Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.755174

IOT, AI, AND BLOCKCHAIN: SHAPING THE FUTURE OF IT LEGISLATION IN INDIA

Bhushan
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida.
bhushanbajaj3992@gmail.com

Ashok Singh Gaur
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida
Email ID: ashok07mc03@gmail.com

Priyanshi Sharma
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida.
reachpriyanshi@gmail.com

Varsha Shukla
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida
varshashukla1015@gmail.com

Ms. Babita kumari
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida
babita.kumari@niet.co.in

Himanshi Sharma
Assistant Professor, Department: School of Computer Applications, NIET Greater Noida
hs84818@gmail.com

ABSTRACT

Humans have a distinctive quality that sets them apart from other organisms: their ability to reason, rationalize, and function effectively within large, organized groups. This intrinsic human trait has driven the evolution from basic counting tools like the abacus to the modern era of sophisticated robotics. To maintain order and safeguard individual freedoms, nations establish legislation and the rule of law, preventing domination by a privileged few. This study highlights the ambiguous aspects and limitations of current Information Technology Laws, with a focus on the growing domain of cyberspace. It aims to draw the attention of policymakers and legislators to the urgent need to update the Information Technology Act, 2000, to address emerging challenges in cyberspace. Utilizing a quantitative research methodology that systematically reviews historical data and qualitative techniques, the study's findings and recommendations will assist in creating or revising comprehensive IT laws that reflect the dynamic nature of technology and its applications.

Keywords: Indian Institute of Information Technology Act, IT Act 2000, Artificial Intelligence, Cyber Crime, Internet of Things.

Introduction

The internet and the World Wide Web are profoundly altering our world. Today, the threat of cyber-attacks on national defense or economic infrastructure overshadows concerns about poverty, famine, and conflicts. The COVID-19 pandemic has elevated the internet and computer systems to unprecedented levels of importance. Administration, education, and governance are now largely conducted through electronic and digital means.

