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

Cybercrime in India: Insight Into the Extra-Territoriality of the Information Technology Act

S. Karpagapriya

M.L., Advocate, High Court of Madras.

Abstract

This article covers the ins-and-outs of cybercrime, its categorization and the space it occupies in India's ever-increasing cyberspace. It further explores the IT Act which till date serves as India's primary statute regulating the cyberspace and the crime therein. The article discusses the challenges posed by the advancement of technology that creates inefficiencies in the IT Act and hopes to provide substantial solutions to these issues.

Keywords: Cybercrime, Information Technology Act, Cyberspace.

"In the information-communication civilization of the 21st Century, creativity and mental excellence will become the ethical norm. The world will be too dynamic, complex, and diversified, too cross-linked by the global immediacies of modern (quantum) communication, for stability of thought or dependability of behaviour to be successful [1]."

Introduction and Categorizing Cybercrime

Multiple taxonomies have been suggested for categorising cybercrime. David Wall (2001) identified four categories of detrimental behaviour on the internet: Cyber-trespass, cyber-deceptions/thefts, cyber-pornography/obscenity, and cyber-violence are all forms of illicit activities that occur in the digital realm (Wall, David, 2007) [2]. Subsequently, he put out the notion that cybercrime can be categorised into three primary criminologies: crimes involving the integrity of computer systems, crimes facilitated by computers, and crimes related to computer material. Kirwan & Power (2013) categorise cybercrime into three distinct types: crimes targeting individuals in virtual spaces, offences facilitated by the Internet, and offences that are unique to the Internet [3]. The phrase 'old wine in new bottles' refers to the phenomenon where various forms of cybercrime have offline counterparts, but are now being carried out in a different environment (Viano, Emilio C, 2017) [4].

The following table contains the typology of cybercrime as prescribed in the COMPREHENSIVE STUDY ON CYBERCRIME, by the UNODC [5]:

[1] Leary, Timothy. Chaos & Cyber Culture. Grupo Editorial Norma, 1994.
[2] Wall, David. Cybercrime: The Transformation Of Crime In The Information Age. Vol. 4. Polity, 2007.
[3] Kirwan, Grainne, And Andrew Power. Cybercrime: The Psychology Of Online Offenders. Cambridge University Press, 2013.
[4] Viano, Emilio C. "Cybercrime: Definition, Typology, And Criminalization." Cybercrime, Organized Crime, And Societal Responses: International Approaches (2017): 3-22.
[5] Comprehensive Study On Cybercrime, UNODC, United Nations Office On Drugs And Crimes, Pg. 16, Https://Www.Unodc.Org/Documents/Organized-Crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.Pdf

Acts against the confidentiality, integrity and availability of computer data or systems	Computer-related acts for personal or financial gain or harm	Computer content-related acts
Illegal access to a computer system	Computer-related fraud or forgery	Computer-related acts involving hate speech
Illegal access, interception or acquisition of computer data	Computer-related identity offences	Computer-related production, distribution or possession of child pornography
Illegal interference with a computer system or computer data	Computer-related copyright or trademark offences	Computer-related acts in support of terrorism offences
Breach of privacy or data protection measures	Sending or controlling sending of Spam	
	Computer-related acts causing personal harm	
	Computer-related solicitation or 'grooming' of children	

The following table highlights an Empirical Typology of Cybercrime (Jay Albanese, 2022) [6]:

1. Computer as Target	Freq.	Percent
a. Hack for information to use to defraud.	40	13.1
b. Hack for damage/malware/ransom	20	6.6
c. Hack to subvert government or infrastructure	13	4.3
2. Computer as Instrument		
a. Buy/sell illicit goods or services	121	39.7
b. Phishing for fraud victims	58	19.0
c. Transmit threats/extortion	53	17.4
Total cases	305	100 %

Introduction to the cyberspace in India

Due to the increasing advancements in technology, cyberspace has become an essential component of human existence. It has facilitated a wide range of activities, ranging from reserving a taxi through the internet to launching missiles capable of accurately striking targets. The 2007 cyber-attack on Estonia served as a catalyst for other countries, prompting them to recognise the significance of cyberspace and

[6] Jay Albanese, A Typology Of Cybercrime: An Assessment Of Federal Prosecutions, Vol. 6, Is. 2, Journal Of Criminal Justice And Law, 2022.1

its imperative for security (Chopra, Rohit, 2008) [7]. India's cyber defence capabilities have emerged a critical worry due to recent incidents such as the compromise of customer data in corporate businesses, the Mumbai power outage on October 12, 2020, and the malware attack at Kudankulam Power Plant in 2019 (Dilipraj, E, 2019) [8].

