

МЕЖДУНАРОДНО-ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ ОТ ЦИФРОВЫХ УГРОЗ

Анна Владимировна Хромова^а

DOI: 10.22394/2070-8378-2023-25-6-110-114

Амина Сурпкелова^а

^а Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

Аннотация: С развитием информационных технологий и глобализацией Интернета личные данные стали уязвимыми перед новыми видами рисков и угроз. Цель статьи – рассмотреть ключевые международно-правовые нормы, стандарты и конвенции, ориентированные на защиту прав личности в сфере цифровой безопасности. В статье определяются сильные и слабые стороны существующих механизмов и их соответствие вызовам современного цифрового ландшафта. На фоне быстрого технологического развития и появления новых видов угроз авторы подчеркивают важность постоянного обновления и адаптации международных правовых инструментов для обеспечения эффективной защиты личности от цифровых рисков. Цифровые технологии имеют потенциал как для снижения, так и для усугубления дискриминации в различных сферах жизни. Важно учитывать, что технологии сами по себе нейтральны, но их разработка, применение и алгоритмы могут стать источником дискриминации. Угрозы в киберпространстве часто имеют трансграничный характер, и их решение требует совместных усилий мирового сообщества.

Ключевые слова: цифровые технологии, цифровые угрозы, личные данные, международное право, защищенность личности, информационная безопасность

Благодарность: Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС при Президенте Российской Федерации по теме: «Совершенствование законодательства в области защищенности личности от информационных угроз в цифровой среде».

Дата поступления статьи в редакцию: 10 декабря 2023.

INTERNATIONAL LEGAL MECHANISMS FOR PROTECTING INDIVIDUALS FROM DIGITAL THREATS

Anna V. Khromova^a

Amina Surpkelova^a

^a Russian Presidential Academy of National Economy and Public Administration

Abstract: The evolution of information technology and the Internet has made the issue of personal data security relevant to new types of risks and vulnerabilities. The article focuses on the core international legal norms, standards, and conventions centered on protecting individual rights in the field of digital security. The authors identify the strong and weak points of existing mechanisms and their relevance in addressing the challenges of today's digital environment. The author emphasizes the significance of constant updates and adaptations of international legal instruments in order to ensure efficient protection of individuals from digital risks, given the rapid advancement of technology and the emergence of new categories of security threats. Digital technologies have the potential to both reduce and exacerbate discrimination in different areas of life. It is important to keep in mind that technologies are generally neutral, but their design, application, and algorithms can be a source of discrimination. Threats in cyberspace are often cross-border in nature and addressing them requires the joint efforts of the global community.

Keywords: digital technologies, digital threats, personal data, international law, personal protection, information security

Acknowledgement: The article was prepared as part of the research work for the state assignment of the Russian Presidential Academy of National Economy and Public Administration on the topic «Improving the legislation in the field of personal protection from information threats in the digital environment».

Received: December 10, 2023.

Introduction

The advancement of digital communications and the evolution of information technology have made it necessary to create efficient international legal frameworks to protect personal data from emerging online threats. In this regard, the main goal of such mechanisms is to achieve a balance between privacy, innovation, and freedom of expression.

Safeguarding against digital threats is inextricably linked to the information security field. Within the framework of information law, information security is a self-contained and multifaceted legal construct that impacts all aspects of public life and guarantees sustainable functioning of the state [Beketov, 2004. P. 33].

Defining “information security” and “information security mechanisms”

The term «information security» is enshrined in the Information Security Doctrine of December 5, 2016. «Information security is a condition for protecting the individual, society, and the State from internal and external information threats, which ensures the realization of constitutional rights and freedoms of man and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity, and sustainable socio-economic development of the Russian Federation, national defense, and state security»¹. Legal regulation ensures a balance of interests for the individual, the state, and society in the digital information environment.

Thus, the definition of information security is a rather broad and complex concept; information security is becoming a global and transboundary concern, implying a comprehensive approach to security.

There are several approaches to defining the «information security mechanism». This category is not disclosed at the legislative level; however, if we look at the definition of «mechanism» in jurisprudence, we find that it refers to a system of interconnected, functional elements [Morozova, 2011]. Therefore, given the context of the topic under consideration, we can say that the existing mechanisms are used to guarantee the object's information security.

A.S. Boitsov mentioned that the «information security mechanism» is aimed at preventing the source of threats [Boitsov, 2015].

