Page 3460 - 3470 **DOI:** *https://doij.org/10.10000/IJLMH.117821*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 3

2024

Cybersecurity and Human Rights: Protecting Individual in Connected World

ABHISHEK GUPTA[1] AND ASTHA GUPTA[2]

ABSTRACT

With the invention of cyberspace, the world has become more interconnected, and the convergence of human rights and cybersecurity has emerged as a crucial subject of apprehension. Such exponential growth of digital technologies has presented us with unique prospects for social interaction, commerce, and communication. Irrespective of this fact, cybersecurity introduces new kinds of threats to the privacy, freedom of expression, and other fundamental rights of individuals. In this paper we would investigate the problems and possibilities associated with protecting human rights in the face of expanding cybersecurity risks.

It is considered to be vital that cybersecurity measures continue to advance in order to safeguard organisations and individuals from malicious cyber activities. However, these types of measures frequently involve data collection and surveillance, which may violate fundamental human rights including privacy, freedom of expression, and access to information. And it is believed that achieving a harmonious coexistence between the security of cybersecurity measures and the protection of human rights is an intricate and urgent matter.

The paper will examine the subsequent fundamental questions as follows: To what extent do modern cybersecurity practices affect the privacy and freedom of expression of individuals? What type of ethical considerations arise when surveillance technologies are employed to improve cybersecurity measures? What can be the ways in which human rights can be safeguarded effectively by international frameworks and regulations in this digital age? What are the respective functions of governments, technology corporations, and civil society organisations for ensuring cybersecurity and protecting the rights of individuals? This paper aims to enhance an understanding regarding ways by which one navigates through the intricacies of cybersecurity and human rights in a world that is progressively more interconnected through addressing these questions.

Keywords*: Human Rights, Cybersecurity, privacy, freedom of expression, access to information, surveillance technology, international framework.*

[1] Author is a student at Presidency University, Rajankunte, India.
[2] Author is a student at Presidency University, Rajankunte, India.

 [ISSN 2581-5369]

I. INTRODUCTION

In past few decades, the world has undergone through a significant transformation due to the result of the rapid expansion of cyberspace. The internet and digital technologies have now created a global network of interconnectedness, leading to transformation of social interaction, commerce, and communication[3]. The digital domain has become one of the essential aspects of contemporary life, from conducting international business transactions online to instant messaging with loved ones across continents[4].

Regardless, this interconnectedness is accompanied by a critical caveat: i.e. cybersecurity. The vulnerability to cyberattacks has also increased as our dependence on digital infrastructure increased. Now Individuals, organizations, and even critical national infrastructure are consistently threatened by malicious actors[5]. Robust cybersecurity measures cannot be ignored in order to mitigate these types of danger.

The potential conflict between cybersecurity and fundamental human rights is a very crucial matter. Although it is unquestionably crucial to protect our digital space, certain cybersecurity measures raise concerns regarding freedom of expression and privacy as well. The use of surveillance technologies can have a debilitating effect on free speech and assembly, and the data collection practices employed by governments and corporations can be intrusive[6].

This paper will explore the intricate interconnection between human rights and cybersecurity. As we will examine the opportunities and challenges that are linked to safeguarding human rights in the context of increasing cybersecurity risks. We will endeavor to elucidate a path toward a more balanced approach by way of analyzing the ethical considerations, the role of various stakeholders, and the impact of modern cybersecurity practices.

The following questions will guide our exploration:

To what extent do modern cybersecurity practices affect the privacy and freedom of expression of individuals?

[3] International Telecommunication Union (ITU). (2023). The State of Broadband 2023. https://www.itu.int/pub/S-POL-BROADBAND.28-2023

[4] Manyika, J., Chui, M., Osborne, M., Groves, P., & Dobin, A. (2017). Digital globalization: The new era of global flows. McKinsey Global Institute. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

[5] ENISA. (2023). Threat Landscape Report 2023. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

[6] European Parliament. (2021). Resolution of the European Parliament of 21 January 2021 on the rights and principles of natural persons with regard to the processing of personal data in the context of law enforcement cooperation (COM (2020)0602 – C9-0021/2020 – 2020/0202(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52012SC0072

 [ISSN 2581-5369]

What type of ethical considerations arise when surveillance technologies are employed to improve cybersecurity measures?

