

Article

Protection of Human Rights in Cybersecurity Policy: Analysis of Global Governance and National Approaches

Gavharoy Qavulova*¹

1. Student of Fergana State University

*Correspondence: alfargoniy.uz@gmail.com

Abstract: This article examines the complex relationship between cybersecurity policy and the protection of human rights from the perspectives of global governance and national approaches. As digital transformation continues to accelerate, maintaining a balance between cybersecurity requirements and fundamental rights such as privacy, freedom of information, and freedom of expression has become an increasingly important challenge. The study explores international legal and regulatory frameworks developed by global organizations, analyzes the experiences of advanced countries, and evaluates the impact of national cybersecurity strategies on the protection of human rights. Furthermore, the article assesses the implications of emerging technologies, including artificial intelligence (AI), Big Data, and digital surveillance systems, for the realization and protection of human rights in the digital environment. The findings demonstrate the necessity of developing cybersecurity policies grounded in human rights principles in order to ensure both security and individual freedoms in cyberspace.

Keywords: Cybersecurity, human rights, global governance, digital security, data protection, Internet governance, artificial intelligence, digital freedom, right to privacy, cyberspace.

Citation: Qavulova G. Protection of Human Rights in Cybersecurity Policy: Analysis of Global Governance and National Approaches. Middle European Scientific Bulletin 2026, 46(3), 20-23.

Received: 05th Mar 2026Revised: 10th Apr 2026Accepted: 15th May 2026Published: 05th Jun 2026

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

Introduction

In the twenty-first century, digital technologies have become an integral part of human development. The increasing digitalization of public administration, economic activities, education, healthcare, and social communication has elevated cybersecurity to one of the most important issues on the global political agenda. However, measures aimed at ensuring cybersecurity may, in certain circumstances, lead to restrictions on human rights and fundamental freedoms. In particular, the expansion of internet traffic monitoring, mass surveillance systems, biometric identification technologies, and artificial intelligence-based control mechanisms has raised significant concerns regarding the right to privacy and freedom of information. Therefore, one of the primary objectives of contemporary cybersecurity policy is to establish an appropriate balance between security requirements and the protection of human rights. International legal instruments, including the United Nations' Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and various UN resolutions concerning digital rights, recognize that human rights must also be protected and exercised within the digital environment [1]. At the same time, the need to safeguard national security interests and combat cyber threats has, in some cases, encouraged the development of political mechanisms that may limit digital freedoms. Consequently, the relationship between cybersecurity and human rights has emerged as a significant area of contemporary

political-philosophical and legal research, attracting growing attention from scholars, policymakers, and international organizations worldwide.

Materials and methods

The relationship between cybersecurity and human rights has become one of the most extensively studied topics within the international academic community over the past decades. While early research primarily focused on information systems security and national security concerns, the rapid expansion of the Internet and digital technologies has led to the emergence of human rights protection in cyberspace as a distinct field of scholarly inquiry. In particular, Daniel J. Solove identified privacy protection as one of the most significant legal and ethical challenges of the contemporary information society and examined the impact of digital surveillance technologies on individual freedoms [1]. According to Solove, the uncontrolled collection and processing of personal data pose serious threats to individual autonomy and legal protection. Similarly, David Lyon developed the concept of the “surveillance society,” emphasizing the growing capacity of both governments and corporations to monitor individuals through digital technologies [2]. These studies have contributed significantly to the theoretical foundations supporting the integration of human rights principles into cybersecurity policymaking.

Among the most influential scholars in the fields of Internet governance and global cybersecurity are Laura DeNardis and Milton Mueller. DeNardis argues that Internet governance should not be understood merely as a technical process but rather as a system of political and geopolitical relations [3]. In her view, control over Internet infrastructure is directly linked to human rights, freedom of information, and democratic governance. Mueller, on the other hand, analyzes the interactions between state and non-state actors in Internet governance and highlights the advantages of a multi-stakeholder governance model in global cyberspace [4]. His research demonstrates that effective cybersecurity governance requires the participation of governments, private companies, civil society organizations, and technical communities. These theoretical perspectives have become essential for understanding the transnational nature of cybersecurity challenges and for improving global governance mechanisms.