In their study, Litvinova Yu.I. and Kiss S.V. [Litvinova, Kiss, 2020] defined «information security mechanisms» as several existing or newly created state bodies, public entities, and deliberately formed legal, political, and

other links between them to ensure the national interests of the state and the individual in the information sphere.

International privacy law and standards

In the past, society paid little attention to the concepts of «safety» and «information security» [Levda, 2017]. This was mainly due to the barriers for accessing them, which were supported by the closed nature of the security field, seen as the prerogative of the highest political bodies, mainly focused on military aspects. However, presently, there is a paradigm shift.

When we refer to the protection of personal information, it includes two major aspects: the protection of personal data and the right to personal privacy. International regulations strive to balance the need to use data with protecting individual rights in the digital environment.

International privacy law encompasses a set of standards, norms, and conventions aimed at safeguarding the rights and privacy of individuals in an international context. In an era of globalization and world connectivity, we see a lot of data crossing borders. International norms provide guidelines for the safe and legal transfer of data between countries.

According to E.V. Vostretsova [Vostretsova, 2019. P. 209], the primary goal of information security standards is to create a basis for interaction between producers, consumers, and certification specialists.

Representatives of the realistic approach, R. Anderson and R. Hundley [Hundley, Anderson, 1994], consider the issue of ensuring information security through information infrastructure and efficient threat counteraction principles.

At the same time, representatives of the liberal approach insist on the mutual trust and cooperation principle. We should note that a number of international documents refer precisely to the liberal approach.

International legal mechanisms can be divided into two comprehensive and interdependent strands:

1. International legal agreements;
2. Standardization.

The authors incorporate concepts, declarations, doctrines, conventions, and other agreements governing the information domain into the legal direction. International legal agreements are the foundation for further elaboration of standards.

Software developers and data processors are required to follow certain standards as part of standardization. Certification specialists view standards as an instrument to provide an assessment of a system's security level. Other core aspects of data protection include encryption techniques to safeguard data confidentiality, intrusion monitoring and detection, and application security.

1 Doctrine of Information Security of the Russian Federation. Approved by the Decree of the President of the Russian Federation dated December 5, 2016, No. 646. <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html>

Международный опыт

The international human rights law imposes certain obligations on the State².

International treaties and conventions have been developed in response to the violation of people's rights to personal security. With the growing threat of information attacks and cybercrime, the documents below are still relevant:

1. The Universal Declaration of Human Rights was adopted by the UN General Assembly in 1948. Article 12 recognizes privacy and protection from arbitrary interference with personal and family life³.

2. The European Convention for the Protection of Human Rights and Fundamental Freedoms was adopted by the Council of Europe in 1950. Article 8 of this convention guarantees the right to protect privacy and personal data⁴.

3. The International Covenant on Civil and Political Rights (ICCPR, Art. 17) provides the right to protection against arbitrary or unlawful interference with personal life or privacy⁵.

4. The 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108. The treaty aims to ensure the protection of human rights in the field of automated processing of personal data⁶.

5. The Budapest Convention on Cybercrime, which was adopted by the Council of Europe in 2001, contains rules regarding offenses against computer systems and data security. This convention is the earliest international treaty on crimes committed through the Internet and other computer networks⁷. This convention aims to protect society from cybercrime and promote international cooperation.

6. In 2016, the European Union adopted the General Data Protection Regulation 95/46/EC. This regulation regulates the processing of personal data in member states and establishes the rights of data subjects and the requirements for data collection and processing⁸.

Digital technologies can both lessen and increase discrimination in different spheres of life. Technology itself is neutral, but its application, design, and algorithms may contribute to discrimination.

Using the Declaration on the Manipulative Power of Algorithmic Processes as a guide, let us examine some aspects of how digital technologies affect discrimination⁹:

- **Algorithmic discrimination:** algorithms may rely on insufficiently diverse data or contain biases that lead to incorrect conclusions and discrimination. For example, job recommendation algorithms may restrict certain groups of individuals.

- **Social and economic segregation:** technological solutions that rely on accessible data may increase social and economic inequalities. For example, the use of digital profiles can increase social segregation.

Digital threats are not limited to the borders of a particular country; therefore, international cooperation in data protection becomes critical. Promoting agreements and standards governing cross-border data processing is a primary goal for international organizations such as the UN and the OSCE. The Russian Federation supports its allies at the United Nations in their efforts to ensure that states fulfill their commitments¹⁰ and prevent cyberattacks originating from their territory that could threaten personal security and state sovereignty. Article 19 of the Updated Concept of the UN Convention on International Information Security provides that ICTs should not be used to violate human rights and freedoms.