What can be the ways in which human rights can be safeguarded effectively by international frameworks and regulations in this digital age?

What are the respective functions of governments, technology corporations, and civil society organizations for ensuring cybersecurity and protecting the rights of individuals?

II. THE INTERSECTION OF CYBERSECURITY AND HUMAN RIGHTS

The activity of safeguarding digital infrastructure, including networks and systems, from malicious attacks is known as cybersecurity.[7] Cybersecurity includes various tools and methods that are used to keep people, systems, data, and important assets safe from cyberattacks, in a very layman language. There are many forms these attacks can take, including from unauthorized entry, data breaches, the release of malware, to denial-of-service attacks and all of these can have very bad results. In this digital age, as information technology has become very important for supporting and maintaining important infrastructure like power grids, banking systems, and communication networks. A successful cyberattack on this kind of equipment could cause a lot of problems, cost a lot of money, and even hurt people[8]. In order to protect these important systems, it is imperative to put in place cybersecurity steps.

That being said, the digital age has also brought about a new era of discussions about human rights. In this way, the idea of human rights includes the basic freedoms that everyone needs to be able to participate in society. These rights include the right to privacy, which protects a person's control over their personal information, the right to freedom of expression, which lets people say what they think and believe without fear of retaliation from the government, and the right to access information, which lets people actively seek and receive information through any means[9].

Putting these basic rights at risk could happen when cybersecurity steps are put in place. Problems often arise when governments and businesses use the same methods to gather information. A lot of personal information, like your browser history, what sites you visit, and even where you are, is collected using these methods. On the one hand, supporters say that collecting this kind of information helps find possible threats and stop cyberattacks. On the

[7] https://builtin.com/cybersecurity
[8] World Economic Forum. (2020). The Global Risks Report 2020. https://www.weforum.org/reports/the-global-risks-report-2020
[9] Office of the High Commissioner for Human Rights (OHCHR). (n.d.). Human Rights.

 [ISSN 2581-5369]

other hand, critics worry that this information could be misused. People may be afraid to share their different opinions because they think the government will be listening[10]. This can make it harder for people to exercise their right to free speech.

Surveillance tools are an important part of cybersecurity, but they can make people worry about their rights. Software that can recognize faces can be used to track and identify people in public places. This technology can help with investigations and preventing crime, but if it is used too much, it could make people feel like they are always being watched, which violates their rights to privacy and freedom of movement[11].

Also, government programs that use a lot of surveillance while pretending to be cybersecurity measures may wrongly target certain groups or populations based on things like race, religion, or political beliefs. This concerns people about discrimination and the violation of the right not to be discriminated against, which is set out in international human rights law[12].

What needs to be done is finding a good balance between strong cybersecurity means and protecting basic human rights. There needs to be a set of cybersecurity rules that protects people's privacy, freedom of speech, and access to information while also effectively stopping and preventing cyberattacks. To find this sensitive balance, you need a complex plan that includes being open, taking responsibility, and having strong legal systems.

III. MODERN CYBERSECURITY PRACTICES AND THEIR IMPACT ON HUMAN RIGHTS

Many procedures that, although having good intentions, can generate serious human rights issues have been implemented in the quest of complete cybersecurity. Two important areas of concern are the extensive use of data collecting and the increasing reliance on surveillance technologies.

(A) Data Collection Practices: Intrusive and Vulnerable

Governments and businesses alike use sophisticated data collecting techniques, often accumulating large amounts of personal data on people. Apart from the financial information, this data could include location data, social media interactions, browsing history, and online activity. Data mining, according to proponents of these techniques, makes it possible to identify potential dangers and provide focused security features. Still, the huge amount of data collected

[10] Snowden, E. (2019). Permanent Record.
[11] Amnesty International. (2020). Facial recognition technology: A threat to human rights.
[12] United Nations Human Rights Office of the High Commissioner. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

makes one wonder about the possibility of abuse and invasion.