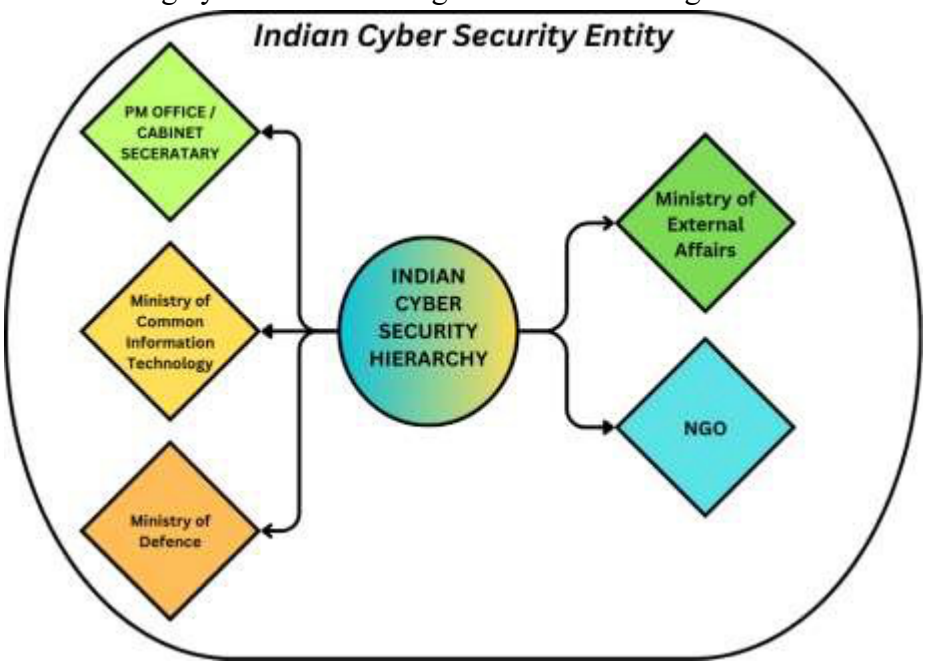

Figure 1: Indian Cyber Security Hierarchy

The figure illustrates the Indian Cyber Security Hierarchy, where various entities such as the Ministry of Defense (MoD), Non-Government Organizations, the Ministry of External Affairs (MoEA), the Ministry of Common Information Technology (MoCIT), and the Cabinet Minister are the key authorities in law and policy-making. The rapid development of digital technologies has left us uncertain about our societal structures and their interactions with algorithms. The pandemic has marked the beginning of a more advanced phase in the development of Digital India. Despite years of adaptation to the evolving cyberspace, concerns about the potential loss of personal and sensitive data to unknown and powerful entities persist. When there is an excessive amount of information circulating in cyberspace, regulations become necessary to organize and control the chaotic elements of bits and bytes, preventing disorder. Implementing or enhancing IT legislation is crucial for supporting the social, cultural, and economic functions of the nation. A robust legal framework is essential as the rules of the physical world cannot be directly applied to cybercrimes. The internet needs a supportive and enabling legal architecture to manage transgressions effectively.

Resources and Techniques

The Information Technology Act, 2000, was established to regulate virtual space due to its vulnerabilities and societal dependencies. Based on the UNCITRAL Model, this act focused on granting legal recognition to electronic documents and online transactions. The 2008 Amendment to the IT Act emphasized Information Security. However, the current legislation

lacks the necessary updates and flexibility required for digital rulemaking in India. Despite being the sole regulated law in India for digitalization, the IT Act has only been revised once in 2008.

In some areas, there may be a perceived need to revise existing regulations, while in others; the law's inadequacy to address emerging cyberspace issues is evident. This often necessitates entirely new legislation to address significant concerns. Informal interviews and open-ended questions provided flexibility in the study, offering valuable insights into real-world challenges and potential remedies for enhancing execution and enforcement. The qualitative study included participant observations, systematic planning, validity, and dependability. Legal precedents and drafts from various countries were examined to gain insights into effective principles and frameworks. Primary documents such as the UNCITRAL Model Law, Budapest Convention, and IT Act were used as data sources.

a. Insufficient Delineation of Cyber Crime

The primary flaw in the statute is the lack of a clear definition of "Cyber Crime" or "Information Technology Offences" in the IT Act, 2000 or its 2008 amendment. This indicates a lack of clarity and assurance from legislators in adhering to a universally accepted definition. Thus, any illegal act using a computer system is broadly classified as a Cyber Crime.

b. Insufficient Legal Framework for Addressing Cyber Offences

The IT Act of 2000 and its 2008 revision do not constitute a standalone Cyber Security law. The legislation fails to encompass all forms of cyber-attacks and breaches, despite including more cybercrimes in 2008. Rapid technological advancements make rigid legislation insufficient to address cybercrime effectively. Consequently, India's cybersecurity system is still developing and not fully equipped to handle cyber threats .

c. Responsibility of the Intermediary

To maintain confidence in a nation's legislative efforts, proactive rule-making is essential. An example is the accountability and legal obligations of intermediaries or Internet Service Providers, prompted by incidents of mob violence incited by social media messages. The government reduced intermediary security and held them accountable for failing to regulate online content.

The Inter-Ministerial Committee, led by Home Secretary Rajiv Gauba in 2018, presented findings to the Home Minister regarding mob-lynching incidents caused by false social media messages. The Committee condemned these provocations and recommended specific measures, such as appointing a Superintendent of Police in each district to handle legal actions against mob violence perpetrators. The Committee also engaged with Google, Facebook, and Twitter to implement measures to filter out undesirable content and expedite complaint resolution.

d. The Indian Institute of Information Technology Laws (Amendment) Bill, 2020

The III-T Laws (Amendment) Bill, 2020, aims to modify the III-T (Public-Private Partnership) Act, 2017, designating specific institutions as national significance institutes. The proposed revisions aim to enhance IT research, fostering a robust cyber community and skilled workforce. Once enacted, the Bill could address multiple disparities in technology infrastructure and human resources.

e. IoT: Data Protection and Privacy

'Big Data' is a rapidly emerging technological innovation in the cyber world, posing significant privacy risks. Accountability, accessibility, and security require privacy laws to include supervisory assignments and redress mechanisms. India currently lacks a robust regulatory authority and independent cybercrime statistics, making it difficult to assess the situation accurately. The National Crime Record Bureau publishes overall cybercrime data, but specific data on cyber security expenditures, enterprise phishing, and thefts from government entities are needed.

