Research Article

Trinity Law Review

Year 2024, Volume-4, Issue-1 (January-June)

DOI: 10.48165/tlr.2024.4.1.5

ISSN 2583-3588 **(Online)**

Digital Dilemma : Human Rights in the Era of Cyber Crimes

Rupali Bhouradia[1] and Richa Tyagi[2]

ARTICLE INFO

Key words: *Human Rights, UNCHR, Cyber-crimes, Government of India, Digitalization, ICT.*

ABSTRACT

The rapid pace of digitalization is reshaping the landscape of human rights, presenting both opportunities and challenges. While digital technologies have facilitated unprecedented access to information, communication, and economic opportunities, they have also introduced new risks to fundamental human rights. From privacy infringements and online surveillance to the spread of disinformation and cybercrimes, the digital era presents a complex ethical dilemma that requires careful consideration. At its core, human rights remain paramount in navigating this digital information. The present paper shall explore the potential of digital technologies; it is imperative to prioritize human rights as the cornerstone of ethical and responsible digitalization efforts, ensuring that technology serves humanity's collective well-being and advances the principle of equality, justice, and dignity for all. It shall highlight the major challenges posed to human rights by cyber offenses such as privacy violations, freedom of expression, access to information, threat to critical infrastructure, etc. The secondary method is employed by the scholar for the collection of data.[4]

Introduction

Human rights concept and development represents as the testament to humanity's collective aspiration for dignity, equality and justice. From ancient philosophical traditions to contemporary international frameworks, the evolution of human rights reflects the ongoing struggle to uphold every individual's inherent worth and rights. The conceptual framework and definition of human rights is dynamic in nature. An important element determining the definition and conceptual framework of human rights are the dynamic environment of the international politics and how the course of international law is evolving. Though there are various definitions which are provided for human rights in the contemporary times. The United Nations defines " human rights are those rights which are inherent in our state of nature and without which cannot live as human beings."[3] (Mishra, 2004). As we continue to confront new challenges and inequalities in an ever-changing world, human rights principles remain indispensable

[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.

[3]Mishra, Pramod Kumar. *Human Rights :Global issues*. New Delhi: Kalpaz Publication, 2004.

*Corresponding author.
E-mail address: richa12789@gmail.com (Richa Tyagi)
Received 03-05-2023; Accepted 04-07-2023

guides for promoting peace, justice, and solidarity among all peoples.

However, in the swiftly changing landscape of the digital era, technological progress has fundamentally altered our modes of communication, work and engagement with the world. The broad accessibility of internet connectivity, cloud computing, and mobile devices has created unparalleled opportunities for worldwide connectivity, innovation, and streamlined operations, devices has opened up unprecedent avenues for global connection, innovation, and efficiency. This digital revolution has changed the dynamics of global interconnectedness on one hand they have enabled the businesses and governments to streamline their operations, boost productivity, and deliver services more effectively to citizens and consumers, fostering a more interconnected and efficient global environment and on other hand it has led to threat of cybersecurity breaches.

With societies increasingly reliant on interconnected digital infrastructure, they are susceptible to exploitation by malicious actors driven by personal gain, political motives, or sheer chaos. Cyber offenses encompass a wide range of activities, including hacking, data breaches, identity theft, malware attacks, and online fraud, posing a significant and immediate danger. These threats compromise the security and privacy of individuals, businesses, and governments and endanger critical infrastructure, financial systems, and democratic institutions, highlighting the urgent need for action.

Furthermore, the repercussions of cyber offenses extend beyond economic or security concerns to infringe upon human rights. In a digitally interconnected world, the privileges of privacy, freedom of speech, and the ability to access information are increasingly in jeopardy. Surveillance technologies, methods of gathering data, and online censorship measures may impinge on individuals' privacy and their right to express themselves, thereby suppressing opposition and hindering democratic dialogue. Additionally, cyber offenses can exacerbate existing inequalities by disproportionately affecting marginalized communities that may lack the resources or technical expertise to protect themselves adequately.

Addressing the complex interplay between digitalization and cyber offenses requires balancing leveraging technology's benefits and mitigating its risks. Policymakers, industry stakeholders, civil society organizations, and individuals all play pivotal roles in safeguarding fundamental rights and freedoms in the digital age. This necessitates the implementation of robust legal frameworks, effective cybersecurity measures, and enhanced digital literacy initiatives to empower individuals to safeguard themselves online. By promoting an environment where individuals practice accountable behavior and upholding human rights principles in the digital realm, we can collectively contribute to a more inclusive, secure, and rights-respecting digital future.