The reason data collecting is so invasive is that people usually have little control over the information that is gathered about them or how it is used. Many online services require consumers to agree to broad and ambiguous data collecting rules in order to utilize them. Users are further concerned since data storage procedures and possible sharing with third parties are not transparent.

Misuse of data is a major further worry. Regretfully, data breaches are much too often and can lead to the exposure of private information, which can cost people money, steal their identities, and damage their reputation. The information that is gathered can be used for non-cybersecurity related reasons such political profiling, targeted advertising, or even societal control[13].

(B) Surveillance Technologies: A Chilling Effect on Freedom

More and more, cybersecurity applications are using huge data collecting, internet monitoring, and facial recognition technologies. With the help of these technologies, one can keep an eye on online activity, spot any risks, and follow people about. Still, the individual liberties they safeguard are given up for their widespread use.

Without their knowledge or permission, face recognition technology, for instance, can be used to identify and track people in public spaces. This presents questions on the freedom of movement and right to privacy. Facial recognition has supporters who argue that it can help prevent crime; detractors point out that it has the potential for widespread monitoring and the creation of a "panopticon effect"—the impression that one is always being watched—which can stifle criticism and limit free speech[14].

Programs for monitoring internet communication and activities can potentially stifle freedom of expression. Many people could be reluctant to voice opposing opinions or participate in internet activism out of concern of government surveillance or reprisals. Critical conversation can be stifled and the free flow of knowledge, which is essential to a functioning democracy, hampered by this[15].

(C) Real-World Examples: The Human Cost

The negative consequences of these activities on human rights are demonstrated by several instances from actual life. 2013 saw the disclosure by Edward Snowden of the whole PRISM

[13] Electronic Frontier Foundation. (2023). How We Fight for Your Privacy Online. https://www.eff.org/issues/privacy
[14] Supra Note 11
[15] Access Now. (2023). Defend Your Right to Free Speech Online.

 [ISSN 2581-5369]

bulk surveillance program of the US government. An aspect of this project was the gathering of vast user data from large internet companies, which raised concerns about the possible infringement of millions of people's right to privacy worldwide[16].

One other example is China's widespread use of facial recognition technology. The facial recognition software-equipped surveillance cameras that the Chinese government has installed form a vast network. With the use of this technology, citizens' behavior, their movements, and even possible dissidents are tracked down. This presents serious questions on the freedom of assembly and privacy[17].

These instances highlight the way that modern cybersecurity procedures may violate basic human rights. A balance between security and individual freedoms requires a more sophisticated approach to data collecting and surveillance technologies.

IV. ETHICAL CONSIDERATIONS IN CYBERSECURITY

Ensuring online safety without compromising privacy is a multifaceted challenge in the digital era. Although surveillance tools such as facial recognition provide security advantages, they also raise ethical concerns regarding the equilibrium between individual freedoms and security.

The fundamental quandary is the trade-off between security and privacy. The collection of vast amounts of personal data by tools that improve cybersecurity often intrudes into the private affairs of individuals. This is in direct opposition to the right to privacy, which is a fundamental component of a free society. It is imperative to strike the appropriate equilibrium; cybersecurity should not be sacrificed for mass surveillance. A more ethical solution is provided by a targeted approach that concentrates on the collection of only the data that is required for specific threats.

It is imperative to prioritize accountability and transparency. Individuals are entitled to be informed about the data that is collected, its use, and its recipients. In order to establish trust, it is imperative to establish clear data collection policies and robust oversight mechanisms. The significance of transparency is exemplified by the 2017 Puttaswamy judgment in India, which acknowledged the right to privacy as a fundamental right.[18]

Ethical practices can be guided by fundamental principles in order to navigate these complexities:

[16] Greenwald, L. (2013). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.
[17] Human Rights Watch. (2023). China: Mass Surveillance Threatens Basic Rights. https://www.hrw.org/world-report/2023/country-chapters/china
[18] Supreme Court of India. (2017). K.S. Puttaswamy (W) and Ors. v. Union Of India and Ors. [Writ Petition (Civil) No. 494 of 2012].