The Personal Data Protection Bill, 2019, awaiting approval in parliament, aims to safeguard individuals' privacy as a fundamental right. Additionally, the Insurance Regulatory and Development Authority of India issued cyber security guidelines for insurance companies in 2017, and SEBI introduced the Cyber Security and Cyber Resilience Framework for Stock Exchanges, Clearing Corporations, and Depositories in 2016. The Ministry of Health and Family Welfare also issued a draft of the Digital Information Security in Healthcare Act for public comments.

The IoT concept is emerging as a network connecting humans, objects, and IT systems, optimizing communication among them. This interaction inevitably leads to privacy and data protection concerns. The government drafted an IoT Policy in 2015, fostering a 'Machine to Machine' ecosystem and introducing Machine Learning concepts. Ensuring the privacy and security of circulating information is paramount.

f. Legal Compliances in AI

Indian law currently lacks specific provisions to address the ethical, legal, and regulatory implications of Artificial Intelligence (AI). Additionally, the Information Technology Act of 2000 does not include specific protections for privacy. In contrast, other countries are implementing regulations to address incidents involving technologies like Tesla's driverless cars and the explosion of Space X Falcon 9. India faces challenges in regulating aggregators such as Uber and Ola when legal issues arise. Furthermore, India lacks substantial literature on product liability and established legal principles regarding wrongful death torts.

In cases of wrongdoing, India relies on Section 43A of the Information Technology Act, 2000 (amended in 2008), and pursues legal action through consumer courts for product defects or service deficiencies. Despite the Ministry of Electronics and Information Technology releasing four AI Committee Reports in 2019, covering platforms, data, national missions, and technological capacity, and cybersecurity, significant progress is still needed compared to other countries. The National AI Programme, proposed by NITI Aayog in the 2018-2019 budget, highlights India's need for preparedness and experience in this domain.

Existing laws in India provide both civil and criminal remedies for AI-related issues. Section 66E of the IT Act addresses deep fake offences involving privacy infringement, with penalties including up to three years of imprisonment or a fine of INR 200,000. Section 66D targets the intentional misuse of communication devices or computer resources, with violators facing imprisonment and/or fines. Sections 67, 67A, and 67B of the IT Act address the dissemination or transmission of explicit deep fake content, requiring social media sites to promptly remove such content or risk losing their 'safe harbour' protection.

The Indian Penal Code also provides additional legal measures for cybercrimes related to deep fakes, including Sections 509 (offences against the modesty of a woman), 499 (criminal defamation), and 153(a) and (b) (inciting communal hatred). The Copyright Act of 1957 addresses the unauthorized use of copyrighted material to create deepfakes, with Section 51 explicitly prohibiting such actions. Recent cases demonstrate law enforcement's use of forgery-related provisions in dealing with deep fake technology.

g. ADVANCED DIGITALIZATION: CRYPTO CURRENCY AND BLOCKCHAIN TECHNOLOGY

The majority of blockchain-based projects in India face significant challenges due to a lack of legislation and regulatory gaps. The IT Act's requirements prohibit the use of digital signatures for transactions or documents related to immovable property, limiting the application of blockchain solutions in a country where many legal issues and disputes are property-related. While the Supreme Court of India has granted legal recognition to Bitcoin, the country still lacks a comprehensive legal framework for cryptocurrencies.

In July 2019, the government introduced the draft "Banning of Cryptocurrency and Regulation of Official Digital Currency Act, 2019," which aims to prohibit activities such as mining, generating, holding, selling, dealing in, issuing, transferring, disposing of, or using cryptocurrencies within India. In September 2019, the Ministry of Finance categorized cryptocurrencies into Utility tokens and Security tokens. In the absence of specific laws, the Reserve Bank of India is responsible for issuing warning circulars on this matter.

India's conceptual jurisprudence is insufficient for addressing emerging disruptive technologies like blockchain and the implementation of AI in the industrial sector. Specific provisions of the Information Technology Act, 2000 and 2008, including Sections 69A, 43A, and 67C, require thorough examination. Research must carefully balance new technology with constitutional rights under Articles 19 and 21. The significant gaps in current research raise concerns about India's preparedness to handle the complexities of drone technology, Bitcoin, military dome systems, and the challenge of autonomous weapon systems.

