Digital Sustainability and Human Rights in the Context of Cybersecurity in India

Dr. Yashodhara Alpesh Bhatt*

Assistant Professor, Department of Law, Veer Narmad South Gujarat University, Surat

Phone No.: 9712902004 ***Scholar ID:*** ***https://scholar.google.com/?authuser=2***
Email ID: yashodharabhatt180977@gmail.com ***ORCID: https://orcid.org/0000-0002-8851-0317?lang=en***

Abstract: *Technological and creative advancements have led to the rise of Digital India, significantly improving lives and strengthening society. Initiated by the Honorable Prime Minister, Shri Narendra Modi, the "Digital India" program has spurred major progress, particularly in IT sectors. Its primary aim is to establish a transparent and participatory system. By enhancing coordination, promoting public accountability, and digitally integrating government services and programs, the initiative seeks to leverage data technology across various government sectors. Ultimately, "Digital India" envisions a digitally empowered and knowledge-driven economy, making it one of the government's most ambitious initiatives.*

The complex relationship between human rights and cybersecurity presents challenges and potential conflicts. As technology becomes more integrated into daily life, ensuring cybersecurity while protecting human rights has become crucial. This study explores how cybersecurity policies impact human rights and vice versa. By analyzing case studies and legal frameworks, the research offers insights into these intricate connections, aiding scholars, legal professionals, and policymakers. Online sharing of data is increasingly common, with social media platforms using personal information for public display. Although websites specify privacy policies, many users remain unaware of them, leading to frequent data breaches. Cybercrime involves unauthorized access to sensitive information through computers and the internet. This paper examines cybercrime, privacy, the right to privacy, and the National Cyber Security Policy's role in safeguarding personal data.

Keywords: *Cyber Security, Digital Era, Digital Sustainability, Human Rights, National Cyber Security Policy*

Introduction

As digital technology continues to be more prevalent in daily living, the significance of cyber security has notably increased. Cybersecurity threats have advanced in both sophistication and frequency, posing a growing challenge in safeguarding against them. Cybersecurity threats vary from simple phishing scams to sophisticated persistent threats that focus on important infrastructure like power grids and financial systems. Cybersecurity incidents can cause considerable economic and social disturbances, leading to possible wide-ranging harm. In a mere decade, India shifted from a cash-driven economy to predominantly embracing digital detection, prevention, and risk management. Regular updates to cybersecurity strategies are crucial due to the constantly evolving threat landscape. Cybersecurity is a complex field that requires the coordinated efforts of various stakeholders including governments, businesses, and individuals.

Additionally, the issue of human rights in cyberspace has become a significant area of global concern. As the internet's reach and impact continue to grow, it is increasingly important to manage the digital domain and safeguard the basic rights of its users. The rise of cybercriminal activities is a direct consequence of internet proliferation, as malicious actors increasingly invade individuals' privacy and compromise their human rights. The internet serves as a crucial medium for free expression and unrestricted access to information, making it imperative to preserve its open nature.

In the early stages of technological advancement, few could have foreseen the profound impact of the internet on fundamental rights. Traditionally, wealth was assessed based on financial assets, whereas, in the digital age, access to information has become a primary indicator of prosperity, reinforcing the notion that "knowledge is wealth." Cyberspace is a dynamic and intricate domain where individuals, software, and services interact, presenting both opportunities and challenges. While technology facilitates societal and legal progress, it simultaneously creates new avenues for human rights violations. In the rapidly evolving digital environment, technological progress significantly impacts people, communities, and the environment. This interconnectedness highlights the crucial link between digital sustainability and human rights, stressing the importance of balanced and ethical management of technology.

Digital Sustainability and Cybersecurity

Digital sustainability focuses on minimizing the environmental and societal impact of digital technologies while maximizing their benefits for future generations. It encompasses aspects such as resource efficiency, energy conservation, e-waste management, and sustainable production methodologies in the technology sector. The objective is to facilitate the sustainable growth and evolution of digital technologies while preventing long-term environmental and societal harm. Sustainable practices range from the eco-friendly production and recycling of electronic devices to the development of energy-efficient software and data centers.

Cybersecurity is essential for digital sustainability as it defends digital systems, networks, and data against cyber threats. It is crucial in protecting privacy and securing data, thus maintaining human rights in the digital world. Strong cybersecurity measures are needed to block unauthorized access to sensitive data and reduce the dangers of data breaches, which helps protect individuals' privacy and digital rights.

Human Rights in the Digital Sphere

The United Nations defines human rights as inherent entitlements that individuals possess by virtue of being human, independent of state authority. These rights are universal and apply regardless of an individual's race, gender, nationality, language, or any other distinguishing characteristic. Human rights range from fundamental rights, such as the right to life, to broader socio-economic rights, including access to adequate food, shelter, healthcare, and education.

The Universal Declaration of Human Rights sets forth fundamental principles concerning human dignity, which include the right to physical integrity (such as life, liberty, and protection from torture and arbitrary detention), social welfare rights (like access to education, employment, and healthcare), legal entitlements (including the right to a fair trial, legal recognition, and participation in governance), and freedoms concerning thought, conscience, religion, and expression.

The United Nations Human Rights Commission asserts that the rights individuals enjoy offline should also be protected online, particularly focusing on the freedom of expression. According to Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR), everyone is entitled to freely seek, receive, and impart

information and ideas, regardless of the medium. Yet, Article 19(3) of the ICCPR recognizes that such freedoms can be curtailed when necessary to safeguard national security, public order, health, morals, or the rights and reputations of others. Any limitations applied must be legally justified and adhere to the conditions specified in the ICCPR.

Recognizing the dual nature of technological advancements, it is important to acknowledge that while the internet facilitates communication and information sharing, it can also be misused in ways that infringe upon individuals' rights. Therefore, limitations on digital content may sometimes be warranted, provided they adhere to internationally accepted legal standards to balance the need for free expression with societal protection.

