A COMPARATIVE ANALYSIS OF TECHNOLOGY LAW IN INDIA WITH REFERENCE TO INTERNATIONAL FRAMEWORKS

Dhatri Mishra*

ABSTRACT

Over the past few decades, we have witnessed remarkable technological advancements that have significantly influenced various fields, including law, social frameworks, economics, and other intersecting disciplines. Beginning with the UN General Assembly Resolution, which paved the way for the approval of the Information Technology Act, we saw the evolution into the enactment of Modern Electronic Trade Law. This progression highlighted the ways in which the right to privacy has been reshaped by the expansion of information technology, necessitating changes to ensure the protection of legal interests. In today's technology-driven world, data has become a valuable asset. India, however, lacks comprehensive legislation dedicated to data protection and privacy. The existing laws and policies are fragmented and primarily sector-specific, with a focus on the IT Law, 2000. Additionally, the amendments to the Information Technology Act, which took effect in February 2009 after receiving presidential assent, have had a significant impact on India's legal landscape. These amendments acknowledged that information confidentiality forms an integral part of our privacy rights, explicitly stating that confidentiality also includes the protection of personal identity.

Keywords: Privacy, Technology, Data Protection, Information, Supreme Court.

INTRODUCTION

We are in an era of significant transformation, where a convergence of technological advancements is reshaping both economic production and the concept of individual freedom. These shifts are primarily governed by legal frameworks. Law has been and will continue to be a vital domain where the conditions for the future are debated and determined. However, a proper understanding of the law's role must also account for the technological, economic, and social landscapes in which it operates, as well as the historical moment when it intersects with other fields. Gaining a thorough understanding of how technology influences human life, and

*RAMAIAH COLLEGE OF LAW, BANGALORE.

how law responds to and interacts with these technological changes, is essential for understanding the various stakeholders and the broader implications of ongoing institutional challenges.

The term "technology," derived from the Greek word "techne," meaning art, skill, or craft, and "logy," meaning the study or theory of, refers to an array of tools, methods, and systems utilized by individuals. This includes both machinery and processes, and it encompasses many disciplines, such as engineering, which focuses on creating and improving new technologies. The influence of technology extends to both human and animal species, shaping their ability to interact with and adapt to their natural environments. In this context, the term technology can be applied broadly, or it can refer to specific domains such as construction technology, medical technology, and, most relevant today, information technology (IT). With IT being at the forefront of modern advancements, it profoundly affects various aspects of life, governance, and business, making it imperative to assess its legal implications.

HISTORY OF TECHNOLOGY LAW

The origins of technology law can be traced back to significant international milestones, such as the UN General Assembly Resolution of 30 January 1997, which was instrumental in the approval of the Information Technology Act. This ultimately led to the establishment of the Modern Electronic Trade Law under the framework of International Trade Law. Drafted in July 1998 by the Department of Electronics (DoE), this legislation represented a crucial step forward in regulating digital transactions. However, it wasn't until the creation of a new Ministry of Information Technology on 16 December 1999 that the process gained momentum. The legislation's development was influenced by various factors, including issues related to e-commerce and compliance with World Trade Organization (WTO) obligations, which were becoming increasingly critical in the global trade landscape.

The draft of the IT Act faced considerable debate when introduced in Parliament. After consultations and recommendations from various Members of Parliament, it was referred to the 42-member Parliamentary Standing Committee for further evaluation. One highly discussed proposal was the requirement for cybercafé owners to maintain a registry of visitors, recording both their identities and addresses, as well as the websites they accessed. This measure was intended to curb cybercrime by allowing law enforcement to quickly trace cybercriminals. However, it faced backlash for infringing on individual privacy and being

overly cumbersome to enforce. As a result, the IT Ministry ultimately removed this provision from the final version of the draft.

