International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

Beyond the Firewall: A Modern Analysis of India's Legal Framework for Cyber Sovereignty and Digital Rights

Baibhaba Chinhara[1], Ashutosh Kumar[2]

[1]2nd year L.L.M. student, G.M. Law College, Puri, Near Sri Vihar, Pin-752003
[2]1st Year LLM student, G.M. Law College, Puri, Near Sri Vihar, Pin-752003

***Abstract*— With a primary focus on the Information Technology (IT) Act of 2000 and the comprehensive IT Amendment Act (ITAA) of 2008, this study critically analyzes the development and state of cyber legislation in contemporary India. Strong legal frameworks are required since conventional crime has crossed geographical boundaries as fast digitalization incorporates technology into daily life. The paper examines the background of India's IT laws, emphasizing the fundamental objectives of its legal recognition of digital signatures, e-governance, and electronic commerce. Critical statutory provisions are systematically examined, such as Section 43's civil liabilities for data theft, Section 43A's reasonable corporate security practices, and Sections 66 and 67's severe penalties for offenses like identity theft, cyberterrorism, and the transmission of explicit content. The study also assesses the broad authority given to authorities for data monitoring and interception (Section 69) in comparison to the intermediaries' due diligence and compliance requirements. The study concludes that a cooperative effort among regulators, intermediaries, and users is crucial for fostering a secure digital environment. Lastly, it addresses important legislative gaps, specifically a pervasive lack of legal awareness and ongoing ambiguities regarding jurisdictional boundaries in cyberspace.**

***Keywords*— Cyber Law, Information Technology Act 2000, Cybercrime, Data Security, Intermediary Liability, Digital Jurisdiction.**

I. INTRODUCTION

Crime is a social and economic phenomena. It predates human civilization. Numerous ancient texts, dating back to prehistoric times, as well as legendary tales, discuss crimes committed by people, whether they are against the nation (such as treason and spying) or against another person (such as common theft and burglary). Written circa 350 BC, Kautilya's Arthashastra is regarded as a genuine administrative treatise in India. It addresses a variety of crimes, security measures that the rulers should take, potential crimes in a state, etc., and it also recommends punishment for a number of specified offenses. For certain offenses, a variety of penalties have been mandated, and the idea of compensating victims for their losses has also been covered. Any kind of crime has a negative impact on every individual in the community. Because of the Internet's quick spread and the digitization of business operations, cybercrime has grown significantly in emerging nations. We see computers and other electronic gadgets permeating human existence because of the enormous penetration of technology in nearly every aspect of society, from corporate governance and governmental administration to the lowest level of petty store owners computerizing their invoicing system.

Man cannot go a day without using a computer or a mobile device due to the widespread infiltration. Taking someone else's phone is the same as putting them in solitary confinement! The Information Technology Act of 2000, the IT Amendment Act of 2008, and no other Indian law define cybercrime. Actually, it can not be either. The Indian Penal Code, 1860, as well as a number of other laws, deal with offenses and crimes in detail, outlining different acts and their associated penalties. Therefore, we may simply describe cybercrime as a mix of computer and crime. "Any offense or crime in which a computer is used is a cybercrime," to put it simply. It is interesting to note that even minor crimes like pickpocketing or theft can fall under the larger category of cybercrime if the fundamental information or support for the crime is a computer or data saved on a computer that the fraudster uses (or abuses). We will now go into more depth regarding the I.T. Act, which defines a computer, computer network, data, information, and all other essential components of a cybercrime. A computer or the data itself is the goal or object of the crime in a cybercrime, or it may be used as a tool to perpetrate another crime by supplying the inputs required for that crime. All of these crimes will fall under the more general category of cybercrime

II. INDIA'S HISTORY OF IT LAW CREATION

Globalization and computerization gained momentum in the mid-1990s, as more countries

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

computerized their government and e-commerce experienced a meteoric rise. Up until that point, the majority of international trade and transactions were conducted only by telex and postal mail. Up until that point, the majority of evidence and documents were either paper records or other physical copies. Recognizing electronic records, or the data saved in a computer or an external storage device linked to it, became urgently necessary as a result of the fact that a large portion of international trade is conducted through electronic communication and that email is becoming increasingly popular. The Model Law on E-Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996. In January 1997, the UN General Assembly passed a resolution, among other things, urging all UN member states to give the aforementioned Model Law favourable consideration. This law recognizes electronic records and accords them the same treatment as paper communications and records.