Evolution Of Human Rights

Human rights are modern societies' moral and legal foundation, representing every individual's inherent dignity and worth. Human rights embody the idea that every person possesses certain inalienable rights simply by being human. These rights are universal, indivisible, and interdependent, encompassing civil, political, economic, social, and cultural dimensions. Grounded in fairness, parity, and human dignity, human rights are a moral compass guiding societal norms, laws, and policies.

Human rights are not just a set of freedoms and entitlements that individuals are inherently entitled to, regardless of nationality, ethnicity, religion, gender, or other characteristics. They are universal, meaning they apply to all people, and indivisible, meaning they cannot be separated or prioritized. They encompass a broad spectrum of entitlements, from the essential entitlements to existence, freedom, and individual safety to freedom of expression, assembly, and participation in societal, cultural, and political affairs. Human rights are enshrined in international treaties, national constitutions, and customary international law, providing legal protections and mechanisms for redress when rights are violated.

The development of human rights is a nuanced and multifaceted process influenced by historical, cultural, political, and social factors. However, it is important to recognize that ancient civilizations sowed the seeds of human rights. These societies established moral and legal codes that acknowledged basic principles of justice and fairness, laying the foundation for the modern understanding of human rights.

During the 17th and 18th centuries, the Age of Reason saw the rise of contemporary human rights discussions, with philosophers such as John Locke and Jean-Jacques Rousseau advocating for the concept of inherent natural rights for all individuals. The 20th century represented a pivotal moment in advancing human rights, spurred by global movements advocating for liberation, equality, and fairness. Incorporating the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly in 1948 is a significant milestone, underscoring the universal applicability of human rights and establishing a comprehensive framework for their safeguarding.

Following this, subsequent treaties, conventions, and regional agreements have further developed and solidified human rights principles, addressing various issues, including discrimination, torture, genocide, and the rights of marginalized groups such as women, children, and indigenous populations.

Conceptual Framework Of Cyber Crime

Crime is a psycho-socio-economic phenomenon, dating back to the dawn of human civilization. Throughout the development of societies, the nature of crime may have varied. However, in legal terms, "crime" is typically defined as an act or omission that violates a law and is punishable by the state. It encompasses various behaviors considered harmful or detrimental to individuals, communities, or society. Crimes range in severity from minor offenses to serious ones. To establish the commission of a crime, three elements are considered: legality, meaning the act must be prohibited by law; actus reus, which refers to the guilty act or behavior constituting the crime; and mens rea, which pertains to the mental state or intent of the perpetrator to commit the crime. However, laws and definitions of crime can vary between jurisdictions and legal systems.

In the last four decades, rapid digitalization has led to modification in conventional crimes as well; a new breed of crimes known as cyber-crimes have emerged with misuse of internet technologies and are much unregulated and a severe threat to society. The complexities involved in cyber-crime make it different from conventional crimes, as the anonymity between the victim and the criminal makes it more prominent. Cybercrime can be broadly categorized into two main types based on its nature: firstly, when the computer network serves as the medium for committing the crime, encompassing activities such as cyber-pornography, identity theft, phishing, cyber-bullying, cyber-warfare, cyber-terrorism, and others. Secondly, when the computer network itself becomes the victim of the crime, including hacking, malware attacks, denial-of-service (DoS) attacks, data breaches, and similar offenses. Individuals who engage in cybercrimes or cyber offenses are commonly referred to as cyber-criminals.

Though there are various scholar who have worked on this niche of crimes and understanding the nuisances of such criminal activity they have defined the term cybercrime. "Criminal acts carried out by means of computer and internet"[4] (Oxford Dictionary). Suresh. T. Viswanathan in his book "The Indian Cyber law"[5] (Vishwanathan, 2001) have provided very elaborated description of cyber-crimes. "Computer abuse encompasses any illicit or unauthorized activity involving computer technology with the intent to influence or disrupt its function. This includes instances where a victim experiences or is at risk of experiencing a loss while the perpetrator aims to obtain a gain through intentional actions. It spans a broad spectrum of behaviors, from illegal activities such as hacking, malware distribution, and phishing to unethical actions like cyberbullying, online fraud, and cyberstalking. In essence, computer abuse pertains to any wrongful or unauthorized behavior concerning the automated transmission of data."

Further, the nature of cybercrimes has evolved into a formidable challenge, exacerbated by jurisdictional complexities and the intersection with human rights issues. With the digital landscape transcending geographical boundaries, cybercriminal activities often occur across multiple jurisdictions, posing significant challenges for law enforcement agencies worldwide. The problem of jurisdiction becomes particularly acute in cases where cybercrimes impact individuals or entities in different countries, leading to legal ambiguities and difficulties in prosecuting offenders. Moreover, the rapid advancement of technology has outpaced the development of comprehensive legislative frameworks, both at the national and international levels, leaving gaps in addressing emerging cyber threats. These gaps not only hinder effective law enforcement but also raise concerns about the protection of human rights in the digital age. As governments strive to balance security concerns with individual rights in cyberspace, critical issues like internet privacy, the right to express oneself freely, and the accessibility of information face growing risks.