Literature Review

Kumar et al. (2019) highlight that technological advancements, regulatory frameworks, and investments in digital infrastructure have significantly enhanced access to financial services, making them more affordable and widespread. Midha (2016) recognizes India's "Digital India" initiative as a transformative strategy for preparing the country for a knowledge-driven future. However, he expresses concerns regarding its execution, citing issues of inflexibility and accessibility, which may hinder its success. Despite these challenges, if implemented effectively, the initiative holds the potential to positively impact citizens' lives.

A study conducted by Gupta and Arora (2015) examines the impact of the Digital India initiative on rural communities, emphasizing its role in fostering entrepreneurship and agricultural development. Additionally, the initiative has contributed to women's empowerment in rural areas by expanding their access to digital resources.

Smith et al. (2018) discuss the prevalence of phishing attacks, wherein cybercriminals exploit users' trust to obtain confidential financial information. Jones and Lee (2020) analyze the risks posed by malware, illustrating how malicious software compromises digital payment platforms, leading to financial losses and data breaches. Further, Varalakshmi et al. (2024) stress the need for collaborative efforts to enhance cybersecurity in digital transactions, ensuring the reliability and integrity of financial systems in an increasingly interconnected world.

Digital Sustainability in India

India's digital sustainability strategy is centered on fostering an ecologically responsible, inclusive, and secure digital landscape. As the country's digital economy continues to expand, the associated environmental concerns, such as increased energy consumption and e-waste generation, necessitate proactive measures.

Several key aspects influence digital sustainability in India:

1. Green Data Centres and Renewable Energy

Expansion of Data Centres and Energy Consumption: India's data Centre sector is witnessing rapid growth due to rising digital demand, data localization mandates, and cloud service adoption. However, the operation of data Centres necessitates significant electricity consumption, particularly for cooling infrastructure.

- **Energy-Efficient and Renewable Solutions:** Businesses and policymakers are increasingly prioritizing energy-efficient data centre operations, integrating renewable energy sources to mitigate environmental impact**.**

2. E-Waste Management

- **Escalating E-Waste Generation:** The increased use of digital devices has significantly contributed to the growth in e-waste. In 2022, India produced around 3.2 million metric tons of electronic waste, making it one of the top e-waste generating countries worldwide.
- **Regulatory Framework and Circular Economy:** The updated e-waste management rules in India (2022) have introduced the concept of extended producer responsibility, requiring manufacturers to actively participate in the disposal and recycling of e-waste. These regulations support the adoption of sustainable recycling and refurbishment, thereby minimizing the environmental impact of digital technology consumption.

3. Digital Inclusion and Bridging the Digital Divide

- **Strengthening Rural Digital Infrastructure:** Programs like Bharat Net, which seeks to connect 600,000 villages to high-speed internet, and PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyaan), which aims to improve digital access in rural regions, are key in bridging the digital gap and promoting equitable development. These initiatives help ensure that rural areas are not left behind in the digital age.
- **Affordable Digital Services:** The expansion of India's telecommunications sector, led by companies like Reliance Jio, has significantly lowered data costs, enabling broader participation in the digital economy. This accessibility promotes social and economic inclusivity**.**

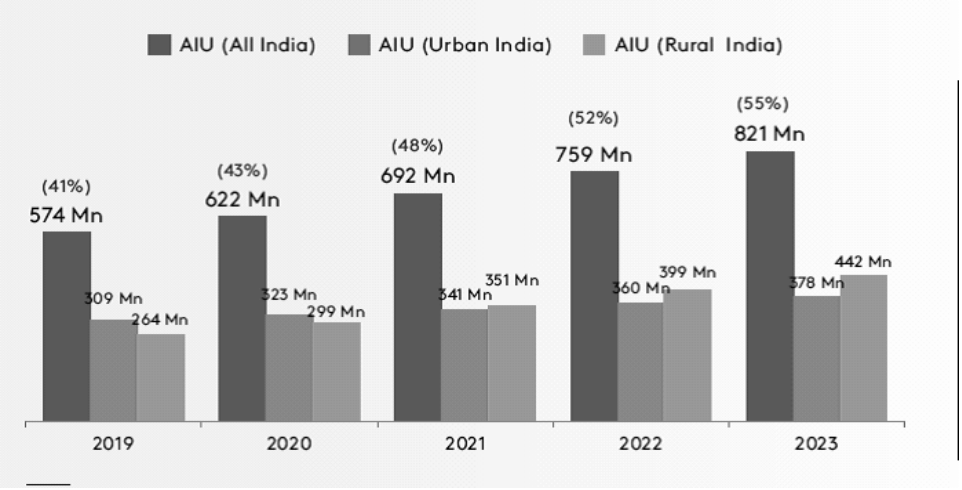
4. Cybersecurity and Data Privacy

- **Cybersecurity Frameworks for Sustainable Development:** Enhancing cybersecurity is crucial for digital sustainability. The Indian government has implemented cybersecurity strategies and data protection legislation, such as the Digital Personal Data Protection Act (2023), to secure digital assets and ensure the privacy of users.
- **Public Awareness Initiatives:** Efforts by both government and corporations to raise public awareness about cybersecurity through campaigns and digital literacy initiatives are vital in creating a secure digital ecosystem.

5. Financial and Digital Literacy for Sustainable Participation

- **Digital Literacy Programs:** India has launched initiatives such as PMGDISHA to equip citizens, particularly in rural areas, with essential digital skills. Digital literacy is fundamental in ensuring safe online interactions and mitigating risks such as financial fraud.
- **Expansion of Digital Payment Systems:** The widespread use of digital payment systems, especially the Unified Payments Interface (UPI), has advanced financial inclusion by offering easy-to-use, cashless payment options. This shift helps create a more transparent and effective economic structure.