The introduction of the Information Technology Act and its subsequent amendments, such as the 2009 revision, have been pivotal in shaping the legal landscape regarding digital privacy, cybersecurity, and e-commerce. The Act, by recognizing data confidentiality as a fundamental aspect of privacy rights, set a precedent for subsequent data protection efforts. In light of the rapid technological changes since its inception, the IT Act has undergone continuous amendments to address new challenges, including data breaches, cyber fraud, and the ethical use of technology in commerce and communication. These legal frameworks have not only shaped the regulatory environment within India but have also aligned with global standards, ensuring India's participation in the global digital economy.

Additionally, with the rise of artificial intelligence (AI), blockchain, and the Internet of Things (IoT), the scope of technology law is expanding rapidly. These emerging technologies bring forth new legal challenges in areas such as intellectual property, data sovereignty, and digital ethics. Understanding the evolution of technology law, from its early stages to its current complexities, is crucial for policymakers, businesses, and individuals navigating the digital world.

EVOLUTION OF TECHNOLOGY LAW

The rise of networked personal computers has disrupted the long-standing structure of information production and exchange, a structure that has been stable for over 150 years. Although it is difficult to pinpoint an exact figure, estimates suggest that between 600 million and one billion people globally now possess the essential physical tools needed to generate knowledge, information, and culture, thereby enabling their participation in the global economy that revolves around these elements.

Nearly a billion individuals now have the capability and freedom to choose whether they want to contribute to knowledge or culture, as they already possess the necessary physical resources along with human intuition, creativity, and wisdom. There’s no longer a need to develop a formal business plan to write software that meets their personal needs. If they know how they can simply create it and collaborate with others who share the same goals to improve the software further.

This concept is exemplified by the overwhelming success of free and open-source software. Over a million developers actively contribute to tens of thousands of projects, many of which are integral to Internet communication. Some of these open-source projects have even faced competition from proprietary software companies but have prevailed, ultimately establishing themselves as essential components of the digital ecosystem.

Additionally, platforms like Wikipedia, where over thirty thousand people collaborate to build a free online encyclopedia, serve as alternatives to other digital encyclopedias, although they may not yet surpass established sources like the Encyclopedia Britannica. Numerous examples already exist, and there are strong economic models to explain why peer production and the generation of common information thrive in a networked information environment.

HOW IS TECHNOLOGY LAW HELPING THE SOCIETY?

The law in society goes beyond merely regulating behaviour—it is designed to implement social programs that benefit individuals and communities. For instance, certain laws provide compensation for workers injured on the job, offer healthcare services, and enable students to access financial aid to attend universities they might not otherwise afford.

One key aim of the law is to ensure fairness, meaning that fundamental personal rights and freedoms—such as liberty and equality—are upheld and protected. The law also works to prevent powerful individuals or groups from exploiting weaker ones through their positions of dominance in society.

As seen with the right to privacy, which has been redefined by advancements in information technology, technology has the potential to alter the scope of protected legal interests. The concept of "technological convergence" in telecommunications, for example, has eliminated the elements that previously made the industry a natural monopoly. This has opened the market to more competition and encouraged free-market principles. Similar dynamics can be observed in the legal framework, such as the distinction between Articles 15 and 21 of the Italian Constitution, particularly when balancing issues of freedom and secrecy.

Furthermore, the law can leverage new technologies to achieve goals that were previously met through traditional means. For instance, e-documents, e-signatures, electronic payments, and the completion of contracts in digital form are all examples of how new regulations allow the use of digital tools to achieve the same objectives that were once fulfilled by other methods.

Technological rules are often shaped by the unique characteristics of these new technologies. For example, there is a difference between creating laws that govern physical materials (atoms) and those that regulate digital information (bits). In some cases, legal concepts that traditionally apply to tangible items, such as ownership and possession, must be reimagined, or entirely new concepts must be created, such as "title" and "legitimization" in the context of digital financial instruments.

