International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Protecting Human Rights in the Digital Age: The Menace of Cyber Crimes

Dr Rupali Bhouradia[1], Richa Tyagi[2]

[1]Associate Professor, Department of Political Science & Public Administration, Banasthali Vidyapith, Rajasthan.
[2]Research Scholar , Department of Political Science & Public Administration, Banasthali Vidyapith, Rajasthan.

Abstract
As digitalization accelerates, it transforms the landscape of human rights, presenting significant opportunities and serious challenges. Digital technologies have facilitated unprecedented access to information, communication, and economic growth. However, they have also introduced new threats to fundamental human rights, notably through cyber-crimes. Privacy breaches, online surveillance, misinformation dissemination, and cyber-crimes pose complex ethical dilemmas requiring careful consideration and action. Protecting human rights must remain a priority in this digital transformation. Ethical and responsible digitalization should ensure that technology enhances collective well-being and upholds the principles of equality, justice, and dignity for all. This paper explores the potential of digital technologies while emphasizing the crucial importance of digital rights in safeguarding human rights. The study addresses significant challenges posed by cyber offenses, including privacy violations, restrictions on freedom of expression, access to information, and threats to critical infrastructure. It highlights the urgent need for comprehensive digital rights frameworks to protect individuals from these emerging threats. The paper analyzes these issues using secondary data collection methods and offers insights into developing effective strategies to combat cyber- crimes in the digital age.

Keywords: Digital Technologies, ICT, Cybercrime, Human Rights, UDHR, Privacy, Security, Digitalization.

INTRODUCTION

In the contemporary world, digital technologies overpower every interaction domain in human life. In the fast-changing technological world, the relationship between digitalization and human rights has become a significant topic of discussion and study for scholars. As digital technologies become more integrated into daily life, they have the potential to both support and pose challenges to fundamental human rights. The dual aspect of digitalization represents exploring new opportunities to advance the limitations of human rights in the digital landscape on one side and another it poses serious challenges and threats to the very

[1] Dr Rupali Bhouradia, Associate Professor, Department of Political Science & Public Administration, Banasthali Vidyapith, Rajasthan.
[2] Richa Tyagi , Research Scholar , Department of Political Science & Public Administration, Banasthali Vidyapith, Rajasthan.

fabric of human rights by compromising privacy, security, and individual freedom through the enactment of cybercrimes.

The availability of information has been opened up by digital technologies, allowing people to connect, communicate, and work together regardless of their location or culture. The internet and social media platforms have become influential tools for amplifying voices, creating awareness around social issues, and mobilizing efforts for change. For example, digital campaigns have been essential in progressing women's rights, environmental conservation, and political openness. Furthermore, digital technologies have contributed to economic expansion by opening up new markets and employment opportunities. Small businesses can reach global audiences through e-commerce platforms, and remote work technologies allow individuals to work from anywhere, leading to greater workforce flexibility and inclusivity. The availability of online education has broadened learning opportunities, giving individuals the skills, they need to improve their lives. In terms of governance, digital technologies can potentially improve transparency and accountability. E-government initiatives streamline public service provision and reduce corruption, building trust between citizens and authorities. Open data initiatives allow citizens to access information about government activities, encouraging informed civic engagement and advocacy.

With the proliferation of sophisticated tools of information and communication technologies, a new breed of offenses has taken the digital diaspora commonly known as cyber-crimes, and the expansion of digital platforms has further accelerated the rate at which these crimes are occurring. One of the most urgent concerns is the erosion of privacy, as personal data collection and surveillance activities become more widespread. Misinformation and disinformation spread through digital platforms can have far-reaching negative effects, including undermining public trust, deepening social divisions, and inciting violence. In addition, cybercrimes such as hacking and cyberbullying violate individuals' right to security and can cause significant harm. The digital divide further compounds existing inequalities, restricting access to education, jobs, and civic engagement for marginalized communities. It's critical to address these challenges to ensure that all members of society can reap the benefits of technological advancements.

In such a vulnerable environment, it becomes a prime responsibility of not only government organizations but also private individuals to empower themselves with not only the knowledge of benefits withdrawn from digitalization but also to safeguard their intrinsic value of individual security and privacy against the cyber predators and equip themselves with an understanding of their so-called “Digital rights.”