Chart - I
Internet Users in India



Source: ICUBE 2023, Internet in India 2023 report by Kantar & Internet and Mobile Association of India, 2023

Expansion of Internet Access and Digital Payment Systems in India

India has witnessed significant growth in internet penetration, with overall usage rising from 41% in 2019 to 55% in 2023. This expansion has been observed across both urban and rural areas, driven by improved digital infrastructure and affordability:

- Internet Users in Urban Areas: Rose from 309 million in 2019 to 442 million in 2023.
- Internet Users in Rural Areas: Increased from 264 million in 2019 to 378 million in 2023.

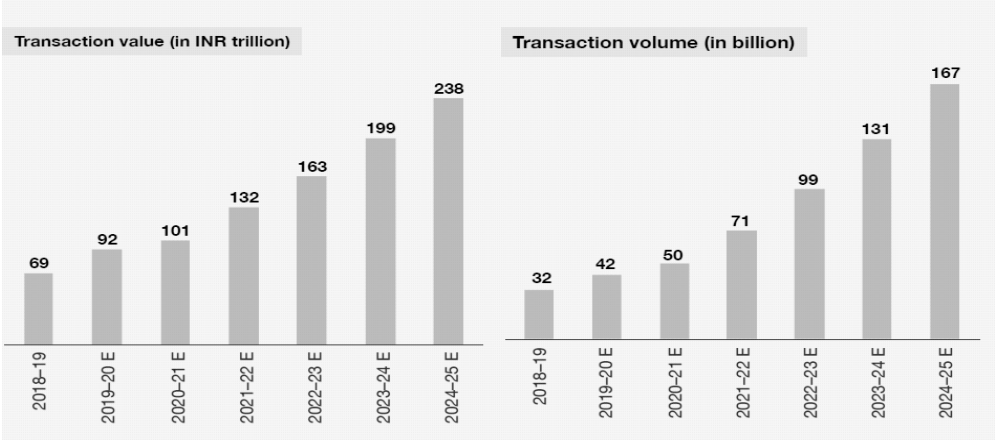
This surge in connectivity has been instrumental in fostering digital inclusion and enabling financial technology adoption.

The Unified Payments Interface (UPI) has become a pivotal element in revolutionizing India's digital payment landscape, showing rapid expansion over time:

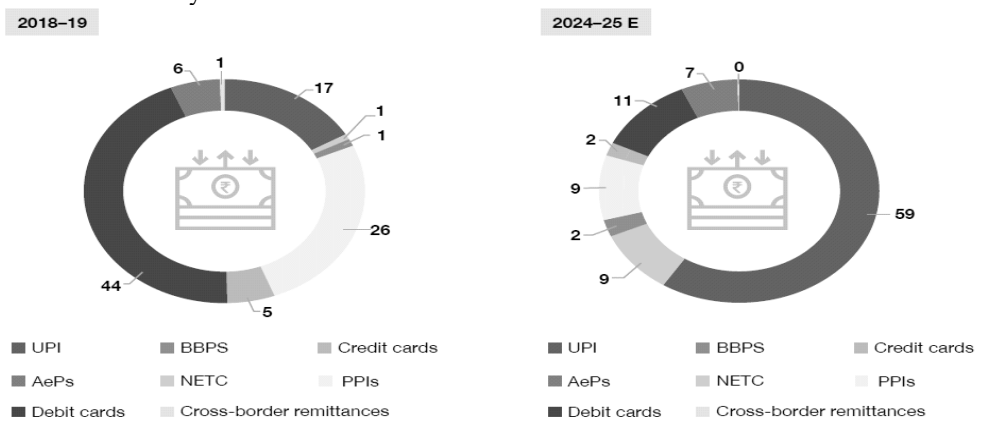
- 2017: Processed over 100 million transactions, amounting to INR 67 billion, reflecting a 900% year-on-year (YoY) surge.
- 2018: Transaction value surpassed INR 1.5 trillion, marking a 246% increase compared to the previous year.
- 2019: UPI transactions grew further to INR 2.9 trillion, registering a 67% YoY rise.

- 2020 (December): Monthly transaction volume reached INR 4.3 trillion, reflecting a 63% growth from the previous year.
- 2021 (June): Transactions via UPI surpassed 1.49 billion, totaling INR 5.6 trillion, which marks a 72% year-over-year increase.
- 2022: As reported by NPCI, the annual UPI transaction value hit INR 125.95 trillion, showing a 1.75-fold increase over the prior year. Importantly, UPI transactions comprised about 86% of India's GDP for the fiscal year 2022.
- 2023: UPI recorded a total of 83.75 billion transactions.

The significant uptake of UPI underscores the growing dependence on digital payment methods in India, indicating a wider move towards a cashless society. This trend is likely to persist, further promoting financial inclusion and digital innovation across different industries.



Source: PwC analysis of data from the Reserve Bank of India



Source: PwC analysis of data from the Reserve Bank of India

Upcoming Developments in UPI and Digital Payment Usage in India

Dominance of UPI in Payment Systems

The Unified Payments Interface (UPI) is expected to emerge as the payment method of choice for Indian consumers in the near future. Its adoption is likely to grow with its increasing application in various transactions such as cash withdrawals and daily purchases. By 2025, UPI is projected to dominate the digital payment scene, especially for small-value purchases at local stores.

The growth of UPI is anticipated to also boost the development of Prepaid Payment Instruments (PPIs) and the use of debit and credit cards. Nonetheless, despite the rise of UPI, payment cards are expected to remain integral to India's financial framework, supported by the adoption of card tokenization and the National Common Mobility Card (NCMC).