India's primary means to address cybercrimes

In 1996, the United Nations Commission on International Trade Law produced a model law on e-commerce and digital complexities (Blythe, Stephen. E, 2006) [9]. Additionally, it mandated that each country establish its own legislation regarding e-commerce and cybercrimes. The Act was enacted in 2000 to safeguard the data of both citizens and the government. This legislation positioned India as the 12th country globally to implement laws addressing cyber crimes. The IT Act, commonly known as the Information Technology Act, establishes the legal structure for safeguarding data pertaining to e-commerce and digital signatures. It underwent additional amendments in 2008 and 2018 to address the evolving societal requirements. The legislation also delineates the authorities and constraints of intermediaries (Basu Subajith & et. Al., 2003) [10].

Extra-territorial application of the IT Act

As per Section 1, the Act is applicable nationwide, encompassing the state of Jammu and Kashmir. This Act also has extraterritorial jurisdiction, meaning it applies to anyone who commit offences outside the country. If the origin of the offence, specifically a computer or similar equipment, is located in India, then the individual will be subject to punishment under the Act, regardless of their nationality [11].

Act to apply for offence or contravention committed outside India

A contravention is considered to have occurred outside of India if a person's actions or behaviour that constitute an offence or contravention involve a computer, computer system, or computer network located within India. Section 75 encompasses a wider scope that includes cybercrime perpetrated by cyber criminals of any nationality and in any geographical location (Pal Sayani, 2022) [12].

R v/s Governor of Brixton prison and another.

Here's what happened: Citibank experienced a serious breach in its cash management system, leading to unauthorised transfers of funds from customers' accounts to the hacker's accounts. The hacker responsible for this incident was Valdimer Levin, along with his accomplices. Following Levin's arrest, he was extradited to the United States. One of the key considerations revolved around the jurisdictional matter

[7] Chopra, Rohit. Technology And Nationalism In India: Cultural Negotiations From Colonialism To Cyberspace. Cambria Press, 2008.
[8] Dilipraj, E. "Supposed Cyber Attack On Kudankulam Nuclear Infrastructure—A Benign Reminder Of A Possibile Reality." Cent. Air Power Stud 129 (2019): 1-5.
[9] Blythe, Stephen E. "A Critique Of India's Information Technology Act And Recommendations For Improvement." Syracuse J. Int'l L. & Com. 34 (2006): 1.
[10] Basu, Subhajit, And Richard Jones. "E-Commerce And The Law: A Review Of India's Information Technology Act, 2000." Contemporary South Asia 12.1 (2003): 7-24.
[11] Pal, Sayani. "India's New IT Rules: An Analysis In The Background Of Fundamental Rights And Cyber Jurisdiction." Issue 3 Indian JL & Legal Rsch. 4 (2022): 1.
[12] Sumanjeet. "The State Of E-Commerce Laws In India: A Review Of Information Technology Act." International Journal Of Law And Management 52.4 (2010): 265-282.

of determining the "place of origin" of the cyber crime. The Court determined that the communication link between Levin and Citibank computer was in real-time, establishing that Levin's keystrokes were taking place on the Citibank computer. It is crucial to address the conflicts surrounding jurisdiction by adopting a more comprehensive approach that considers principles of reasonableness and fairness. This approach should aim to accommodate the overlapping or conflicting interests of states, in line with the concept of universal jurisdiction [13].