In the past, technology played a key role in the development of new products, which eventually led to the creation of new intellectual property rights, often following lengthy procedures. In recent years, we've seen this with databases (and even human tissue databases, among others). The law must constantly adapt to regulate new, previously unknown commodities. Technological advancements also influence the source and structure of laws, with legal systems sometimes opting to regulate emerging issues through international agreements or non-binding regulatory frameworks, such as codes of conduct.[1]

ROLE OF DATA IN TECHNOLOGY LAW OF INDIA

Data surrounds us in almost every aspect of our lives, generated through everything we do. Whether we travel, place an order, or transport a meal, we intentionally or unintentionally create data. This data can be of significant value, making it highly sought after by various organizations that are ready to invest in strategic data acquisition. In today's technologically advanced world, data has become the new currency. Despite the increasing awareness of its importance, the full potential of data is yet to be fully understood. New technologies and applications are continuously being developed to further enhance its value. This leads to several critical questions: Who truly owns the data? Who should have access to it? What are the boundaries on how such data should be used? These are issues that legal professionals across the globe are still grappling with in an effort to better understand and regulate data-related matters.

As data becomes increasingly valuable, governments worldwide are also seeking access to it for both public and national interests. However, this raises important questions about individual privacy. Should data be made available to support essential services or government functions like travel and security? Should national security concerns override individual privacy rights?

[1] Nabarun Chandra Ray, 'Law and Technology', Lawctopus, (Dec., 23, 2014) https://www.lawctopus.com/academike/law-andtechnology/ accessed 29 August, 2021.

On 24 August 2017, the Supreme Court of India ruled that the right to privacy is a fundamental right under Part III of the Indian Constitution. This landmark ruling established a foundation upon which future laws and regulations could be built. Any new legislation would now need to be scrutinized against the criteria of whether it infringes on an individual's personal freedom, as protected by Article 21 of the Constitution. While the decision was a major step forward, many questions remain about the limitations and scope of privacy rights.

India, at present, does not have a comprehensive data protection or privacy law. The existing legal framework is primarily sectoral, with laws such as the Information Technology Act, of 2000, outlining rules for the collection, use, and protection of sensitive personal data. However, this law alone is insufficient in addressing the growing complexities surrounding data privacy and protection in the modern world. Recognizing this, the Indian government has been working on drafting more detailed legislation to enhance data protection.

Further efforts are required, as highlighted by a 2012 report led by Justice A.P. Shah, a former Chief Justice of the Delhi High Court, which recommended significant improvements in privacy regulations. The government also appointed an expert committee, chaired by Justice B.N. Srikrishna, a former Supreme Court judge, to review data protection issues and provide recommendations for a robust legal framework.

In mid-2018, the Srikrishna Committee submitted its report, and around the same time, the Telecom Regulatory Authority of India (TRAI) issued a discussion paper addressing privacy, data ownership, and security concerns within the telecommunications sector. Additionally, the Reserve Bank of India's Committee on Budgetary Funding proposed a data protection framework based on rights, moving away from the traditional reliance on consent as the primary mechanism for data protection.

Given that data is constantly being generated by our actions, its protection has become increasingly crucial, especially considering rising data breaches and security threats. As a result, the need for updated legislation to safeguard individuals' and organizations' digital information has become more urgent. In India, lawmakers are continuously striving to address privacy concerns as new laws are introduced and existing regulations are refined.

The question of whether the "right to privacy" is a fundamental right in India has been examined by the Supreme Court in multiple cases. One of the early cases was M.P. Sharma &

Ors. Vs Satish Chandra, District Magistrate (1954)[2], in which the court considered whether search and seizure under sections 94 and 96 of the Code of Criminal Procedure infringed upon fundamental rights. The Supreme Court held that such powers of search and seizure, granted by law, did not violate any constitutional rights.

Another case, State of Uttar Pradesh vs Kharak Singh (1963)[3], further explored whether surveillance of a suspect violated Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty. The court ruled that night-time visits to a suspect's house constituted an infringement of privacy. However, the majority opinion held that Article 21 could not be broadly interpreted to include an explicit right to privacy.[4]

The Information Technology Act, of 2000 was introduced primarily to give legal recognition to e-commerce in India. Much of the Act focuses on the establishment of digital certification processes within the country. However, it falls short in addressing broader cybercrime issues, as it only briefly touches upon crimes related to computers without delving into the full spectrum of online offences.