CONCLUSION AND SUGGESTIONS

In conclusion, the laws that are adopted or amended today must align with the essential needs of the future world. While it's impossible to completely eliminate flaws in such a rapidly expanding field, standards can be set by incorporating terms like 'technology collateral or incidental thereto' in relevant clauses to encompass any technological advancements. Strategically formulating laws in the swiftly evolving domains of networks and technology can reduce the need for excessive legislation, repeated enactment, and constant modifications.

The government's role in developing policies, rules, and regulations is crucial. Currently, urgent attention is needed to revise laws, as the nation increasingly resides and operates in the virtual realm rather than the physical world. The state should enforce stringent laws on intermediary liability, digital ethics, and the prompt resolution of cyber-related grievances. Additionally, addressing privacy concerns by advancing the Data Protection Bill is essential. Establishing a legislative framework for emerging technologies such as blockchain, cryptocurrencies, and drones is imperative.

Efforts have been made to proactively prevent cyber invasions and breaches through the implementation of Artificial Intelligence and real-time intelligence. To address regulatory ambiguities, targeted innovations can be implemented, such as an Intuitive Intrusion Detection System. This application offers robust protection against malicious cyber-attacks, even without prior knowledge of the specific characteristics of those threats.

REFERENCES

1. Agarwal, P. (2007). Higher education in India: Growth, concerns and change agenda. *Higher Education Quarterly*, *61*(2), 197–207. https://doi.org/10.1111/J.1468-2273.2007.00346.X
2. Chatterjee, S., & Kar, A. K. (2018). Effects of successful adoption of information technology enabled services in proposed smart cities of India: From user experience perspective. *Journal of Science and Technology Policy Management*, *9*(2), 189–209. https://doi.org/10.1108/JSTPM-03-2017- 0008/FULL/XML
3. Desai, A. (2003). *DRC Working Papers Global Software from Emerging Markets CENTRE FOR NEW AND EMERGING MARKETS LONDON BUSINESS SCHOOL The Dynamics of the Indian Information Technology Industry*.
4. Ghosh, J., & Shankar, U. (n.d.). *PRIVACY AND DATA PROTECTION LAWS IN INDIA: A RIGHT-BASED ANALYSIS*. Retrieved May 14, 2024, from http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspxArticle.
5. Greenleaf, G., Vivekanandan, V., Chung, P., Singh, R., & Mowbray, A. (2018). Challenges for Free Access to Law in a Multi-Jurisdictional Developing Country: Building the Legal Information Institute of India. *Https://Doi.Org/10.1177/2277401720130105*, *1*(1), 63–93. https://doi.org/10.1177/2277401720130105
6. Gupta, M. P., Kanungo, S., Kumar, R., & Sahu, G. P. (2007). A Study of Information Technology Effectiveness in Select Government Organizations in India. *Http://Dx.Doi.Org/10.1177/0256090920070202*, *32*(2), 7–21. https://doi.org/10.1177/0256090920070202
7. Jain, D. M., & Khurana, R. (2016). A framework to study vendors' contribution in a client vendor relationship in information technology service outsourcing in India. *Benchmarking*, *23*(2), 338–358. https://doi.org/10.1108/BIJ-04-2014-0029/FULL/XML