Post-Pandemic Shifts in Consumer Payment Preferences

Following the COVID-19 pandemic, consumer behavior is expected to shift towards debit cards for everyday expenses and credit cards for high-value purchases. Additionally, contactless payments are projected to gain further traction, especially with RBI's revised regulations, which now permit PIN-authenticated contactless transactions exceeding INR 10,000. These changes are expected to reshape payment habits, particularly in urban and metropolitan regions.

Emergence of Mobile and Wearable Payment Systems

The adoption of mobile-based and wearable payment solutions incorporating card tokenization is set to accelerate in key urban markets. Businesses that have traditionally relied on physical Point-of-Sale (PoS) systems may need to integrate QR code-based UPI payments and digital wallets to align with evolving consumer preferences.

Evolution of Bill Payments and Emerging Digital Payment Technologies

The Bharat Bill Payment System (BBPS) will continue to streamline the bill payment sector, with transaction volumes expected to rise as more categories are integrated. Faster adoption is anticipated if BBPS expands its range of mobile-based payment options. Even as the effects of the pandemic subside, a growing number of consumers are expected to favour digital transactions over cash payments. Additionally, business correspondents and channel partners linked to BBPS may gain prominence as preferred bill collection points, as service providers encourage digital payments to reduce physical crowding at collection centres.

The National Electronic Toll Collection (NETC) system is expected to drive the digitization of low-value cash transactions, further strengthening digital payment adoption. The introduction of new applications for NETC, including fuel and parking payments, is likely to accelerate its acceptance among consumers. With advancements in payment technologies and their growing application across various industries, the digital payment sector is set to maintain its upward trajectory. By 2024–2025, the industry is projected to generate INR 2,931 billion in revenue, solidifying the role of digital payments in India's economic framework.

Cybercrime Patterns and Legal Structure in India

Cyberspace comprises a worldwide domain that includes connected information technology infrastructures like the Internet, telecom networks, computer systems, and embedded processors. Acknowledging the growing importance of this digital realm, India enacted the Information Technology (IT) Act in 2000, marking the country's initial legislative measure to regulate cyberspace. This act was later revised in 2008 to enhance regulations concerning data security, electronic commerce, and cybercrimes.

The National Cyber Security Policy is built on five key principles: engagement, empowerment, innovation, inclusiveness, and international collaboration. The

policy outlines six primary objectives for enhancing India's cyber defense mechanisms, including:

- Establishing a secure cyber ecosystem,
- Building trust and confidence in IT systems and digital transactions, and
- Creating a governance framework and supportive structure to tackle cybersecurity issues, particularly emphasizing the protection of critical information infrastructure.

India has recognized the need for a flexible and dynamic national cyber law to maintain an effective cybersecurity framework. The National Security Council Secretariat has emphasized the importance of establishing adaptable legal and organizational frameworks that can evolve to counter new and emerging cyber threats.

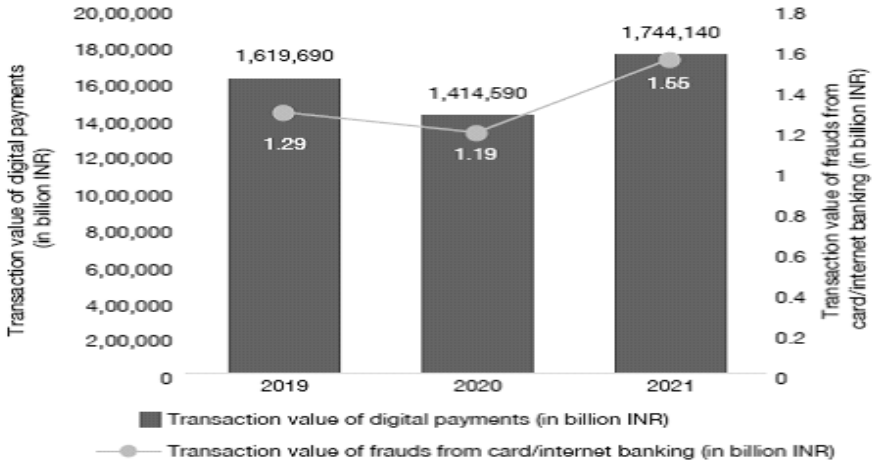
Enhancing Cybersecurity through Strategic Policy and Partnerships

Enhancing Cybersecurity through Strategic Policy and Partnerships The Ministry of Home Affairs is deeply involved in creating detailed legislation to address cyberterrorism and cyberespionage, working closely with essential stakeholders to build a strong legal and enforcement structure. Developing partnerships between public and private sectors is considered vital for achieving international cooperation, enhancing collaboration across ministries, and nurturing a proactive approach to cybersecurity.

As malicious software increasingly threatens both government and private entities, perpetrated by state and non-state actors alike, cybersecurity professionals stress the importance of remaining vigilant. The World Economic Forum has pointed out that financial crimes and fraud constitute industries worth trillions of dollars. By 2017, private companies had already spent $8.2 billion on anti-money laundering (AML) initiatives. Financial losses from cybercrimes, including both known and undetected cases, are escalating rapidly.

Cybercrime Trends and Digital Payment Security

In recent years, India has seen a series of significant cybersecurity incidents affecting various industries, a worrying trend amidst the rapid increase in digital payment transactions. Over the past four years, the number of digital transactions has increased fourfold, from 3,134 crore in the fiscal year 2018-19 to 5,554 crore in 2020-21, reaching 7,422 crore by February 28, 2022. As the digital financial landscape continues to expand, maintaining the security and robustness of online transactions is increasingly critical. The adoption of sophisticated cybersecurity strategies, strengthened regulatory frameworks, and enhanced international collaboration are essential to reduce cyber threats and protect India's digital financial sector.