III. The Goals of India's IT Legislation

According to the preface of the Act, the Government of India enacted the Information Technology Act 2000 with the following goals: "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies, and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891, the Reserve Bank of India Act, 1934, and for matters connected therewith or incidental thereto." As a result, the Information Technology Act, 2000 was approved as Act No. 21 of 2000, received the president's assent on June 9, and went into force on October 17, 2000. In essence, the Act addresses the following problems:

- Electronic Documents' Legal Recognition
- Legal Acceptance of Electronic Signatures
- Violations and Offenses
- Cybercrime Justice Dispensation Systems.

IV. The 2008 IT Amendment Act

The Act, which was the first piece of legislation in the country pertaining to technology, computers, e-commerce, and e-communication, was the focus of lengthy discussions, in-depth analyses, and detailed criticisms. One sector of the industry claimed that some of the Act's provisions were too harsh, while another said they were too lenient and diluted. Additionally, there were several glaring gaps that led to investigators increasingly depending on the tried-and-true Indian Penal Code, which is 150 years old, even in instances involving technology and the Internet of Things. In the process, the Act is also brought up, and the IPC is cited more often than the ITA. As a result, the I.T. Act needed a comprehensive update relatively immediately in 2003–2004. In order to investigate the alleged shortcomings in the I.T. Act, compare it with comparable laws in other countries, and provide recommendations, advisory committees were established and major business bodies were engaged. These suggestions were examined and then adopted as a comprehensive Amendment Act. Following extensive administrative processes, the Information Technology Amendment Act 2008 was introduced in Parliament and passed with little discussion towards the end of 2008 (by which point the 26 November Mumbai terrorist attack had occurred). This Amendment Act became operative on October 27, 2009, after receiving the President's assent on February 5, 2009.

The following are some of the ITAA's noteworthy characteristics:

- Putting data privacy first
- Putting Information Security First
- What is a cybercafe?
- Ensuring the neutrality of digital signature technology
- Outlining appropriate security procedures that corporations should adhere to
- Redefining middlemen' roles
- Understanding the Indian Computer Emergency Response Team's mission
- Adding a few more cybercrimes, such as child pornography and cyberterrorism, and giving an inspector the authority to look into these offenses (as opposed to the DSP previously)

V. The IT Act's Structure

The Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934 were amended in the final four parts (sections 91 to 94 in the ITA 2000). The Act is divided into thirteen chapters and ninety sections. The Act starts with introductory definitions and then moves on to parts that address digital signatures,

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

electronic record authentication, and other topics. Comprehensive protocols have been established for certifying authority (for digital certificates under the IT Act 2000, which have subsequently been superseded by electronic signatures under the ITAA 2008). Data theft is a civil offense, and the adjudication and appeals processes have been explained. The Act then goes on to list some of the most well-known cybercrimes, define them, and specify the associated penalties. After that, the idea of due diligence, the function of middlemen, and a few more clauses were explained. The Act's rules and procedures have also been established gradually; the most current one, which defines private and sensitive personal data, the role of intermediaries, due diligence, etc., was only established in April 2011. Later in this chapter, we will also go over some of the key clauses of these regulations.