CONCEPTUAL FRAMEWORK OF CYBER-CRIMES & HUMAN RIGHTS

Cybercrimes refer to unlawful activities executed through computers or the internet. Any criminal act within the digital realm, or cyberspace, is classified as a cybercrime. The term "cyberspace," coined by William Gibson in 1984, describes the digital environment where communication over computer networks occurs. This virtual space is dynamic and populated by digital replicas of machines, allowing users to share information, interact, and participate in social media and other online activities.

Dr. Halder and Dr. Jaishankar defined cybercrimes as “*offenses committed against individuals or groups with the criminal intent to harm the victim's reputation or to inflict physical, mental, or financial harm. These crimes are carried out using modern telecommunication networks such as the internet (through*

chat rooms, emails, message boards, and groups) and mobile phones (via SMS/MMS).”[3] (Halder & Jaishnakar, 2016)

Initially, cybercrimes were perceived as unconventional offenses. However, as these crimes have evolved and proliferated, they have acquired all the characteristics of conventional crimes, with the notable exception of a physical act. The element of anonymity in cybercrimes adds to their complexity and danger. Cybercrimes can be categorized based on their nature, target group, or the networking systems involved. However, they are primarily divided into two categories: cyber-dependent crimes and cyber-enabled crimes.

Cyber-dependent crimes can only be perpetrated using information and communications technology (ICT) devices, including hacking, malware distribution, and denial-of-service (DoS) attacks. Cyber-enabled crimes are traditional crimes significantly facilitated by the internet or digital devices, such as fraud, identity theft, and online harassment

The motives for committing cybercrimes vary, ranging from financial gain to political activism (hacktivism), personal vendettas, or the desire to cause disruption or damage. The perpetrators may include individual hackers, organized crime groups, nation-states, and insider threats. As digital technology has advanced, so too have the methods used to commit these crimes. Common techniques now include phishing, malware distribution, and ransomware attacks. Additionally, more sophisticated tools and techniques have emerged, such as social engineering, exploitation of software vulnerabilities, and advanced persistent threats (APTs).

Human rights are not negotiable. They are fundamental principles that guarantee every individual’s dignity, freedom, and equality, regardless of nationality, ethnicity, religion, gender or any personal attributes. These universal, inherent, and interconnected rights serve as the basis for freedom, justice, and peace worldwide.

The concept of Human Rights has deep historical and religious roots. Early ideas about rights and justice emerged from ancient civilization and spiritual teachings emphasizing the individual’s inherent dignity and value. During the Enlightenment period, philosophers like John Locke introduced the notion of natural rights, advocating for life, liberty, and property, which heavily influenced vital historical documents such as the “American Declaration of Independence 1776”[4] (Historian) and “1789, and “The French Declaration of the Rights of Man and Citizens”[5] (Robinson, 1889). Embracing the Universal Declaration of Human Rights by the UN General Assembly in 1948 became a landmark event in world history. The fundamental document outlines fundamental rights and freedoms for all individuals furbished in 30 articles. This declaration acted as an umbrella term for all the civil, political, economic, and cultural rights where all the rights are equally essential for human dignity.

The International human rights framework is not just limited to UDHR. Some numerous international treaties and covenants have been derived from it, like the “International Covenant on Civil & Political

[3] Halder, D., & Jaishankar, K. (2016). *Cyber Crimes Against Women In India.* New Delhi: Sage Publictaion.

[4] Historian, O. o. (n.d.). *https://history.state.gov/milestones/1776-1783/declaration#:~:text=*. Retrieved from Department of State, United States of America. (Accessed on 24th May 2024)

[5] Robinson, J. H. (1889, Dec). The French Decleration of the Rights of Man, 1789. *Political Science Quaterly, 14*(4), 653-662.

Rights"[6] (UDHR, 1966) and "International Covenant on Economic, Social & Cultural Rights"[7] (OHCHR, 1966) both adopted in 1966. These agreements are supported by various UN bodies, regional organizations, and non-governmental organizations that monitor and promote adherence to human rights standards. Despite the efforts of these entities, enforcing human rights remains challenging, necessitating continued global cooperation and advocacy to ensure that these fundamental principles are upheld for all individuals.

THREATS & CHALLENGES TO HUMAN RIGHTS BY CYBER CRIMES

The rapid growth of technology and the internet has created new opportunities for cybercriminals to infringe upon individuals' rights, leading to various challenges in safeguarding these rights in the digital realm. Some of prominent challenges faced are the discussed below.