Consumers today can choose from a variety of digital payment options such as debit and credit cards, digital wallets, mobile banking, QR codes, and the Unified Payments Interface (UPI). Of these, UPI has been instrumental in accelerating the growth of digital transactions across India.

Between 2021 and 2022, UPI accounted for 46 billion out of the 72 billion total

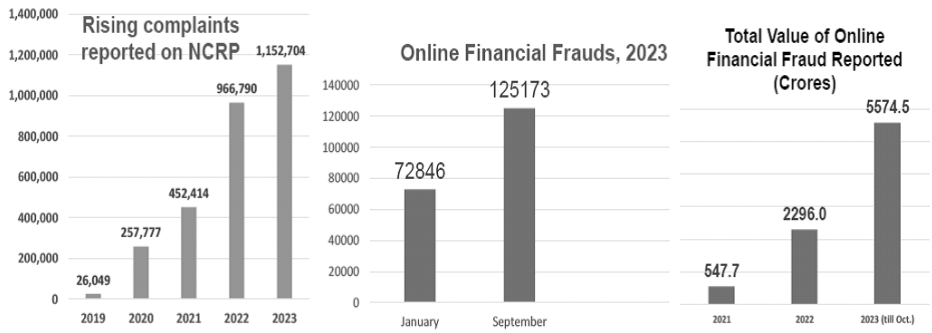
digital payment transactions, marking a 109% increase from the 22 billion transactions recorded in the previous year. During the same period, overall digital payments grew by 64%, further highlighting the increasing adoption of cashless payment solutions.

However, while these advanced payment technologies have enhanced transaction efficiency and accessibility, they have also created new vulnerabilities. Cybercriminals are increasingly exploiting human errors and weaknesses in digital payment infrastructures, leading to a rise in fraudulent activities. As digital payment systems continue to evolve, strengthening security frameworks and fraud prevention mechanisms remains critical to ensuring a safe and resilient financial ecosystem.

Cyber Crime Statistics based on complaints reported on NCRP

Category	2021	2022	2023
Biometric theft based frauds	0	0	3986
Authorized Push Payments frauds	118525	376531	632267
Demat / Depository Fraud	4301	8207	15770
Fraud Call/Vishing	27104	55839	66069
E-Wallet Related Fraud	28078	30700	23874
Business Email Compromise/ Email Takeover	1769	2339	2705
Internet Banking Related Fraud	33335	99793	154609
Debit/Credit Card Fraud/SIM Swap Fraud	49733	121031	131429

Source: NCRP



Legal Framework for Human Rights and Cybercrime in India

The Information Technology (IT) Act, established in 2000, has been crucial in acknowledging the significance of personal identity in the digital realm. The Indian government has introduced initiatives like Digital India and Make in India, each with unique yet complementary goals. Digital India is designed to transform the country into a digitally empowered society and knowledge-based economy, whereas Make in India aims to attract investment, advance technology, improve skills, protect intellectual property, and create top-tier manufacturing facilities. An essential aspect of the Digital India program is its focus on cybersecurity, vital for its success through the creation of a secure online ecosystem. This section discusses various cybersecurity strategies and the roles of different entities in maintaining a robust digital space.

The IT Act of 2000 aligns with international treaties and declarations, ensuring the harmonization of legal provisions with global standards in cyberspace governance. It covers five fundamental dimensions: access, commerce, governance, individuals, and rights. The legislative landscape has evolved to accommodate both IT law and international legal frameworks, particularly concerning cybersecurity and digital rights. A key element of cybersecurity—privacy rights—was greatly strengthened by revisions made to the IT Act in 2008. Additionally, the Supreme Court of India cemented the constitutional foundation of privacy in the digital age with a seminal decision on August 24, 2017. As India's primary legislation governing cybercrimes, digital offenses, and online transactions, the IT Act draws inspiration from the United Nations Model Law on Electronic Commerce (UNCITRAL Model, 1996), which was endorsed by the UN General Assembly on January 30, 1997.

Key Features of the IT Act, 2000

- Legal recognition for email as an official mode of communication.
- Authorization of digital signatures, ensuring secure online authentication.

- Establishment of Certifying Authorities to regulate the issuance of digital certificates.
- Facilitation of e-governance, allowing the government to publish notifications and conduct transactions online.
- Enabling business-to-business (B2B) and business-to-government (B2G) communications via the internet.
- Introduction of digital signatures as a mechanism to verify an individual's identity online, enhancing security.
- Provision for financial compensation to organizations in case of financial losses or damages resulting from cybercrime.

Legal Provisions Addressing Cybercrime and Human Rights Violations

In response to the escalating menace of cybercrime, effective regulatory frameworks are crucial for addressing cyber offenses like hacking, cyberterrorism, data breaches, and identity theft. The IT Act categorizes a broad array of offenses and outlines penalties for cybercriminal activities, which include:

- Penalties for damaging computer systems (Section 43).
- Compensation requirements for failing to protect personal data (Section 43A).
- Tampering with computer source codes (Section 65).
- Hacking and unauthorized access to data (Section 66).
- Sending offensive messages through electronic communication services (Section 66A).
- Illegitimately acquiring stolen computer resources or devices (Section 66B).
- Identity theft and the fraudulent usage of electronic credentials (Section 66C).
- Cheating by impersonation via digital means (Section 66D).
- Infringement of privacy using unauthorized digital methods (Section 66E).