Additionally, the absence of alignment among national laws and differing interpretations of international agreements complicates efforts to safeguard human rights in the digital domain. Given the proliferation and evolution of cybercrimes, there's an urgent demand for robust legal frameworks that prioritize fundamental human rights while effectively addressing global cyber threats. This highlights the significance of global collaboration and coordination in combating cybercrimes effectively.

Cyber Crimes As A Challenge To Human Rights To

The Universal Declaration of Human Rights[6] (UDHR) is a seminal document adopted by the UN General Assembly on 10th December 1948, in the aftermath of the profound atrocities and human rights violation of the World War-II. Conceived as a universal affirmation of the inherent

[4]Oxford Dictionary

[5]Vishwanathan.The Indian Cyber Laws. New Delhi:Bharat Publication, 2001.

[6]https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed on 24th April 2024)

human dignity and inalienable rights, UDHR was drafted by representatives from diverse legal and cultural backgrounds across the globe, ensuring a broad and inclusive perspective on human rights. It consists of 30 articles that outline a comprehensive range of civil, political , economic , social and cultural rights, setting a common standard of achievements for all peoples and nations. As the foundational text for numerous international human rights laws, treaties, and national constitutions, the UDHR serves as a guiding beacon in the global effort to safeguard human dignity and promote justice. But the challenges posed and ethical quandaries created by the cyber-crimes have endangered the very fabric of human rights.

- **Freedom from Torture**[7]
  Article 5 of the charter of the UDHR establishes protection against torture and any form of cruel, inhumane, or degrading treatment as a fundamental human right . However , the rise in cyberbullying, cyber-harassment, cyber-stalking, and cyber-pornography significantly undermines this right by inflicting severe psychological harm and emotional distress on individuals. Cyber bullying involves persistent and malicious online attacks, often resulting in anxiety, depression, and even suicidal ideation. Cyber harassment includes unwanted, aggressive behavior online that can be rentless, causing victims to feel unsafe and humiliated. Cyber-stalking, which entails the use of digital means to track and intimidate individuals, results in a constant state of fear and anxiety for the victim. Cyber-pornography, especially when involving the non-consensual distribution of explicit material, severely degrades personal dignity and privacy. These cyber-crimes inflict mental cruelty and degrade individuals, violating the spirit of Article 5 and challenging the commitment to uphold human dignity.
- **Right to Privacy**
  The Right to Privacy[8] is guaranteed under Article 12 of the UDHR and Article 17 of the ICCPR is a fundamental human right that protects individuals from arbitrary interference with their personal life, home, correspondence, and reputation. It empowers individuals to control their personal information and protects against misuse and exploitation. In the digital age the personal sovereignty secured by the right to privacy is put to threat by the unauthorized access to personal data through hacking and unlawful surveillance which leads to exposure of sensitive information to the cyber-criminals, further this information is misused to impersonate individuals as Identity theft, leading to privacy invasion. With advent of social media platforms these vulnerabilities have led to another level.
- **Right to Security**
  Cybercrime represents a profound violation of the right to security, encompassing various malicious activities that disrupt the fabric of society and compromise individuals' safety and well-being. Cyberterrorism, for instance, strikes at the heart of national security by targeting critical infrastructure such as power grids and transportation systems. These attacks disrupt essential services and endanger public safety, undermining citizens' trust in their government's ability to protect them. Moreover, online financial crimes, including fraud, scams, and theft, erode an individual's financial security and destabilize economic systems and institutions.
- **Right to Information**
  The right to information is a cornerstone of a free and informed society, enabling individuals to access accurate data and make well-informed decisions. However, this right is increasingly under threat from cybercrimes that deliberately manipulate or obstruct the flow of information. Misinformation and disinformation campaigns are prime examples of this violation. Additionally, cyber-attacks targeting information systems can impede access to critical information and services. For instance, Distributed Denial of Service attacks can overwhelm websites and online platforms, making them inaccessible to users. By blocking access to these vital resources, cybercriminals not only impede the free flow of information but also jeopardize public safety and well-being.
- **Right to Work**
  In the digital era it has become an important task to secure individuals right to work. Cybercrime undermines the right to work by disrupting economic activities and compromising business stability. Attacks like ransomware and phishing can cripple business operations, leading to financial losses, business closures, layoffs, and reduced job opportunities. Such economic disruption increases unemployment and economic stability. Intellectual Property theft further threatens businesses by stealing trade secrets and sensitive data, damaging competitive edge, reducing innovation and revenue, and forcing cost-cutting measures, including workforce reductions.
- **Right to Fair Trial**
  Cyber-crimes significantly undermine the right to a fair trial by disrupting judicial systems and compromising the integrity of legal proceedings. Cyber-attacks, such as DDoS attacks, can delay court operations, hearings, and the processing of legal documents, resulting in prolonged cases and denied timely justice. Hackers