1. Violation of Privacy Rights

- **Data Breaches**

The consequences of data breaches cannot be overstated. Unauthorized acces to personal and sensitive information can have devastating effects, including identity theft and financial fraud, causing significant harm to individuals. In 2018, a massive breach of India's Aadhaar database exposed vulnerabilities, leading to reports that the personal information of over a billion citizens, including names and addresses, was being sold online. This incident raised gave concerns about privacy and data concern. Similarly, in 2020, Haldirams's a well-known Indian snack company, fell victim to a data breach that resulted in cybercriminals gaining access to sensitive employee and financial information. This event underscored the escalating threat to cybercrimes to businesses and its potential impact on individual privacy and financial security.

- **Surveillance and Monitoring**

Government and corporate surveillance programs often lack sufficient oversight, posing significant threats to individual privacy by enabling the unauthorized collection and monitoring of personal data. The 2019 Pegasus spyware[8] (Josh, 2022)scandal exemplified these concerns when it was revealed that journalists, activists, and politicians In India are targeted by sophisticated spyware developed by Israeli company NSO group. The spyware could intercept communications, access files, and activate cameras and microphones on devices, sparking widespread concern over government surveillance and the potential abuse of such technologies. Similarly, the 2013 Call Data Records[9] (Sikdar, 2013)scam highlighted issues of privacy violations in India, where private detectives and police officials illegally acquired and sold CDRs without proper authorization, raising concerns about misuse of surveillance capabilities.

---

[6] UDHR. (1966, December 16). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[7] OHCHR. (1966, December 16). *International Covenant on Economic, Social and Cultural Rights.* Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

[8] Josh, J. (2022, August 25). Retrieved from jagranjosh.com/general-knowledge/explained-what-is-the-pegasus-case-in-india-know-about-the-pegasus-project-revelations-and-the-history-1661446834-1(Accesed on 25th May 2024)

[9] Sikdar, S. (2013, November 15). *Three policemen among 6 held for obtaining call records illegally*. Retrieved from https://www.thehindu.com/news/cities/Delhi Accesed on 25th May 2024)

2. Threats to Freedom of Expression

- **Censorship and Control**

Freedom of expression is increasingly under threat from cybercrime, as malicious actors target activists, journalist, and dissenting voices . They employ tactics such as hacking, phishing, and other cyber-attacks to silence or intimidate individuals and organizations advocating for various causes.

- **Misinformation and Disinformation**

The proliferation of false information online, often orchestrated cybercriminals, poses a significant threat to freedom of expression. This deliberate dissemination of misleading information can manipulate public opinion, limit access to accurate information, and subvert democratic process, eroding the foundation of open and free discourse.

3. Economic Exploitation and Inequality

Cybercriminals engage in a range of deceptive activities, such as fraud lent online schemes, unauthorized use of credit card information, and ransomware attacks. These criminal acts tend to have a more profound impact on vulnerable populations, further exacerbating economic disparities. Additionally, unequal access to digital technologies and cybersecurity resources places marginalized groups at a higher risk of falling victim to cybercrime , ultimately widening the existing inequality gap.

4. Security and Personal Safety Concerns

- **Cyberstalking & Harassment**

Cyberstalking involves using the internet or electronic means to stalk or harass individuals, groups, or organizations, leading to repeated and unwanted attention or contact with the intent to intimate and instill fear. Forms of cyber harassment include doxing, which is the non-consensual public exposure of personal information, and cyberbullying, where digital communication tools are used to intimidate or threaten individuals. These activities can cause severe psychological distress, such as anxiety, depression, and PTSD, particularly impacting women, children, and minority groups, who are inappropriately targeted. Legal frameworks often fall short in addressing cyberstalking, presenting challenges for victims in obtaining Justice and protection.

- **Threat to Critical Infrastructure**

Critical infrastructure comprises essential systems and assets, including power grids, water supply, transportation systems, communication networks, and healthcare facilities, that are crucial for society and the economy. Cyberattacks pose significant threats to these infrastructures by attempting to disrupt, damage, or gain unauthorized access to computer systems, networks, or devices. Such attacks can severely impact public safety and national security, leading to chaos, economic loss, and even loss of life. For instance, cyberattacks on healthcare systems, like the 2017 WannaCry ransomware attack on the UK's National Health Service (NHS), can jeopardize patient safety and compromise sensitive data. Transportation systems are also vulnerable, as demonstrated by the 2020 ransomware attack on a U.S. natural gas pipeline, which highlighted vulnerabilities in energy infrastructure. To mitigate these threats, robust cybersecurity measures, including firewalls, intrusion detection systems, and encryption, are essential to protect critical infrastructure from cyber threats.