THE AMENDMENT TO THE INFORMATION TECHNOLOGY ACT ENTERED INTO FORCE IN FEBRUARY 2009 WITH THE PRESIDENTIAL ASSENT COMPRISES THE FOLLOWING IMPORTANT FEATURES:

The amendments made to the Information Technology Act, which came into effect in February 2009 following presidential approval, brought about several significant changes:

• The modifications to Section 43 of the IT Act, 2000, introduced provisions where a person is liable to pay compensation of up to five crore rupees for failure to implement adequate security measures while dealing with sensitive personal information. This applies when such negligence results in wrongful loss or gain.

• Section 66 was updated to encompass offences mentioned in the revised Section 43, with penalties that can include imprisonment of up to three years, a fine of up to five lakh rupees, or both. This marked a shift from the earlier stance, where only imprisonment was prescribed for

[2] Mr. P. Sharma and Mr. Ors v Satish Chandra, 1954 SCR 1077.
[3] State of Uttar Pradesh and Ors vs Kharak Singh, 1964 SCR (1) 332.
[4] Rishabh, 'A critical analysis on Data Protection and Privacy Issues in India' Legal Services India, accessed 29 August 2021.

introducing malware into a system.

• Though not explicitly mentioned, the provisions under Section 66A could be interpreted in this context. Sending threatening, offensive, or false messages now carries a penalty of up to three years in prison along with a fine.

• A new Section 66B was added to address the fraudulent receipt and retention of stolen computer resources, punishable with imprisonment of up to three years or a fine of one lakh rupees, or both.

• Unauthorized use of another person's digital signature is now punishable by imprisonment of up to three years, along with a fine of up to one lakh rupees. Computer-related fraud is also penalized with imprisonment of up to three years and a fine extending to one lakh rupees (Section 66D).

• Section 66F was newly introduced to cover acts of cyber terrorism, which pose a threat to India's unity, integrity, and sovereignty, or harm its citizens. Acts covered under this section include:

1. Denial of access to critical national resources.
2. Attempting to gain unauthorized access to or exceeding permitted access to computer systems.
3. Introducing computer contaminants with the intent to cause injury, death, property destruction, or disruption of essential services for the public, or obtaining restricted data related to national security or foreign affairs. Thoffencesnses carry a maximum penalty of life imprisonment. The rise of cyber terrorism in India, particularly in the wake of incidents like the 2008 serial blasts in Ahmedabad, Delhi, Jaipur, and Bangalore, and the Mumbai attacks (26/11), has made this a critical area of concern.

• One significant change was the introduction of inspectors as investigating officers for offences covered under the Act (Section 78). Previously, only officers of the rank of Deputy Superintendent of Police or higher could conduct investigations, which limited the number of cases that could be addressed. This amendment is expected to increase the number of cases investigated by law enforcement.

• All offences punishable with three or more years of imprisonment have now been made cognizable. Even offences with a penalty of three years are no longer bailable (Section 77B). While this is a welcome change, there is still a need to ensure that only serious offences like cyber terrorism, child pornography, and intermediary liability are treated with such severity.

• Section 69 of the IT Act, 2000, was amended to allow the government to intercept and monitor cyber communications to combat cyber terrorism. The government now has the authority not only to monitor traffic but also to block websites through intermediaries. Failure to comply by intermediaries can lead to a penalty of seven years in prison and fines (Section 69(4)). This provision previously did not mention any fines.

SHORTCOMING IN THE INFORMATION TECHNOLOGY ACT, 2000

While the IT Act provides a legal framework for cyberspace and addresses some immediate concerns related to technology misuse, there are several gaps that remain unaddressed. According to legal experts like Supreme Court advocate and cyber law activist Pavan Dugga[5]l, the law lacks adequate teeth to effectively deter and punish offenders who misuse cyberspace. Several critical issues need further attention:

- **Spam**

Spam refers to unsolicited bulk email. Initially viewed as a mere nuisance, spam has now evolved into a serious economic problem. The absence of strong legal protections against spam is a notable shortcoming of the IT Act. Countries like the USA, EU, and Australia have stringent anti-spam laws, with Australia imposing fines of up to $1.1 million per day on spammers.