[7]https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed on 24th April 2024)
[8]https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed on 24th April 2024)

can manipulate or delete critical legal data, leading to wrongful convictions or the dismissal of valid cases. Infiltration of case management systems can alter schedules and procedural details, causing confusion and unfair advantages. The unauthorized release of sensitive information can prejudice public opinion, endanger witnesses, and breach confidentiality, all compromising trial fairness. Cybercriminals can manipulate digital evidence and disrupt its chain of custody, undermining the reliability of evidence and affecting trial outcomes. Such kind of repeated cyber attacks erode public confidence in the legal system, making it difficult to hold perpetrators accountable and undermining the perceived fairness of the legal process.

Cyber offenses that violate human rights present a significant ethical challenge for individuals, organizations, and governments. A critical issue is balancing privacy and security, as enhanced surveillance efforts, while aiming to prevent cyber-crimes, can infringe on the individual privacy rights. Data protection initiatives must navigate the delicate line between securing sensitive information and respecting privacy. The right to freedom of expression is also at risk; regulating harmful content and combating online harassment must be done without suppressing legitimate speech. Security measures can restrict access to information, raising ethical concerns about the balance between transparency and the need of confidentiality. Economically, the impacts include job losses due to automation and high costs of cyber-security diverting funds from other essential services. Further, the right to fair trial is compromised by the challenge of maintaining the security of legal data and protecting sensitive information. The ethical use of technology including AI and hacking, raises questions about biases and the legitimacy of certain activities. Global disparities further complicate the situation, highlighting the need to address cybersecurity in way that does not disadvantage developing nations, balancing national security with the imperative of international cooperation. Addressing these dilemmas requires a nuanced approach that balances competing rights and interests while upholding principles of justice, fairness, and human dignity.

Conclusion

Implementing a multi-layered approach is crucial to prevent various cyber-crimes and protect human rights effectively. Legal and regulatory mechanisms, such as comprehensive cybersecurity laws, data protection regulations, and regular audits, create a solid legal framework to deter cyber offenses. Technical measures, like advanced encryption, multi-factor authentication, intrusion detection and prevention systems, and regular software updates, help protect sensitive data and enhance security. Further, organizational strategies, including employee training , incident response plans, and strict data access controls, strengthen internal defenses against cyber threats. International cooperation through global cybersecurity alliances and harmonized cyber laws fosters a united front against cybercrime. Ethical and social mechanisms promote responsible technology use and raise public awareness about cyber threats. Judicial and law enforcement mechanisms, such as specialized cybercrime units and judicial training, ensure effective prosecution and fair trials. Technological innovations, like blockchain and AI for threat detection, improve security and transparency. Cross-sector collaboration between public and private entities enhances cybersecurity capabilities. By integrating these mechanisms, we safeguard human rights, create a secure digital environment, and uphold principles of justice, fairness, and dignity in the face of evolving cyber threats.

Bibliography

- Ahuja, V. (2019). *Human Rights: Contemperory Issues.* EBC Publishers.
- Mishra, A. (2021). *Cyber Crime and Procedural Laws:in Human Rights.* New Delhi: VL Media Solutions.
- Mishra, A. K. (2020). *An Overview on Cybercrime & Security Volume - I.* Delhi: Notion Press.
- Sen, G. (2022). *Cyber Security & cyberspace in International Relations.* Delhi: VIJ Publishers.
- Sirohi, M. (2015). *Transformational dimensions of Cyber Crime.* Alpha Editions.
- Aggarwal, S. (2001). *Training on Cyber law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements.* New Delhi: CBI Bulletien.
- Amarnatham, L. (1999). *Cyber Crimes- Prevention and Control Startegies.* Delhi: CBI Bulletien.
- Malik, J., & Chaudhary, S. (2019, 3). Cyber Space - Evolution and Growth. *Journal of Education, Humanities and Literature, 2*(3), 170-190.
- Malik, J., & Choudhary, S. (2018). Policy Considerations In India Against Cyber Crime. *International Journal of Recent Scientific reserach, 9*(12), 29811-29814.
- https://www.un.org/en/about-us/universal-declaration-of-human-rights