JCB Ltd. V. Abhinav Gupta

Section 81 of the Information Technology Act appears to relax the rigid requirement of enforcing the law within a particular jurisdiction with regards to the offences outlined in the Act and the amendments made by the IPC. (Retanlal, et. al., 1997) [14]. However, a compelling argument can be made for the expansion of the Act beyond national boundaries by examining the 'terminator' doctrine in American and English law, as well as the concept of 'consequence' outlined in section 179 of the Code of Criminal Procedure in India (Devashish Bharuka, 2002) [15].

Issues

The above two provisions clearly indicate that the offence, despite being committed outside of India, can be punished in India. Therefore, if a Nepalese individual residing in Canada were to engage in a Distributed Denial of Service attack targeting computer networks in India with the intention of disrupting Yahoo e-mail services, they could potentially face legal consequences under the IT Act if brought to trial in India. The above provisions have been formulated in a comprehensive manner. Some provisions of the Indian Penal Code also indicate that its rules can be applied to unlawful actions carried out outside of India, albeit with certain conditions. Section 2 of the Indian Penal Code focuses on the punishment of offences committed within India. This presents no issue. If a criminal act involving computers is committed within India, the provisions of the Code would be applicable to such acts. Section 3 of the Indian Penal Code states the punishment for offences committed outside of India but which can still be tried within the country according to the law. Any individual who is subject to prosecution under Indian law for a crime committed outside of India will be handled in accordance with the provisions of this Code, as if the act had taken place within India. This section will be relevant in a scenario where the individual, when committing the offence they are being charged with, falls under the jurisdiction of Indian courts. Section 3 of the IPC has a wide scope, encompassing individuals who may not be citizens of India but are subject to Indian law for actions carried out outside of India (Shelke, Atmaram et. al., 2019) [16].

Conclusionary Statement and the way forward:

The IT Act is the primary framework for digital governance in India. Nevertheless, it was implemented in 2000. Just to provide some context, back in 2000, only a mere 0.5% of the population, which was approximately 55 lakh people, were using the internet. BSNL was also established 4 months after the

[13] R V. Governor Of Brixton Prison, Ex Parte Levin, HL 10 Apr 1997
[14] Retanlal And Dhirajlal, The Indian Penal Code (Universal Publication, 29th Edn., 2002).
[15] Devashish Bharuka, "Indian Information Technology Act 2000; Criminal Prosecution Made Easy For Cyber Psychos" 44 JILI 354 (2002).

[16] Shelke, Atmaram, And Shashikala Gurpur. "Problem Of Jurisdiction In Cyberspace And Its Impact On International And Domestic Laws." Available At SSRN 3500049 (2019).

passing of the Act. It is evident that there is a pressing requirement to revise the Act in order to incorporate policy and legal advancements, as well as adapt to current technological circumstances. Both the USA and UK have signed this Convention, which encompasses a range of extraditable offences. These offences include violations against the confidentiality, integrity, and availability of computer data and systems, such as illegal access, interception, data interference, system interference, and device misuse. Additionally, the Convention covers computer-related crimes like fraud and forgery, content-related offences such as child pornography, and offences related to copyright and related rights infringements, as well as attempts and aiding or abetting [17].

In general, it appears that India's decision to join the Budapest Convention has been driven more by diplomatic and foreign policy factors rather than a genuine focus on enhancing criminal justice collaboration in cybercrime and e-evidence matters [18]. India is on the fast-track to become one of the biggest cyber-environments in the world, naturally exposing it to multitudes of cybercrimes. It is of utmost importance for India to ratify the Budapest convention, thereby, collaborating with other participating nations in making extensive regulations and robust safeguards to protect the expansive cyberspace.

[17] Convention On Cybercrime, ETS 185, Available At: Http://Www.Europarl.Europa.Eu/Meetdocs/ 2014_ 2019/Documents/Libe/Dv/7_Conv_Budapest_/7_Conv_Budapest_En.Pdf (Visited On April 8, 2017).
[18] Alexander Seger, India And The Budapest Convention: Why Not?, 14/7/23, Https://Www.Orfonline.Org/Expert-Speak/India-And-The-Budapest-Convention-Why-Not/