- **Phishing**

Phishing is a fraudulent method of obtaining sensitive information such as usernames, passwords, or credit card details by impersonating a trusted entity. This practice, typically carried out through emails, deceives users into divulging personal information on fake websites. Although phishing is a form of social engineering fraud, there are no specific provisions in the IT Act to address this issue. A recent phishing attack targeting State Bank of

[5] Parthsarthy&A.S.Pati, 'I.T. Act Its Strength and Short Comings, Overview and Suggestion for Amendments - Information Technology Act' Legal Service India acc essed on 30 August 2021

India (SBI) customers through a fake SBI website underscores the need for stronger legal measures against phishing.

- **Data Protection in Internet Banking**

Data protection regulations are essential to safeguard the rights of individuals whose information is processed by third parties. Internet banking, for instance, involves multiple parties beyond just the banks and their customers. Banks deal with a vast amount of customer data, and there is a high risk of data breaches. While the IT Act addresses unauthorized access to computer systems, it does not impose specific obligations on banks to protect customer data. By contrast, the UK introduced a data protection law in 1998, which holds banks and other organizations accountable for any failure to secure sensitive information. In India, however, bank liability for data breaches would arise from contractual obligations rather than statutory requirements, as there is no comprehensive data protection law.

- **Privacy and Data Protection**

Data security and privacy have become critical issues in today's world, especially as information technology plays an increasingly vital role across personal, business, and professional domains. Several countries, including the European Union and the United States, have implemented strict regulations to safeguard personal data when it crosses borders.[6] In India, however, the absence of a dedicated privacy law has resulted in the loss of foreign investments and economic opportunities. This gap has also stunted the growth of electronic commerce. To address these concerns, it is crucial to enact laws focused on privacy and data protection, if not an entire legal framework. At a minimum, certain privacy safeguards should be embedded in existing statutes.

- **Identity Theft**

Identity theft is a growing global issue that the IT Act 2000 fails to sufficiently address. This poses a significant challenge for India, especially given its robust outsourcing sector where the protection of personal identities is crucial. There have been high-profile cases of identity theft, such as when UK clients' personal data was compromised by an Indian online marketing firm. To secure India's outsourcing industry, a strong legal framework against identity theft is

[6] HarisZargar, 'India's Information Technology Act has not been effective in checking cyber crime: Expert' DNA India (April 03 2021, 10:48 am) accessed on 30 Aug 2021.

urgently needed.

- **Cyber Warfare**

The IT Act 2000 lacks provisions addressing the growing threat of cyber warfare, an area of increasing concern in international law. Countries must adopt regulations to address this new form of conflict. India has already been the target of numerous cyberattacks, notably from China, whose hackers have been able to breach Indian firewalls with alarming ease. Furthermore, the 26/11 terrorist attacks involved the use of cyber intelligence to obtain sensitive information. Despite the seriousness of these breaches, the IT Act does not hold perpetrators accountable for these actions.

- **Copyright Violations and Downloading**

One of the most prevalent forms of cyber misuse today is illegal downloads, especially of films, through peer-to-peer networks. This rampant infringement of copyright laws remains difficult to control due to the sheer volume of offenders. While blocking websites is sometimes used as a countermeasure, this has been criticized as an infringement on freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. Additionally, the lack of clear definitions for terms like "due diligence" and "lack of knowledge" in the IT Act makes prosecution challenging.

- **Extraterritoriality**

One major shortcoming of the IT Act is its lack of extraterritorial reach. Although the legislation was enacted to tackle cybercrime as a global issue, it fails to account for the borderless nature of cyber threats, neglecting to impose territorial restrictions.[7]

INDIA ON GDPR FOR DATA PROTECTION LAW

Although the European Union has long acknowledged the right to data protection, India still lacks a comprehensive legal framework for personal data security. The IT Act 2000 focuses more on regulating cybercrime and intermediary responsibilities but includes some data protection provisions. For example, Section 43A provides compensation for damages caused by inadequate security measures in handling sensitive information. However, India currently

[7] Soumik Chakraborty and Sridhar Kusuman, 'Critical Aparaisal of Information Technology Act' Lawctopus, (Dec. 17, 2014) accessed on 30 August 2021.

relies on a fragmented system of sector-specific laws to address data protection and confidentiality issues.