VI. Data Security and E-Governance

The legal recognition of electronic records is covered in detail in Section 4 of Chapter III's discussion of electronic governance issues and procedures. This is followed by a description of procedures pertaining to the storage, upkeep, and validity of contracts formed through electronic means. The following sections contain procedures pertaining to electronic signatures as well as regulatory standards for certifying agencies. Chapter IX, which deals with Penalties, Compensation, and Adjudication, is a crucial step for preventing data theft, making compensation claims, introducing security measures, and other topics covered in Section 43, all of which merit further explanation. Penalties and compensation for damage to computers, computer systems, etc. are covered in Section 43. This part is India's first serious legislative move to address the problem of data theft. Like physical theft or larceny of goods and commodities, the IT industry has long called for legislation in India to combat the crime of data theft. The civil offense of data theft is covered in this section. If someone accesses, downloads, copies, or extracts any data without the owner's or another person in charge of a computer's permission, introduces a computer contaminant like a virus, damages or disrupts a computer, denies access to a computer to an authorized user, tampers, etc. He will be responsible for compensating the harmed party. The maximum damages under this head were previously limited to Rs. 1 crore under the ITA-2000; this threshold was later lifted in the ITAA 2008. Civil responsibility is the main focus of this section. Data theft is a crime that will be addressed individually in Sections 65 and 66. This section covers the creation of virus programs, the dissemination of viral emails, the use of bots, Trojan horses, or other malware in computer networks, as well as the creation of Denial-of-Service attacks on servers that result in legal liability and compensation. Terms like "computer virus," "compute contaminant," "computer database," and "source code" are all defined and explained within this section. During the first few years of ITA-2000, the concept of due diligence, the extent of the employer's or owner's responsibility, and the employees' liability in an organization sued for data theft or similar offenses were all discussed in court cases such as the Bazee.com case. The necessity to define corporate liability for data protection and information security at the corporate level was then recognized and given careful consideration. As a result, the ITAA-2008 created the new Section 43-A, which deals with compensation for failure to protect data. In terms of data protection, particularly at the business level, this is yet another turning point. According to this section, if a body corporate fails to adopt appropriate security procedures and causes someone to suffer an unjustified loss or gain, that body corporate will be responsible for compensating the affected person for damages. The terms "body corporate" and, more importantly, "reasonable security practices and procedures" and "sensitive personal data or information" are further explained in this section. Appropriate Security Procedures

- Certification of the site
- Initiatives for security
- Training in Awareness
- Standards compliance and certification
- Rules and following them
- Email policies, password policies, access control policies, and so forth
- regular observation and evaluation.

Information technology (sensitive personal data and information, as well as reasonable security methods and processes) Since then, on April 11, 2011, the Government of India, Department of IT, has issued regulations. A corporate entity or an individual acting on its behalf will be deemed to have adhered to reasonable security practices and procedures if they have put these standards and practices into practice and have a well-documented information security program and information security policies that include managerial, technical, operational, and physical security control measures appropriate for the type of business and the information assets being safeguarded. As and when called upon by the

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

legally mandated agency, the body corporate or an individual acting on its behalf must prove that they have put security control measures in place in accordance with their documented information security program and information security policies in the event of an information security breach. One such standard mentioned in sub-rule (1) is IS/ISO/IEC 27001, an international standard on "Information Technology – Security Techniques - Information Security Management System - Requirements". Given the aforementioned, it has now emerged as a significant compliance concern for IT firms as well as those in the banking and financial sector, particularly for banks that rely significantly on technology and have extensive computerized operations handling public data. It would be the great responsibility of those corporate entities to demonstrate that the aforementioned "Reasonable Security Practices and Procedures" were in fact in place and that all of the actions outlined in the Rules passed in April 2011 had been taken in the event of a lawsuit or security breach that resulted in a claim for damages or compensation of a monetary loss amount.