Additionally, the 77th session of the UN General Assembly, held on December 7, 2022, adopted a resolution on «Developments in the field of information and telecommunications in the context of international security». This document emphasizes the importance of

2 International human rights law. UN Office of the High Commissioner for Human Rights. <https://www.ohchr.org/ru/instruments-and-mechanisms/international-human-rights-law>

3 The Universal Declaration of Human Rights. Adopted by Resolution 217 A (III) of the UN General Assembly of December 10, 1948. https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

4 The European Convention on Human Rights (as amended and supplemented by Protocols No. 11, 14, and 15, together with the Additional Protocol and Protocols No. 4, 6, 7, 12, 13, and 16) of 1950. https://www.echr.coe.int/documents/d/echr/Convention_RUS

5 The International Covenant on Civil and Political Rights. Adopted by General Assembly resolution 2200 A (XXI) of December 16, 1966. https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

6 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, January 28, 1981). <https://26.rkn.gov.ru/law/p7096/p14811/>

7 The Budapest Convention on Cybercrime. Council of Europe. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

8 The European Union's General Data Protection Regulation (GDPR). GDPR Text. <https://gdpr-text.com/ru/>

9 The Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes of February 13, 2019. Council of Europe. https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

10 Updated Concept of the United Nations Convention on International Information Security (2023). National Agency for International Security. <https://namib.online/wp-content/uploads/2023/07/86%D0%B8%D0%B8-%D0%9E%D0%9D-%D0%BE-%D0%9C%D0%98%D0%91-%D1%80%D1%83%D1%81%D1%81%D0%BA.pdf>

international cooperation for security¹¹. The adoption of such an instrument demonstrates states' desire to effectively regulate and coordinate efforts in the field of information security.

Special attention is paid to international cooperation as a key factor in ensuring security in the digital environment. This emphasizes the recognition that cyber threats are often cross-border in nature, and their solution requires the joint efforts of the global community.

Technical security measures are a set of standards and practices that guide organizations and governments across the globe to establish effective practices to protect personal data. For example, the International Organization for Standardization (ISO) is the most authoritative in the field of standardization. ISO has developed several standards dedicated to data protection and information security, including ISO/IEC 27001 and ISO/IEC 27701. The standards define requirements for information security management systems and a series of practical guidelines for ensuring data security. We should also mention the NIST cybersecurity Framework¹², which is a guide from the U.S. National Institute of Standards and Technology that describes cybersecurity principles, methods, and practices.

Despite the numerous documents developed and the comprehensive approach to the issue of personal data protection in the digital environment, there are still several gaps. For example, rapid technological advancement can cause existing standards to become outdated and fail to regulate identity protection reliably.

Legal mechanisms may not keep up with innovation due to the complexity of international decision-making, which could lead to threats evolving more quickly than countermeasures. Furthermore, ineffective state coordination and cooperation may leave gaps that attackers can take advantage of.

States are finding it difficult to agree on information security measures because of the tense international environment and the growth of full-scale information warfare. As a result, they are ignoring the chance to work together and prioritizing their interests over the safety of individuals in the digital sphere.

Conclusion

Protecting personal information online is becoming a more relevant and complicated concern in the digital age, as technology plays a growing role in the digital world. International legal frameworks are crucial instruments for guaranteeing the safety and security of private data in the digital era. They provide the foundation for setting standards, legislation, and required practices. Nevertheless, to address emerging risks and challenges, we must continuously modify these mechanisms due to the rapidity of technological development.

All foreign laws, acts, and standards are diverse; however, they all follow the same logic: as a requirement for compliance, every regulation mandates the regular implementation and maintenance of a risk management process. This requires ongoing cooperation. Apart from creating a formal information security policy, regulators are also requiring more frequent audits of the implemented security measures that have been evaluated by an impartial third party.

These mechanisms provide the foundation for a safer and more secure digital environment where individual rights and privacy remain a priority.