- Cyberterrorism and digital threats to national security (Section 66F).
- Publication or transmission of obscene electronic content (Section 67).
- Criminal penalties for distributing child sexual exploitation material (Section 67B).
- Obligation for intermediaries to preserve digital evidence (Section 67C).
- Governmental authority to intercept, monitor, and decrypt digital communications for security purposes (Section 69).
- Restriction of public access to specific online content for security reasons (Section 69A).
- Authority to collect traffic data and cybersecurity-related information (Section 69B).
- Unauthorized entry into protected systems (Section 70).
- Penalties for deceit in digital transactions (Section 71).
- Violation of confidentiality and privacy in the digital realm (Section 72).
- Issuing fraudulent digital signature certificates (Sections 73 & 74).
- Jurisdictional application of IT Act offenses beyond Indian Territory (Section 75).
- Provision ensuring that penalties and compensations do not interfere with other legal remedies (Section 77).
- Compounding of cyber offenses under certain conditions (Section 77A).
- Criminal acts subject to a maximum of three years in prison (Section 77B).

Additionally, the Act provides for:

- Limited liability exemptions for intermediaries under specific conditions (Section 79).
- Penalties for aiding, abetting, or attempting cyber offenses (Sections 84B & 84C).
- Corporate liability for cyber offenses committed by an organization (Section 85).

The enforcement of these provisions is contingent on the nature of the cybercrime, investigative reports filed by law enforcement agencies, and the approach adopted by investigating officers. India's evolving legal framework seeks to strike a balance between cybersecurity, human rights protection, and digital governance, ensuring a safer and more secure cyberspace.

National Cyber Security Policy

National Cyber Security Policy and the Cybercrime Environment in India

Indian Computer Emergency Response Team (CERT-In)

Active since January 2004, the Indian Computer Emergency Response Team (CERT-In) is crucial to India's cybersecurity infrastructure. As the central agency tasked with addressing cybersecurity issues, CERT-In safeguards the security of the Indian cyber ecosystem (Mehta et al., 2021). Its primary duties involve:

- Gathering, analyzing, and distributing reports on cyber incidents.
- Predicting and alerting on potential cybersecurity threats.
- Providing rapid response mechanisms to cyber incidents.
- Continuous monitoring of cyber activities to detect potential threats.
- Developing data security policies, frameworks, and guidelines to assist in cyber defense, incident identification, and tracking.

CERT-In also issues security advisories, vulnerability bulletins, and whitepapers, ensuring that organizations and individuals remain informed about evolving cyber threats and mitigation strategies.

Right to Privacy: The 2017 Supreme Court Judgment

The pivotal decision in Justice K.S. Puttaswamy v. Union of India (2017) by a nine-member bench of the Supreme Court declared privacy a fundamental right under the Indian Constitution. The verdict acknowledged that diminishing privacy can adversely impact other essential rights, such as freedom of speech and expression. This judgment has elevated the status of privacy from a simple ethical or

philosophical issue to a right protected by the constitution, especially relevant in the digital era.

Indian Laws on Data Privacy and Protection

The 2017 Supreme Court ruling on privacy solidified informational privacy as a crucial right, empowering individuals to manage their personal data. This verdict strengthened the legal framework for data protection in India, guaranteeing that personal freedom and privacy are protected in the digital space.

In addition to provisions under the IT Act, other legal safeguards for cybersecurity and privacy include:

- Section 425 of the IPC (now Section 324 of the BNS) – Addresses compensation, penalties, and asset confiscation in cyber-related offenses.
- Sections 77, 77A, and 77B of the IT Act – Define the penal framework for cybercrimes, including provisions for compounding offenses and punishments extending up to three years in prison.

Cyber Surakshit Bharat Initiative

The Cyber Surakshit Bharat (CSB) initiative was launched under a Public-Private Partnership (PPP) model to train and empower Chief Information Security Officers (CISOs) and IT professionals in cyber risk management. The program focuses on capacity building across government institutions, banks, and public sector units (PSUs) to strengthen India's cyber resilience.

The training curriculum was developed in consultation with industry consortiums and knowledge partners. As of September 2022, 31 training sessions had been conducted, benefiting 1,266 CISOs and IT experts from various government and financial organizations.

Cybercrime Prevention against Women and Children (CCPWC) Initiative the Ministry of Home Affairs (MHA) has distributed ₹93.12 crore to states and union territories through the Cybercrime Prevention against Women and Children

(CCPWC) Scheme. From this fund:

- ₹87.12 crore was allocated for establishing cyber forensic laboratories and employing skilled operators.
- ₹6 crore was allocated for the training of 40,500 police personnel, prosecutors, and judicial officers by March 2020 (MHA, 2021).

This initiative underscores the government's commitment to combating cybercrimes, particularly those targeting women and children.

Case Studies on Cybercrime in India

1. NSP Bank Cybercrime Case

A management trainee at NSP Bank got involved in a cyber-conflict. The trainee had regularly communicated with a colleague via the company's email system. Following the termination of their relationship, the female employee fabricated email addresses (like "Indian Bar Associations") and dispatched harmful emails to the male employee's overseas clients. This action tarnished the company's reputation and resulted in considerable financial losses. Consequently, the company faced a lawsuit from the bank, which accused it of being responsible for the unauthorized use of its IT infrastructure.

2. Bazee.com Case (2004)

In December 2004, the CEO of Bazee.com was detained following the discovery that the platform was offering compact discs (CDs) with explicit content for sale. These CDs were also being sold in markets in Delhi, leading to police interventions in both Delhi and Mumbai. Although the CEO was eventually released on bail, the incident highlighted the difficulties in overseeing online marketplaces and making intermediaries responsible for illegal content.

3. Cyber Attack on Cosmos Bank (2018)

In August 2018, the Pune branch of Cosmos Bank suffered a sophisticated cyber-attack, leading to a loss of ₹94 crore. Cybercriminals successfully breached the

bank's main server and transferred the funds to a Hong Kong-based bank.

The attackers infiltrated the ATM switching system, which serves as a gateway between payment processing networks and the bank's core system. This enabled them to extract sensitive financial data from numerous VISA and Rupay debit cards. Due to the compromise of the payment gateway, the bank and its customers remained unaware of the fraudulent transactions until substantial damage had occurred.