VII. Penalties and Verdicts

After discussing civil offenses, the Act elaborates on the adjudication process as a civil remedy for such offenses, which eliminates the need to file a complaint with law enforcement or other investigative bodies. Sections 46 and later provide a detailed description of adjudication authorities and procedures. Any official not lower than a director of the Indian government or a state government may be appointed as the adjudicator by the central government. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. This clause is the only part of the IT Act that can be said to be completely unpopular. Only a small number of applications have been filed nationwide in the first 10 years of the ITA's existence, and practically all of them are in various stages of the legal process. In less than five cases, adjudications have likely been achieved. The first ruling under this clause was made in a case involving ICICI Bank in Chennai, Tamil Nadu, in April 2010. The bank was ordered to reimburse the applicant for the money that was incorrectly deducted from their Internet banking account, in addition to costs and damages. The public, particularly those who have been the victims of cybercrimes and data theft, should be made aware of this section's existence and the fact that there is an alternative to going to the police and making a complaint. In order for the litigant public to fully exploit the beneficial provisions that have been implemented, the state should invest some time and consideration in raising awareness of the adjudication provisions for civil offenses in cyber litigations, such as data theft, etc. This process includes an appeals mechanism, and the Act also describes the national Cyber Appellate Tribunal's membership. The Cyber Appellate Tribunal has the same authority as a civil court under the Code of Civil Procedure, and each adjudicating officer has the same authority as a civil court. The Act then discusses the actual criminal activities that fall under the more general definition of cybercrimes after going over the procedures pertaining to appeals, etc., as well as the responsibilities and authority of the Cyber Appellate Tribunal. It is important to remember that the Act simply specifies a few cybercrimes—it does not define any—and outlines the penalties for these offenses. Chapter IX, "Offences," contains the criminal provisions of the IT Act as well as those pertaining to crimes and cognizable offenses.

In the past, hacking was prohibited by Section 66. Following the modification, Sec. 66 now refers to data theft of Sec. 43, giving it greater meaning and removing the word "hacking." Previously, the term "hacking" was considered a crime in this section, and academic courses on "ethical hacking" were also offered at the same time. This resulted in an unusual circumstance where people asked how an illegal behaviour with the word "ethical" attached could be taught academically. Can there be classes on physical defense, for example, or training programs on "Ethical burglary," "Ethical assault," etc.? The ITAA ended this complex situation by rewording Section 66, deleting the word "hacking," and connecting it to the civil culpability of Section 43. Though some experts view "hacking" as typically for good purposes (clearly to facilitate the labelling of the courses as ethical hacking) and "cracking" as generally for unlawful purposes, hacking is nonetheless unquestionably an offense under this section. It is important to remember that the technology and the conduct are the same, but in "hacking," the owner's permission is sought or presumed, while in "cracking," the act is seen as illegal. Thanks to ITAA, Section 66 has been expanded to include the following list of offenses:

A. 66A:

This section covers sending inflammatory communications via communication services, annoying people, etc., or sending an email that misleads or deceives the receiver about where the message originated (sometimes referred to as IP or email spoofing). These

offenses carry a maximum sentence of three years in jail or a fine.

B. 66B:

Receiving a stolen computer resource or communication equipment dishonestly is punishable by up to three years in prison, a fine of one lakh rupees, or both.

C. 66C:

Identity theft, including the use of someone else's password or electronic signature. Three years in prison, a fine of one lakh rupees, or both might be the punishment.

D. 66D:

Cheating by personation utilizing a computer resource or communication device is punishable by up to three years in prison of any kind and a fine of up to one lakh rupees.

E. 66E:

Violation of privacy: Disseminating or publishing someone else's private information without that person's permission, etc. Three years in prison, a fine of two lakh rupees, or both are the possible penalties.

F. 66F:

Cyberterrorism is defined as having the intention of endangering the nation's unity, integrity, security, or sovereignty by preventing anyone who is authorized from using a computer resource or by attempting to access or breach a computer resource without authorization. This section covers acts that result in a computer contamination (such as a virus, Trojan Horse, or other spyware or malware) that could kill or injure people, damage or destroy property, etc. Life in jail is the penalty.