The protection of personal data and digital rights has also received considerable attention in contemporary scholarship. Christopher Kuner’s work is particularly significant in this regard. He examines cross-border data flows and international data protection frameworks, highlighting the emergence of new forms of privacy rights within the global digital economy [5]. In addition, the European Union’s General Data Protection Regulation (GDPR) is widely recognized in academic literature as one of the most successful examples of a human rights-based cybersecurity framework [6]. Scholars argue that the GDPR has strengthened individuals’ control over their personal data, enhanced corporate accountability, and improved transparency in the digital environment. At the same time, some researchers suggest that strict data protection requirements may create certain constraints on technological innovation and digital entrepreneurship [7]. This debate reflects the broader challenge of balancing the protection of fundamental rights with the promotion of technological development.

Results and discussion

In recent years, the rapid advancement of artificial intelligence and algorithmic governance has generated new discussions concerning cybersecurity and human rights. Luciano Floridi, through his theory of information ethics, analyzes the implications of artificial intelligence for human rights and emphasizes the importance of transparency, fairness, and accountability in algorithmic decision-making processes [8]. Furthermore, the United Nations Human Rights Council has repeatedly affirmed that the same rights people enjoy offline must also be protected online, urging states to ensure that cybersecurity policies comply with international human rights standards [9]. The contemporary literature therefore suggests that cybersecurity is not merely a technological or military

concern but a complex socio-legal phenomenon closely connected with human rights protection, democratic governance, and digital justice. Consequently, current academic research increasingly focuses on developing institutional and normative mechanisms capable of maintaining an appropriate balance between security imperatives and fundamental freedoms in the digital age [10].

Cybersecurity and Human Rights in the Global Governance System

The transnational nature of cybersecurity challenges necessitates the development of effective global governance mechanisms. The Internet functions as a borderless communication space where cyber threats frequently transcend national jurisdictions and affect multiple countries simultaneously [11], [12]. As a result, international organizations and regional institutions have increasingly focused not only on strengthening cybersecurity but also on establishing normative frameworks for the protection of human rights in cyberspace. Documents adopted by organizations such as the United Nations, the Council of Europe, and the European Union emphasize the importance of safeguarding fundamental human rights in the digital environment [13]. In particular, the European Union's General Data Protection Regulation (GDPR) is widely recognized as one of the most advanced legal instruments for protecting personal data in the digital age. This regulation grants individuals greater control over their personal information and imposes strict obligations on organizations regarding data collection, processing, and storage. At the same time, international experts increasingly support the multi-stakeholder model of Internet governance, which promotes cooperation among governments, private-sector actors, civil society organizations, and academic institutions [14]. Such a collaborative approach is considered essential for addressing the complex and rapidly evolving nature of cyber threats. However, the absence of universally binding cybersecurity norms at the global level has contributed to persistent political and legal differences among states. While some countries prioritize national security and strengthen governmental control over the Internet, others advocate an open Internet model grounded in the protection of human rights and digital freedoms [15], [16]. These contrasting approaches continue to represent a significant challenge to the effectiveness of global cybersecurity governance.