5. Challenges to Access to Justice

- **Jurisdictional Issues**

Jurisdictional issues in cybercrime stem from its cross-border nature, where crimes often span multiple countries, complicating the determination of applicable laws. Perpetrators can easily commit crimes in

one country while residing in another, leveraging the internet's global reach. This transnational aspect poses significant challenges for law enforcement, as coordinating investigations and prosecutions across jurisdictions requires substantial international cooperation. Differences often hinder such cooperation in legal systems, priorities, and resources. Additionally, holding perpetrators accountable is difficult due to the need for evidence admissible in various legal contexts and potential jurisdictional disputes over prosecutorial authority. These complexities can lead to delays or failures in justice, obstructing victims' access to legal redress.

- **Lack of Legal Protection**

The lack of legal protections against cybercrime arises from several key issues. Many regions need more legal frameworks that fail to comprehensively address cybercrime, with existing laws often not covering the complexities and technicalities of these offenses. This leaves significant gaps in legal protections for victims. Additionally, the sophisticated technology and techniques used in cybercrimes present challenges that traditional legal systems are not equipped to handle, making it difficult to define and prove offenses and to identify and capture digital evidence. As a result, victims of cybercrime frequently have limited legal options due to the absence of specific laws targeting these offenses, leaving them vulnerable and without sufficient protection or means to seek compensation for the damages they suffer.

THE NEED FOR DIGITAL RIGHTS IN HUMAN RIGHTS FRAMEWORK TO COMBAT CYBER CRIMES

In this fast-paced era of digitization, there is an urgent need to redefine human rights in the context of the digital age. The pervasive influence of digital technologies has revolutionized communication, information access, and the exercise of fundamental freedoms. Integrating digital rights into the overarching framework of human rights is imperative to shield individuals from the unique opportunities and threats posed by digital progress.

Digital rights are fundamental human rights that empower individuals to utilize, create, and share digital content, as well as access and use electronic devices and communication networks. These rights are crucial for ensuring equal participation in the digital realm. They encompass various rights such as the right to privacy, freedom of expression, access to information, the right to be forgotten, and digital literacy.

The integration of digital rights to human rights frameworks is crucial in several reasons . Digital technologies have become essential for exercising fundamental rights, including freedom of speech assembly, and access to information. Without digital rights, these freedoms are at risk of being violated in the digital realm. Furthermore, the increasing prevalence of data breaches, cyber-attacks, and online surveillance emphasizes the importance of protecting individual’s privacy and online security. Digital rights serve as defense against these threats, ensuring that individuals retain control over their personal information and digital identities. Additionally, the digital divide continues to widen social and economic disparities. By integrating digital rights into human rights frameworks, we cannot only promote digital inclusions but also ensure responsible and accountable utilization of digital technologies.

The GOI (Government of India) has made significant progress in acknowledging digital rights within its legal framework “The Information and Technology Act of 2000”[10] (IT Act, n.d.) provides legal recognition for electronic transaction and addresses issues related to cybersecurity and data protection. However, critics argue that the act needs to be updated to better reflect the complexities of the digital age.

[10] *IT Act*. (n.d.). Retrieved from https://www.meity.gov.in/content/information-technology-act-2000-0

The "Personal Data Protection Bill 2019"[11] (htt2) , "The Data Privacy and Protection Bill 2019"[12] (htt3), & "The Digital Personal Data Protection Bill,2022"[13] (htt5) aims to enhance data protection and privacy rights for Indian citizens. They propose stringent regulations on data collection and processing, giving individuals greater control over their personal data. In a landmark case, **Puttaswamy v. Union of India**[14] (Justice K.S Puttaswamy Versus Union of India, 2018)**,** the Supreme Court of India recognized the right to privacy as a fundamental right under the constitution, establishing a precedent for safeguarding digital privacy.

Several international frameworks and initiatives address digital rights globally. The General Data Protection Regulation of the European Union is one of the most comprehensive data protection laws, providing individuals with strong privacy rights and imposing significant obligations on organizations that personal data. While International organizations like United Nations and Council of Europe have become very critical about development more robust and comprehensive legal frameworks to secure digital rights and expand its horizons to combat cyber crimes

SUGGESTIONS & CONCLUSION

The threats from cybercrimes are multifaceted thus it requires a comprehensive mechanism to safeguard and protection of human rights in this digital age. The following are some suggestions which can be implemented in for further enhancing the meet the challenge of cybercrimes posed to human right:

Strengthen Legal Frameworks: it's important to update laws and regulations to combat cybercrimes while protecting human rights. This includes incorporating principles for privacy and freedom of expression and implementing comprehensive data protection regulations like the EU's GDPR. Clear jurisdictional rules are also essential for defining jurisdiction in cross-border cybercrime cases and ensuring effective legal enforcement.