It is evident that all offenses under S.66 are punishable by law and do not require bail. The main components to bring any act under this section include destruction, deletion, alteration, or decrease in value or utility of data, as well as the knowledge or intention to cause unjust loss to others (i.e., the existence of criminal intention and the wicked mentality, i.e., mens rea). In summary, what was meant by civil liability with the right to damages and compensation under Section 43 has been alluded to here. If it is committed with criminal intent, it is a criminal liability that carries a fine and/or imprisonment.

Publishing or sending pornographic content electronically is covered under Section 67. The ITAA 2008 expanded the previous ITA section, adding provisions for child pornography and intermediary record keeping. This section deals with the publication or transmission of pornographic content in electronic format. A first conviction carries a maximum sentence of three years and a fine of five lakh rupees; a second conviction carries a sentence of five years and a fine of ten lakh rupees, or both, for publishing or transmitting any material that is lewd, appeals to the prurient interest, or has the potential to corrupt and deprave those who are likely to read the content. Since the momentous ruling in what is regarded as the first conviction under IT, this section has historical significance. In the well-known case of "State of Tamil Nadu vs. Suhas Katti" on November 5, 2004, the Indian Act 2000 was secured in this section. In this case, which involved sending obscene messages in the name of a married woman, the prosecution demonstrated the Section's strength and the validity of electronic evidence, leading to a conviction. This case involved email spoofing, cyberstalking, and other criminal activities listed in this Section. The publication or transmission of content in electronic form that contains sexually explicit acts is covered by Section 67-A. When content from Section 67 is mixed with sexually explicit content, this Section penalizes the combination. Section 67B is the only law that addresses child pornography. This section covers things like showing children performing sexually explicit acts, producing text or digital images, advertising or promoting such content, or showing children in an offensive or degrading way, among other things. It also covers things like encouraging child abuse online or getting kids involved in relationships with other kids online. People who have not reached the age of eighteen are considered "children" for the purposes of this section. First-time offenders face a maximum sentence of five years in prison and a fine of ten lakh rupees. Second-time offenders face a maximum sentence of seven years in prison and a fine of ten lakh rupees. In order to prevent the printing and distribution of ancient epics, heritage material, or pure academic books on education and medicine from being unduly impacted, authentic heritage material that is printed or distributed for the purpose of education, literature, etc. is expressly excluded from the coverage of this section. This includes creating pornographic film or MMS clippings or disseminating them via mobile devices or other Internet-based communication channels, as well as screening images and videos of illicit activity. In accordance with Section 67-C, intermediaries are required to maintain and retain information for the time and in the way that the Central Government specifies. Failure to comply can result in a fine or up to three years in prison.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

VIII. Transmission of Electronic Communications and Messages

As long as the steps mentioned here are followed, Section 69 allows the government or agencies named in it to intercept, monitor, or decrypt any data produced, transferred, received, or stored on a computer resource. This makes it an interesting section. This authority may be used if the Central Government or State Government, as the case may be, is convinced that it is required or advantageous for the protection of India's sovereignty or integrity, defense of India, security of the State, good relations with other countries, or public order, or for the investigation of any crime or for preventing incitement to commit any of the aforementioned crimes. In any of these situations, the required process must be followed, and the justification for the action must be documented in writing by an order instructing any relevant government agency. When asked to do so, the subscriber or middleman must provide necessary facilities and technical support. Under the same conditions as previously stated, the Central Government or any of its personnel may make orders to limit public access to any material via any computer resource under Section 69A, which was added to the ITAA. The authority to monitor and gather traffic statistics or information using any computer resource is covered in Section 69B.