Human Rights Challenges and Risks in the Digital Age

The rapid advancement of technology in recent decades has introduced significant challenges and risks to human rights. As individuals engage in digital interactions—whether through financial transactions, the use of digital devices, urban navigation, or online platforms such as social media, email, or encrypted messaging tools—a vast amount of data is generated. This transactional data, initially neutral, is increasingly being de-anonymized, transforming it into personally identifiable information.

Although online and mobile environments offer some degree of quasi-anonymity, this does not guarantee privacy, as observed data can be leveraged to infer connections between individuals, families, or communities. Despite the legitimate and non-controversial nature of most digital transactions, governments and corporations are leveraging digital surveillance to obtain granular insights into personal behaviours for administrative, commercial, or security purposes. When misused, this informational power poses significant risks to individuals, organizations, and society. Heightened surveillance can exacerbate online harassment and hate speech, disproportionately targeting marginalized communities. The growing use of mass surveillance techniques justified under the pretext of security and law enforcement arises profound ethical concerns, as highlighted by various experts.

Beyond direct surveillance, digital activities are now being used as indicators of human rights violations and as tools for monitoring and controlling dissent. The suppression of political activism and free expression in online spaces mirrors historical patterns of authoritarian control and repression, revealing traces of fascist and totalitarian tendencies that persist in contemporary societies.

Privacy and Surveillance Concerns

The issue of government surveillance has been particularly scrutinized in light of the Supreme Court's acknowledgment of public apprehension toward state surveillance. Surveillance operates through three primary methods:

- Electronic Surveillance
- Manual Surveillance
- Communication Surveillance

The Indian government employs extensive monitoring mechanisms, accessing content-level data from telecom and internet service providers (ISPs) while maintaining secrecy through official exemptions. Several national and state-level surveillance programs operate within this framework, including:

- National Intelligence Grid (NATGRID)
- Network Traffic Analysis (NETRA)
- Lawful Intercept and Monitoring (LIM)
- Centralized Monitoring System (CMS)

Without robust data protection legislation, residents of India must rely solely on the privacy policies of internet and telecom service providers. The idea of surveillance capitalism is especially pertinent here, where personal data is converted into predictive analytics that influence and predict future behavior.

While technology has greatly facilitated data collection, the lack of a well-defined legislative framework places individuals at risk of excessive government control over digital information. Technology firms, network equipment providers, and

search engine operators have a crucial role to play in mitigating the risks of unchecked surveillance by ensuring greater transparency and accountability in data collection practices.

Hate Speech and Online Harassment

The expansion of digitalization has led to the emergence of new human rights challenges in online spaces, disproportionately affecting vulnerable and marginalized groups. Social media platforms and other digital forums have increasingly become hotbeds of coordinated online harassment, where individuals face targeted digital attacks in highly public and visible spaces.

Rather than being isolated occurrences, these attacks are often systematic and widespread, creating a hostile digital environment. Online discourse frequently includes hate speech, abuse, and threats of violence, particularly against oppressed communities. While some online spaces foster genuine intellectual discourse, others perpetuate discriminatory ideologies, contradicting the principles of democratic and free expression. The increase of hate speech online underscores the critical need for detailed regulations and technological solutions to combat online extremism while preserving freedom of speech.

Cybersecurity Measures to Protect Human Rights

In the digital age, a secure online environment is vital for protecting human rights. Enhancing cybersecurity infrastructures is key to improving privacy, data security, and freedom of speech. It is essential to protect the integrity of sensitive personal data from unauthorized access, data breaches, manipulation, and cyber theft.

A robust cybersecurity infrastructure can improve the resilience of digital platforms, ensuring the confidentiality and security of personal and official communications. Some recommended measures include:

- End-to-end encryption in messaging services to prevent unauthorized access.

- Enhanced cybersecurity protocols for digital public services.
- Implementation of strong data protection laws to regulate government and corporate surveillance.

By incorporating advanced security mechanisms, individuals and organizations can better defend against cyber threats, thereby ensuring that human rights remain protected in an increasingly digital world.

Conclusions

India's security measures must incorporate the protection of the environment, natural resources, and individual rights, all of which are fundamentally interconnected with the broader framework of human rights protection. Essential strategies such as encryption, attribution, and trust-building should be integrated into security doctrines to facilitate peaceful conflict resolution in cyberspace.

Discussions on digital sustainability in India have grown more intricate, with varied viewpoints arising from civil society, experts, academics, and policymakers. Some stress the importance of digital freedom and privacy rights, while others highlight the significance of data localization for geopolitical security, the role of machine learning in managing data, or the necessity of robust cybersecurity measures for national defense.

India has been instrumental in diversifying global Internet governance, particularly through its active participation in the World Summit on the Information Society (WSIS) and its role as a central hub for Digital Development and Inclusion Governance (DDIG). However, concerns persist regarding the expansion of state surveillance, data localization policies, and the inadequacy of existing data protection laws. Critics argue that India’s approach to international cyber policy has not sufficiently addressed individual privacy rights and other human rights frameworks established in global conventions.

To promote freedom and stability in cyberspace, India must prioritize digital

sustainability, which entails protecting environmental resources, ensuring data privacy, and upholding fundamental freedoms. The rapid evolution of cybercrime—driven by technological advancements—has amplified threats to individuals and national security. Given the transnational nature of cybercrimes, legal and technical challenges in investigation and prosecution persist. Therefore, a harmonized global approach with international cooperation and legal coordination is crucial for effectively combating cyber threats.