- Reduce the amount of data collected: Only gather the data that is absolutely essential for the specific threats.
- Maintaining informed consent necessitates transparency regarding the data collected, its utilization, and its distribution. Whenever feasible, obtain informed consent.
- Use surveillance tools responsibly: Only employ them when they are unquestionably necessary and under the supervision of a qualified individual.
- User discretion and data security: Enable individuals to exercise some degree of control over their data, such as the ability to access, rectify, or eliminate it within reasonable limits, and establish robust data security measures.
- Consistent review and auditing: Conduct regular reviews and audits of cybersecurity practices to guarantee their efficacy and compliance with ethical standards.

V. LEGAL AND REGULATORY FRAMEWORKS FOR PROTECTING HUMAN RIGHTS

The preservation of human rights is a multidimensional concern in the digital age. Despite the presence of international and national regulatory frameworks, they usually fail to keep up with the rapid progress of technology and cybersecurity practices. This part investigates the significance of these frameworks in preserving human rights and assesses their limits, which point to the necessity for more specific rules.

(A) Instruments for International Human Rights

International human rights instruments are critical for laying the groundwork for the protection of human rights in the digital domain. There are two major instruments:

The Universal Declaration of Human Rights (UDHR): The Universal Declaration of Human Rights (UDHR), adopted in 1948, protects a wide range of fundamental rights, including the right to privacy (Article 12) and freedom of expression (Article 19). The UDHR does not directly address the digital age; however, its core principles might be understood to encompass online actions[19].

The International Covenant on Civil and Political Rights (ICCPR): The ICCPR (1966) expands on civil and political rights, expanding on the Universal Declaration of Human Rights. Article 17 of the ICCPR protects the right to privacy, highlighting the need of preventing unauthorized interference with one's privacy. In the same line, Article 19 ensures the right to

[19]United Nations General Assembly. (1948). Universal Declaration of Human Rights. https://www.un.org/en/documents/udhr/

 [ISSN 2581-5369]

free expression, which includes the ability to seek, receive, and publish information and ideas[20].

(B) Constraints of International Framework

Despite their importance, international human rights instruments are limited in scope. These instruments usually lack clear guidance on how to use them in the context of changing technologies, and they are often broad in reach. Furthermore, enforcement measures are ineffective, with a strong focus on intergovernmental discourse and state reporting.

This lack of definition has made it difficult to interpret and enforce these rights in the digital era. For example, the UDHR's definition of "privacy" may not fully account for the substantial data collection activities that governments and corporations already employ. Similarly, it can be difficult to reconcile the right to free expression with restrictions in place to fight online hate speech or cybercrime.

In response to these limits, national and regional legislation have been developed to provide more specific guidance on human rights and cybersecurity.

a. India:

The Information Technology Act of 2000 (IT Act) aims to regulate cybercrime and boost e-commerce in India. It includes rules on data protection and privacy (Section 43A), however it has been criticized for being insufficiently thorough and out of date in light of contemporary concerns[21].

Digital Personal Data Protection Act 2023[22]: The proposed legislation aims to create a comprehensive framework for data protection in India. It defines the principles of data reduction, user consent, and data security measures. Although this is a welcome development, the efficacy of this Bill will be determined by its final shape and implementation.

Indian Constitution: The Indian Constitution also protects human rights in the digital era. The Supreme Court of India recognized the right to privacy as a basic right in the historic Puttaswamy decision (2017). This ruling has significant consequences for India's cybersecurity and data protection standards[23].

(C) Effectiveness of these Regulations:

There is a continuing debate about the effectiveness of national and regional rules in preserving

[20] United Nations Office of the High Commissioner for Human Rights. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[21] Information Technology Act, 2000. (Act 21 of 2000), s. 43A
[22] Digital Personal Data Protection Act, (Act 22 of 2023)
[23] Supra Note 18

human rights. Although many rules, such as the proposed Indian Data Protection Bill (now an Act), constitute a positive step toward protecting user privacy, their enforcement and implementation remain critical. Furthermore, the transnational aspect of the internet frequently complicates the regulation of online activity across national borders, as national rules frequently face this difficulty.