IX. Authority to Monitor, Block, and Intercept Websites

In summary, the authority to intercept, monitor, or decrypt does exist within the circumstances specified in this section. Examining the history of telephone tapping in India, as well as the laws (or lack thereof) in our country, and contrasting them with the authorities listed below would be fascinating. Clause 5(2) of the Indian Telegraph Act of 1885, which stated that "On the occurrence of any public emergency, or in the interest of the public safety, the Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any individual or group of individuals or concerning any specific topic, presented for transmission by, transmitted by, or received by any telegraph, must not be forwarded, nor shall it be intercepted, held, or revealed to the government issuing the order or an official designated in the order. The government should develop "precautions to be taken for preventing the improper interception or disclosure of messages," according to other parts of the legislation. The creation of regulations to control the application of Clause 5(2) has been the subject of several attempts, if not petitions. However, no government has developed any such safeguards since 1885, maybe for the apparent reason of maintaining the ability to spy for over a century. The People's Union for Civil Liberties challenged the constitutionality of this Clause 5(2) in a 1991 writ petition submitted to the Supreme Court. The petition claimed that it violated the constitutional rights to life, liberty, and freedom of speech and expression. In its ruling in December 1996, the Supreme Court noted that "the authorities have no jurisdiction to exercise the powers" granted them under 5(2) "unless a public emergency has occurred or the interest of public safety demands." They continued by defining public safety as "the state or condition of freedom from danger or risk for the people at large" and public emergency as "the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action." No matter how "necessary or expedient," it could not succeed without the two. The layer of authorities, procedures for maintaining such documents, etc. were also outlined.

Now, compared to the Indian Telegraph Act of 1885's aforementioned clause, Section 69 of the ITAA is significantly more invasive and potent. Subject to following the guidelines and without a magistrate's order warrant, the designated government official will have the authority to monitor websites visited, listen in on all phone conversations, and read emails and SMSs under this ITAA Section. Given the aforementioned, this section was criticized for being harsh and giving the government far more authority than was necessary. However, we should not ignore the fact that the government, represented by the Indian Computer Emergency Response Team (the National Nodal Agency, as designated in Section 70B of ITAA), has hardly ever used this power (of intercepting, monitoring, and blocking). The CERT-In has said that it uses these powers extremely infrequently, if at all. This might be because it believes in the freedom of expression and trusts that the sector is self-regulatory.

X. Intermediary Guidelines and Due Diligence

Section 79 has addressed intermediary liability and the notion of due diligence. Accordingly, an intermediary will not be held responsible for any third-party information that he hosts if his role is restricted to

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

granting access to a communication system that transmits, stores, or hosts information made available by third parties; if he does not initiate the transmission; if he chooses the recipient of the transmission; and if he exercises due diligence and complies with the rules established by the Central Government.

The idea of due diligence is likewise hotly contested. Due Diligence was initially discussed as a direct result of the well-known bazee.com case in New Delhi, where the company's NRI CEO was arrested for selling an MMS clipping that contained offensive and obscene material of schoolchildren on his public domain website (and later the CD was sold). The main topic of discussion at the time was the extent of the content providers and ISP's responsibility, as well as the concept of due diligence, which the CEO of the firm ought to have practiced. On April 11, 2011, the DIT released a set of regulations known as the Information Technology (Intermediaries Guidelines) Rules in response to the ITAA's passage, the introduction of "reasonable security practices and procedures," the responsibility of body corporate as previously seen in Section 43A, and to clear up any confusion regarding the importance of due diligence and what constitutes due diligence. Accordingly, "the intermediary, on whose computer system the information is stored, hosted, or published, shall act within thirty-six hours and, if applicable, work with user or owner of such information to disable such information that is in violation of sub-rule (2) above, upon obtaining knowledge by itself or being brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above." Additionally, for the purpose of an inquiry, the intermediary must keep such data and related documents for at least ninety days.

Essentially, unless the intermediary can demonstrate that he has taken reasonable precautions and has not participated in or encouraged illegal activity, he will be held accountable for any legal violations done by any user. Section 80 describes the authority to enter, search, and so on. Any police officer, not less than the rank of Inspector or any other authorized officer, may enter any public place and search and arrest without a warrant any person found there who is reasonably suspected of having committed, committing, or about to commit any offence under this Act, regardless of what is stated in the Code of Criminal Procedure. Even though it is another powerful weapon, police officers have seldom ever used it. The Act applies to both electronic and truncated checks (i.e., the actual travel of the check from the collecting banker to the paying banker is curtailed and shortened by the image of the check being presented and processed). The following sections have covered the Act's overriding powers as well as the Central Government's and State Governments' authority to enact regulations as needed.