11 Basic documents in the field of international information security. National Agency for International Security. https://namib.online/wp-content/uploads/2023/01/A_RES_77_36-RU-%D0%9C%D0%98%D0%91-7.12.2022.pdf

12 NIST Cybersecurity Framework. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>

Литература

- Бекетов Н.В. Информационная безопасность развития государства. *Информационные ресурсы России*. 2004. № 6. С. 32–35.
- Бойцов А.С. Организационно-правовой механизм обеспечения информационной безопасности пограничных органов. *Актуальные проблемы российского права*. 2015. № 2 (51).
- Вострецова Е.В. Основы информационной безопасности. Екатеринбург: Издательство Уральского университета, 2019.

- Левда М.В. Информационная безопасность РФ. *Форум молодых ученых*. 2017. № 11 (15). С. 549–553.
- Литвинова Ю.И., Кисс С.В. Механизм обеспечения информационной безопасности государства: теоретико-методологические основы. *Юрист-правовед*. 2020. № 2 (93). С. 48–52.
- Морозова Л.А. Теория государства и права. Учебник. 4-е издание. М.: ЭКСМО, 2011.
- Hundley R., Anderson R. Security in Cyberspace: An Emerging Challenge for Society, 1994. In English

References

- Beketov N.V. Information security of state development. *Informatsionnyye resursy Rossii*. 2004. No. 6. P. 32–35. In Russian
- Boytsov A.S. Organizational and legal mechanism for the information security guarantees of the border authorities. *Aktual'nyye problemy rossiyskogo prava*. 2015. No. 2 (51). In Russian
- Levda M.V. Information Security of the Russian Federation. *Forum molodykh uchenykh*. 2017. No. 11 (15). P. 549–553. In Russian

- Litvinova Yu.I., Kiss S.V. Mechanism to ensure information security of the State: theoretical and methodological bases. *Yurist-pravoved*. 2020. No. 2 (93). P. 48–52. In Russian
- Morozova L.A. Theory of government and law. Textbook. 4th edition. M.: EKSMO, 2011. In Russian
- Vostretsova E.V. Fundamentals of information security. Ekaterinburg: Izdatel'stvo Ural'skogo universiteta, 2019. In Russian

Международный опыт

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Анна Владимировна Хромова, аспирант

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119571, Москва, проспект Вернадского, 82). E-mail: a.khrom1221@gmail.com

ORCID: 0000-0003-3329-3682

Амина Сурпкелова, аспирант

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119571, Москва, проспект Вернадского, 82). E-mail: a.surpkelova@gmail.com

ORCID: 0000-0002-3554-0352

Для цитирования: *Хромова А.В., Сурпкелова А. Международно-правовые механизмы обеспечения защищенности личности от цифровых угроз. Государственная служба. 2023. № 6. С. 110–114.*

INFORMATION ABOUT THE AUTHORS:

Anna V. Khromova, postgraduate student

Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119571, Russian Federation). E-mail: a.khrom1221@gmail.com

ORCID: 0000-0003-3329-3682

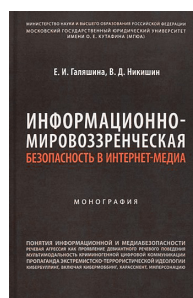
Amina Surpkelova, postgraduate student

Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119571, Russian Federation). E-mail: a.surpkelova@gmail.com

ORCID: 0000-0002-3554-0352

For citation: *Khromova A.V., Surpkelova A. International legal mechanisms for protecting individuals from digital threats. Gosudarstvennaya sluzhba. 2023. No. 6. P. 110–114.*

ЧТО ЧИТАТЬ?



Галяшина Е.И., Никишин В.Д. Информационно-мировоззренческая безопасность в интернет-медиа. Монография. М., «Проспект», 2023.

В монографии рассмотрены наиболее общественно опасные угрозы информационно-мировоззренческой безопасности в новой киберреальности, к числу которых относятся пропаганда и продвижение чужеземно-националистических идеологий и криминальных субкультур сетевыми молодежными сообществами, движениями и организациями, в том числе экстремистского и террористического толка, пропаганда антисемейных ценностей, кибербуллинг и т. д.

Работа содержит анализ действующего законодательства в сфере информации, а именно отдельных статей КоАП РФ, УК РФ, ГК РФ, а также тексты Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и др.

Законодательство приведено по состоянию на 20 октября 2022 г.

Издание предназначено для педагогов, руководителей образовательных организаций, сотрудников органов государственной и муниципальной власти, ответственных за реализацию молодежной политики и политики в сфере защиты прав детей, а также для представителей общественных организаций, реализующих проекты в сфере противодействия деструктивной пропаганде в подростково-молодежной среде.