VI. ROLES AND RESPONSIBILITIES OF KEY STAKEHOLDERS

Human rights and cybersecurity interact in a way that requires a multi-stakeholder approach. Promotion of a safe and human rights-respecting digital environment requires the cooperation of governments, technology companies, and civil society groups.

Governments: Human rights protections must be included into thorough cybersecurity policy in order to achieve balance. Through public consultations, clear legislative foundations for monitoring and data collecting procedures must be established. Confidence is developed via independent monitoring along with openness about cybersecurity techniques and technologies. Global defences are strengthened and data protection is harmonised by international cooperation. Operating as a model is the European Union's General Data Protection Regulation (GDPR)[24].

Technology companies that follow ethical cybersecurity procedures provide customer privacy and data reduction through strong encryption top priority. Clear data collecting guidelines must be established, and users must be able to control their personal data. Trust must be built by openness about cybersecurity procedures and privacy issues. Apple is a prime example of this commitment to user privacy[25].

Civil society organizations, or CSOs, empower people by raising public knowledge of online dangers, risks to data privacy, and self-defense strategies. Human rights-focused legislation is supported by advocates of strong data protection laws and limitations on government surveillance. Civil society groups (CSOs) may also be of use to those who are being violated of their digital rights. Electronic Frontier Foundation (EFF) is one excellent example[26].

Working collaboratively, all parties involved is essential. Recognizing and working together, they may create a safe and rights-respecting internet. By giving ethical behavior, support of human rights, and thorough data protection first priority, we can make the most of technology's

[24] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). eur-lex.europa.eu
[25] Apple. (n.d). Privacy Policy. https://www.apple.com/legal/privacy/
[26] Electronic Frontier Foundation. (n.d.). About EFF.

possibilities.

VII. STRATEGIES FOR HARMONIZING CYBERSECURITY AND HUMAN RIGHTS

A multidimensional strategy is necessary to ensure the coexistence of effective cybersecurity and the protection of human rights. Technological advancements and legislative modifications can be combined to establish a digital environment that is more secure and respectful of rights.

Technological Solutions:

- Encryption Technologies: Scrambled data, unreadable without a key, protects user information even in breaches.
- Privacy-Enhancing Technologies (PETs): Tools like anonymization and statistical noise injection empower users to control their online data and participate privately. (e.g., anonymized browsing)[27]
- Secure Software Development: Building secure software from the start with regular vulnerability checks and patching minimizes exploitable weaknesses.

Modifications to the Policy:

- Global Challenges, Global Solutions: Cybersecurity threats and data breaches often disregard borders. Strengthening international cooperation on data protection standards, cybercrime investigations, and information sharing is crucial. This fosters a more secure digital space while upholding human rights globally.
- Empowering Users: Equipping individuals with digital literacy skills is key. Educational programs can teach users about online threats, data privacy practices, and secure online navigation. This empowers individuals to protect their rights and make informed choices online.

A comprehensive approach is necessary to ensure that human rights and cybersecurity coexist. In conjunction with legislative enhancements such as robust data protection legislation and international collaboration, we can leverage technological advancements such as encryption and PETs to establish a digital environment that prioritizes human rights and ensures security. Additionally, the promotion of digital literacy education empowers individuals to actively engage in the safeguarding of their online rights. By implementing such initiatives, we can ensure that cyberspace continues to evolve and innovate, while simultaneously preserving the fundamental liberties that underpin a democratic society.

[27] Future of Privacy Forum. (2023). Privacy-Enhancing Technologies (PETs).

VIII. Conclusion

Striking a balance between cybersecurity and human rights necessitates effort. In order to implement robust security measures, user privacy and liberties should not be compromised. Ethical concerns, responsible technological advancements, and robust legal frameworks are of paramount importance. Encryption, privacy-enhancing tools, and digital literacy can empower users. Corporations, governments, and civil society all have a role to perform. Data reduction and transparency must be prioritized by governments. It is imperative that digital enterprises prioritize user privacy and data protection. CSOs should be advocates for surveillance restrictions and comprehensive data protection legislation. Ultimately, a digital future that is both secure and respectful of rights necessitates the collaboration of all parties to ensure a safe and unrestricted cyberspace.

*****

 [ISSN 2581-5369]