National Approaches and Mechanisms for Ensuring Human Rights

National cybersecurity policies vary considerably according to each country's political system, legal traditions, and national interests. In democratic states, cybersecurity strategies are generally based on principles such as human rights protection, transparency, accountability, and the rule of law. For example, many European countries regard data protection, Internet freedom, and the safeguarding of citizens' digital rights as key priorities of public policy. In contrast, some authoritarian political systems utilize cybersecurity primarily as a tool for state control and information management. In such contexts, increased Internet censorship, expanded digital surveillance systems, and extensive monitoring of online activities are commonly observed [17]. In the case of Uzbekistan, significant institutional and legal reforms have been implemented in recent years alongside broader processes of digital transformation. The government has adopted various legislative and regulatory measures aimed at promoting digital technologies, expanding e-government services, and strengthening mechanisms for personal data protection. Nevertheless, ensuring that cybersecurity policies remain consistent with international human rights standards continues to be an important challenge [18], [19]. The rapid advancement of artificial intelligence technologies has introduced new legal and ethical concerns, including algorithmic discrimination, automated decision-making, and large-scale digital surveillance. These developments raise critical questions regarding transparency, accountability, and the protection of individual freedoms in the digital environment. Therefore, strengthening institutional mechanisms for human rights protection within national cybersecurity frameworks has become an increasingly important priority [20]. Achieving an appropriate balance between national security

objectives and the preservation of fundamental rights is essential for ensuring sustainable digital development and maintaining public trust in emerging technologies.

Conclusion

The analysis demonstrates that cybersecurity and human rights are two interdependent pillars of contemporary digital society. While the increasing complexity of cyber threats compels governments to strengthen security measures and develop more sophisticated cybersecurity frameworks, it is essential that the fundamental principles of human rights are not compromised in the process. Legal mechanisms and standards developed by global governance institutions play a crucial role in protecting human rights within cyberspace and in promoting a balanced approach between security and freedom. At the same time, the effectiveness of national cybersecurity policies largely depends on their compliance with international norms and their ability to guarantee citizens' digital rights, including privacy, freedom of expression, and access to information. Looking ahead, the rapid development of artificial intelligence, quantum technologies, and advanced digital surveillance systems will create new challenges that require innovative legal and regulatory responses. These emerging technologies have the potential to enhance cybersecurity capabilities, but they may also increase risks related to privacy violations, algorithmic bias, and excessive state or corporate surveillance. Therefore, cybersecurity policy should not be limited to a security-centered perspective alone. Instead, it must evolve into a human rights-based framework that places human dignity, the right to privacy, freedom of information, and democratic values at the center of digital governance. Such an approach is essential for ensuring both security and the protection of fundamental freedoms in the increasingly interconnected digital world.

REFERENCES

- [1]. Solove D. J. *Understanding Privacy*. Harvard University Press, 2008.
- [2]. Lyon D. *Surveillance Studies: An Overview*. Polity Press, 2007.
- [3]. DeNardis L. *The Global War for Internet Governance*. Yale University Press, 2014.
- [4]. Mueller M. *Networks and States: The Global Politics of Internet Governance*. MIT Press, 2010.
- [5]. Kuner C. *Transborder Data Flows and Data Privacy Law*. Oxford University Press, 2013.
- [6]. European Union. *General Data Protection Regulation (GDPR)*, 2016.
- [7]. Brown I. *Research Handbook on Governance of the Internet*. Edward Elgar Publishing, 2013.
- [8]. Floridi L. *The Ethics of Information*. Oxford University Press, 2013.
- [9]. United Nations Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. Geneva, 2021.
- [10]. United Nations. *Universal Declaration of Human Rights*. New York, 1948.
- [11]. United Nations. *Universal Declaration of Human Rights*. New York: United Nations, 1948.
- [12]. European Union. *General Data Protection Regulation (GDPR)*. Brussels: European Parliament and Council, 2016.
- [13]. DeNardis L. *The Global War for Internet Governance*. Yale University Press, 2014.
- [14]. Mueller M. *Networks and States: The Global Politics of Internet Governance*. MIT Press, 2010.
- [15]. Floridi L. *The Ethics of Information*. Oxford University Press, 2013.
- [16]. Kuner C. *Transborder Data Flows and Data Privacy Law*. Oxford University Press, 2013.
- [17]. Brown I. *Research Handbook on Governance of the Internet*. Edward Elgar Publishing, 2013.
- [18]. Solove D. *Understanding Privacy*. Harvard University Press, 2008.
- [19]. Lyon D. *Surveillance Studies: An Overview*. Polity Press, 2007.
- [20]. UN Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. Geneva: United Nations, 2021.