In 2017, the Indian Supreme Court recognized the right to privacy as part of the fundamental right to life under Article 21 of the Constitution. The ruling highlighted that the patchwork approach to privacy laws is insufficient, calling for a more unified legal framework. The Data Protection Committee (DPC), formed by the government, has been tasked with developing a draft law, heavily influenced by the GDPR framework.

The new Data Protection Bill (DPB) presents challenges for businesses, which must adapt to the evolving regulatory environment and consider cost-benefit analyses before entering or exiting certain markets.[8] The bill aims to safeguard citizens' privacy rights by regulating the collection, storage, and use of personal data. However, the implications of the bill extend beyond privacy, affecting the core business models of digital companies that rely on the sale and exploitation of user data.

- **User Consent**

Under the DPB, companies are required to obtain explicit user consent before collecting personal data. The scope and purpose of data collection must be clearly communicated to users, and further consent is needed for any subsequent data processing. This requirement poses challenges for companies, particularly when they use data to generate new insights that fall outside the original user consent.

- **Ownership of Personal Data**

The DPB proposes that personal data should, in theory, be owned by the individual providing it. While this idea appears straightforward, its practical implementation may prove burdensome for digital enterprises. For example, users could request the deletion of their personal information once they stop using a service. In such cases, companies must not only remove the data from their own systems but also ensure that any third parties with access to the data do the same.

[8] Anirudh Burman, Will a GDPR style data protection law work for India, Carnegie India, (May, 15, 2019), accessed on 30 August 2021.

- **Categories of Data**

The DPB defines three classes of data: sensitive data, critical data, and general data. Sensitive data includes information related to finances, health, sexual orientation, caste, and religious beliefs, while critical data pertains to matters of national security. General data encompasses everything else. The bill mandates that sensitive and critical data be stored within India, although sensitive data can be processed abroad, provided that it is returned to India for storage. Critical data must remain within the country's borders at all times.

This localization requirement could increase operational costs for digital companies, disrupting global supply chains and potentially leading to the fragmentation of the internet, often referred to as the "splinternet."

- **Data Sovereignty**

The DPB grants the Indian government access to data stored domestically in the interest of national security. This represents a departure from the GDPR, which does not impose such restrictions. While the GDPR focuses on safeguarding personal data, the DPB treats this information as a national asset, allowing the government to access it under specific circumstances.

- **National Interests vs. Privacy**

Although the DPB emphasizes the importance of privacy, it also grants the government broad powers to override these rights in the name of national security or public health emergencies. For instance, government bodies may collect personal data without user consent in situations involving crime prevention, national security, or disease outbreaks. Critics argue that this could lead to misuse of personal data, with concerns that anonymized data could easily be re-identified.

Digital companies may need to significantly modify their practices to comply with the DPB's requirements, which differ from global privacy standards.

CONCLUSION

The 2008 amendments to the Information Technology Act serve as a fitting example for evaluating cybercrime legislation and policy-making, highlighting the importance of precise

language, foresight, and thoughtful explanations in legal drafting. The gaps and resulting limitations of the law emphasize the critical need for criminal legislation, particularly regarding internet governance, to avoid ambiguous interpretations. This is especially important given the unique nature of cyberspace, which allows certain freedoms that can facilitate illegal activities.

While the IT Act aimed to curb the rising tide of cybercrime and make it more challenging for offenders to operate, the irony lies in the unintended consequence it created. Rather than merely making it harder to be a cybercriminal, the law has, in some instances, made it easier for individuals to be labelled as criminals. Both scenarios present significant risks, and careful attention must be given to the way cybercrime laws are interpreted and enforced.