Enhance Cybersecurity Mechanisms: To bolster cybersecurity, it is essential to deploy state-of-the-art security technologies like encryption, multi-factor authentication, and intrusion detection systems. These technologies are not just tools, but shields that protect sensitive data and systems. Consistent security assessments and software upgrades are vital to identify and rectify weaknesses and fortify defenses against cyber threats. Additionally, creating comprehensive cyber incident response strategies can mitigate harm and expedite recovery in a cyber incident.

Foster International Cooperation: Enhance global cybersecurity through international partnerships to exchange threat intelligence, best practices, and resources. Furthermore, we should advocate for developing international treaties and agreements to boost cooperation in fighting cybercrime and enabling mutual legal assistance.

[11] *GOI*. (n.d.). Retrieved from https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

[12]https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

[13]https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

[14] Justice K.S Puttaswamy Versus Union of India, AIRONLINE 2018 SC 237 (Supreme Court of India September 26, 2018).

Promote Digital Literacy and Awareness: Promotes digital literacy and awareness through education campaigns, integrating cybersecurity training into school curricula, and offering resources for vulnerable populations to understand and mitigate cyber risks.

Encourage Ethical Technology Development: It means advocating for a "privacy by design" approach in companies, so privacy and security are considered from the beginning of designing products and services. It is also important to create ethical guidelines for AI and automated systems to prevent misuse and respect human rights. Additionally, supporting the development and use of open-source security tools that the community can review is essential for improving cybersecurity practices.

Establishing Clear Reporting and Redress Mechanisms: The key points to remember are the need to create user-friendly platforms for reporting cybercrimes and seeking help, establishing support systems for victims that offer counseling, legal aid, and financial assistance, and ensuring transparency and oversight in government surveillance activities to prevent misuse of power.

Advocate for Human Rights in Digital Policy: Advocating for human rights in digital policy development and implementation, ensuring that measures against cybercrime do not violate fundamental rights. Engaging with civil society, academia, and industry stakeholders to gather diverse perspectives and promote balanced policymaking.

The rapid growth of digital technologies brings opportunities for innovation and significant threats to human rights through cybercrimes. Privacy breaches, identity theft, and online harassment undermine fundamental rights. Integrating digital rights into the broader human rights framework and strengthening data protection laws are essential steps to mitigate the impact of cybercrimes. Safeguarding human rights in the digital age requires a united effort to ensure digital technologies' responsible and ethical use, creating a safer and fairer digital environment for all.

References

1. Ahuja, V. (2019). *Human Rights: Contemperory Issues.* EBC Publishers.
2. Mishra, A. (2021). *Cyber Crime and Procedural Laws:in Human Rights.* New Delhi: VL Media Solutions.
3. Mishra, A. K. (2020). *An Overview on Cybercrime & Security Volume - I.* Delhi: Notion Press.
4. Sen, G. (2022). *Cyber Security & cyberspace in International Relations.* Delhi: VIJ Publishers.
5. Sirohi, M. (2015). *Transformational dimensions of Cyber Crime.* Alpha Editions.
6. Aggarwal, S. (2001). *Training on Cyber law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements.* New Delhi: CBI Bulletien.
7. Amarnatham, L. (1999). *Cyber Crimes- Prevention and Control Startegies.* Delhi: CBI Bulletien.
8. Chen, Y. (2023). Jurisdictional challenges in combating cyber-crimes. *International Journal of Law and Technology*, 18(4), 567-589
9. Davis, R. (2019). Online harassment and its impact on freedom of expression. *Digital Rights Review*, 10(2), 89-105
10. Johnson, M., & Miller, S. (2021). Privacy in the digital age: The new battleground. *Privacy and Data Protection Journal*, 9(4), 34-56.
11. Malik, J., & Chaudhary, S. (2019, 3). Cyber Space - Evolution and Growth. *Journal of Education, Humanities and Literature, 2*(3), 170-190.

12. Malik, J., & Choudhary, S. (2018). Policy Considerations In India Against Cyber Crime. *International Journal of Recent Scientific reserach*, *9*(12), 29811-29814.
13. https://www.un.org/en/about-us/universal-declaration-of-human-rights