XI. Critical Thoughts on ITA and ITAA

Following a detailed review of each of the sections of the ITA and ITAA, let us look at some of the Act's more general commissions and omissions as well as the general criticism that the Acts have accumulated over time.

Awareness: The Act makes no real provisions for raising awareness or implementing such programs. Since this is a new field and technology needs to be learned by all stakeholders, including judicial officers, legal professionals, the litigant public, and the general public or users, the government or investigating agencies, such as the Police department (whose job has been made relatively easier and focused, thanks to the passing of the IT Act), have taken any significant steps to raise public awareness of the provisions in these legislations. Many people, even those in the investigative authorities, are unaware of regulations such as the extent of the adjudication procedure.

Jurisdiction: This is a significant problem that neither the ITA nor the ITAA adequately address. Sections 46, 48, 57, and 61 discuss jurisdiction in relation to the adjudication process and the appeal procedure associated with it. Section 80 also mentions jurisdiction in relation to police officers' authority to enter public spaces, search them for cybercrimes, etc. Sections 13(3) and (4) address the location of electronic record delivery and reception, which may be seen as jurisprudential concerns.

However, there are some basic concerns. For example, if someone is mail is hacked and the accused, who lives in a different state, finds out about it in a different city, which police station does he go to? Where does he go to file a complaint if he works for a multinational corporation that has offices across the globe and in numerous Indian cities, and he frequently travels within India, and he suspects someone else—say, another employee of the same company—in his branch or headquarters office and tells the police that there may be evidence in the suspect's computer system? For

jurisdictional reasons, investigators frequently reject such allegations, and court authorities have occasionally been reluctant to take on such cases. It is necessary to disseminate the information that cybercrime occurs in the "cloud" or "space" and is not limited by geography, borders, territory, jurisdiction, or boundaries. All relevant parties in the sector must get the necessary training.

XII. Conclusion

In conclusion, even if a society free from crime is utopian and only exists in the imagination, every effort should be made to enforce laws that will continuously reduce crime. Crime based on electronic offenses will inevitably rise, especially in a society that is becoming more and more reliant on technology. To keep fraudsters at bay, lawmakers must go above and beyond. Technology is always a two-edged sword that may be applied for both positive and negative ends. Technologies like steganography, Trojan horses, scavenging, and even DoS or DDoS are not crimes in and of themselves, but when they get into the wrong hands of criminals who want to profit from or abuse them, they fall under the category of cybercrime and become crimes. Therefore, leaders and legislators should keep working to make sure that technology develops in a healthy way and is utilized for legitimate corporate expansion rather than criminal activity. The three stakeholders—rulers, regulators, legislators, and investigators—should be responsible for it. Internet or network service providers, banks, and other intermediaries; and iii) users to manage information security by carrying out their individual responsibilities within the allowed bounds and guaranteeing adherence to national laws.

References

[1] Avnish Bajaj v. State (N.C.T.) of Delhi [Bazee.com case], 150 DLT 769 (Del. 2008).

[2] Indian Penal Code, No. 45 of 1860, India Code (1860).

[3] Indian Telegraph Act, No. 13 of 1885, India Code (1885).

[4] Information Technology Act, No. 21 of 2000, India Code (2000).

[5] Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009).

[6] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, G.S.R. 313(E) (2011).

[7] Kautilya. (1915). *Kautilya's Arthashastra* (R. Shamasastry, Trans.). Government Press. (Original work published ca. 350 B.C.E.).

[8] People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568 (India).

[9] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Addl. Chief Metropolitan Magistrate, Egmore 2004).

[10] United Nations Commission on International Trade Law. (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996*. United Nations.