Future Directions

To translate current ethical discussions into concrete policy measures, five key areas require further research and activism:

- Strengthening Data Protection and Regulatory Frameworks
    - Domestic cybersecurity and data protection laws must align with evolving ethical security principles.
    - A human rights-centered approach should be embedded in national and civic regulations.
- Government and Institutional Interventions
    - Policymakers should ensure civil society participation in shaping cybersecurity standards.
    - Increased transparency and accountability in governance mechanisms are essential for protecting digital rights.
- Integration of Civil Society in Cybersecurity Standards
    - Ethical cybersecurity practices should incorporate community-led initiatives to enhance digital inclusivity and safeguard human ecology.
- Ethically Driven Research and Development (R&D)
    - Future technological advancements should be guided by ethical considerations.

    - Cybersecurity innovations must account for the narratives and experiences of victims to ensure equitable digital development.
- Rights Impact Assessments in Digital Investments
    - Human rights impact evaluations must be embedded in both public and private sector investments.
    - Assessments should be conducted at all stages of technological development, including preproduction, testing, and deployment.

By addressing these areas, India can bridge the gap between cybersecurity and human rights, fostering a secure, ethical, and sustainable digital ecosystem that aligns with global human rights principles.

References

- Shukla, Dr. Mansi & Bose, Ms. Shilpi (2017). Impact of Digitalization in Economy and the Effects of Demonetization. ELK Asia Pacific Journals, New York.
- Kaul, Mrinalini & Mathur, Purvi (2017). Impact of Digitalization on the Indian Economy and Requirement of Financial Literacy, New Delhi.http://www.cs.cornell,edu/wya/papers/iMP-2000.html
- Ashman, A. (2003), Digitization. In. J. Feather & P.Sturges (Eds), International Encyclopaedia of Information Science (2nd ed., p.138.). Routleg Taylor and Francis Group,London.
- Borah, P. S., Iqbal, S., & Akhtar, S. (2022). Linking social media usage and SME's sustainable performance: The role of digital leadership and innovation capabilities. Technology in Society. [HTML]
- Rai, R. K., Khajanchi, S., Tiwari, P. K., Venturino, E., & Misra, A. K. (2022). Impact of social media advertisements on the transmission dynamics of COVID-19 pandemic in India. Journal of Applied Mathematics and Computing, 1-26. springer.com
- Pop, R. A., Săplăcan, Z., & Alt, M. A. (2020). Social media goes green—The impact of social media on green cosmetics purchase motivation and intention. Information. mdpi.com
- Asghar, M. Z., Barbera, E., Rasool, S. F., Seitamaa-Hakkarainen, P., & Mohelská, H. (2022). Adoption of social media-based knowledge-sharing behaviour and authentic leadership development: evidence from the educational sector of Pakistan during COVID-19. Journal of Knowledge Management, 27(1), 59-83. researchgate.net
- Wielki, J. (2020). Analysis of the role of digital influencers and their impact on the functioning of the contemporary on-line promotional system and its sustainable development. Sustainability. mdpi.com
- Thornton, C. Y. (2024). For the Culture. Inclusion in Linguistics. google.com

- Luo, T., Freeman, C., & Stefaniak, J. (2020). “Like, comment, and share”—professional development through social media in higher education: A systematic review. Educational Technology Research and Development, 68(4), 1659-1683. [HTML]
- Ali Qalati, S., Li, W., Ahmed, N., Ali Mirani, M., & Khan, A. (2020). Examining the factors affecting SME performance: the mediating role of social media adoption. Sustainability. mdpi.com
- Nundy, S., Ghosh, A., Mesloub, A., Albaqawy, G. A., & Alnaim, M. M. (2021). Impact of COVID-19 pandemic on socio-economic, energy-environment and transport sector globally and sustainable development goal (SDG). Journal of Cleaner Production, 312, 127705. nih.gov
- Mujahid, M. S. & Mubarik, M. S. (2021). The bright side of social media: social media platforms adoption and start-up sustainability. Frontiers in psychology. frontiersin.org
- J. Yadav, A. Yadav, M. Misra, N. P. Rana, and J. Zhou (2023). Twitter statistics show that social media plays an important role in technology uptake for sustainable agriculture techniques. Communications of the Association for Information Systems, 52(1), 833–851. uts.edu.au
- Sundaram, R., Sharma, D. R., & Shakya, D. A. (2020). Power of digital marketing in building brands: A review of social media advertisement. International Journal of Management, 11(4). ssrn.com
- Azhar, M., Hamid, S., Akhtar, M. J., & Subhan, M. (2022). Determining the impact of social media use on sustainable rural tourism: a TPB application involving place emotion. Journal of Tourism, Sustainability, and Well-Being, 10(4): 292-312. jsod-cieo.net
- Kaur, J., Mogaji, E., Wadera, D., & Gupta, S. (2022). Sustainable consumption patterns in Indian households: A story of environmental management linked to Indian ethos and generational disparities. Society and Business Review. [HTML]
- Bryła, P., Chatterjee, S., & Ciabiada-Bryła, B. (2022). The impact of social media marketing on consumer engagement in sustainable consumption: A systematic literature review. The International Journal of Environmental Research and Public Health, volume 19, issue 24, page 16637.
- mdpi.com
- Bhatt, R.K. (2011). Libraries in India: collection to connectivity. Ane Books. New Delhi.
- http://portal.unesco.org/ci/en/files/2639 3/12075628443open_acce ss_book_en.pdf/open_access_book_en.pdf.
- Kovacs, Anja and Hawtin, Dixie. (2017). Cyber Security, Cyber Surveillance and Online Human Rights. https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
- Japan.(2013). Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace.
- Kuehl, Daniel T.(2009).From Cyberspace to Cyber power: Defining the Problem *Cyber power and National Security*, Washington: National Defence University Press. http://ctnsp.dodlive.mil/files/2014/03 /Cyberpower-I-Chap-02.pdf