8. Jain, M., & Popli, G. S. (2012). Role of Information Technology in the Development of Banking Sector in India. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2151162
9. Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 305–326. https://doi.org/10.1007/978-3-319-78440-3_7
10. Kumar, P. N. V. (2016). Growing cyber crimes in India: A survey. *Proceedings of 2016 International Conference on Data Mining and Advanced Computing, SAPIENCE 2016*, 246–251. https://doi.org/10.1109/SAPIENCE.2016.7684146
11. *Laws relating to E Commerce in India: Issues & Challenges. | Amity Journal of Computational Sciences | EBSCOhost*. (n.d.). Retrieved May 14, 2024, from https://openurl.ebsco.com/EPDB%3Agcd%3A10%3A23022010/detailv2?sid=ebsco%3Aplink%3Aschola r&id=ebsco%3Agcd%3A162128987&crl=c.
12. Penfold, C. (2009). Off-Shored Services Workers: Labour Law and Practice in India. *Http://Dx.Doi.Org/10.1177/103530460901900207*, *19*(2), 91–106. https://doi.org/10.1177/103530460901900207
13. Raman, R., & Chadee, D. (2011). A Comparative Assessment of the Information Technology Services Sector in India and China. *Journal of Contemporary Asia*, *41*(3), 452–469. https://doi.org/10.1080/00472336.2011.582714
14. Ravishankar, M. N., Pan, S. L., & Myers, M. D. (2013). Information technology offshoring in India: a postcolonial perspective. *European Journal of Information Systems*, *22*(4), 387–402. https://doi.org/10.1057/EJIS.2012.32
15. Roberts, A. (2010). A Great and Revolutionary Law? The First Four Years of India's Right to Information Act. *Public Administration Review*, *70*(6), 925–933. https://doi.org/10.1111/J.1540-6210.2010.02224.X
16. Rudrappa, S. (2009). Cyber-Coolies and Techno-Braceros: Race and Commodification of Indian Information Technology Guest Workers in the United States. *University of San Francisco Law Review*, *44*. https://heinonline.org/HOL/Page?handle=hein.journals/usflr44&id=357&div=&collection=
17. Ryan Ph.D., P. S., Merchant, R., & Falvey, S. (2011). Regulation of the Cloud in India. *D-Lib Magazine*, *1*(6). https://doi.org/10.1045/DECEMBER95-KESSLER
18. Sahay, S., & Walsham, G. (2006). Scaling of health information systems in India: Challenges and approaches. *Information Technology for Development*, *12*(3), 185–200. https://doi.org/10.1002/ITDJ.20041
19. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology*. www.irjet.net
20. Singh, A., & Soltani, E. (2010). Knowledge management practices in Indian

information technology companies. *Total Quality Management*, *21*(2), 145–157. https://doi.org/10.1080/14783360903549832

21. Singh, H. P. (2018). *Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia*. www.amity.edu.in/ajcs
22. Singh, S. (2010). Promoting e-Governance through Right to Information: A Case-study of India. *International Journal of Scientific & Engineering Research*, *1*(2). http://www.ijser.org
23. *State and the IT Industry in India: An Overview on JSTOR*. (n.d.). Retrieved May 14, 2024, from https://www.jstor.org/stable/26698414.
24. Thottoli, M. M., & K.V, T. (2022). Characteristics of information communication technology and audit practices: evidence from India. *VINE Journal of Information and Knowledge Management Systems*, *52*(4), 570–593. https://doi.org/10.1108/VJIKMS-04-2020-0068/FULL/XML
25. Todd, P. R., & Javalgi, R. R. G. (2007). Internationalization of SMEs in India: Fostering entrepreneurship by leveraging information technology. *International Journal of Emerging Markets*, *2*(2), 166–180. https://doi.org/10.1108/17468800710739234/FULL/XML
26. Tripathi, S., & Tripathi, A. (2010). Privacy in libraries: The perspective from India. *Library Review*, *59*(8), 615–623. https://doi.org/10.1108/00242531011073146/FULL/XML
27. Dijk, M. P. (2003). Government policies with respect to an information technology cluster in Bangalore, India. *European Journal of Development Research*, *15*(2), 93–108. https://doi.org/10.1080/09578810312331287495/METRICS
28. Banerjee, P. (2006). Indian Information Technology Workers in the United States: The H-1B Visa, Flexible Production, and the Racialization of Labor. *Http://Dx.Doi.Org/10.1163/156916306777835295*, *32*(2–3), 425–445. https://doi.org/10.1163/156916306777835295
29. Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology and People*, *32*(5), 1153–1183. https://doi.org/10.1108/ITP-05-2018-0251/FULL/XML
30. Chaudhri, V., & Wang, J. (2007). Communicating Corporate Social Responsibility on the Internet. *Http://Dx.Doi.Org/10.1177/0893318907308746*, *21*(2), 232–247. https://doi.org/10.1177/0893318907308746
31. Kaur, Dr. G. (2017). Threats to the Rights of Consumers in E-Banking in India: An Overview. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2983199
32. Singh, M. K., & Kumar, V. (2020). *Impact of Covid-19 Pandemic on Working Culture: An Exploratory Research Among Information Technology (IT) Professionals in Bengaluru, Karnataka (India)*. https://www.researchgate.net/publication/342657957
33. Singh, N. (2004). Information Technology and Rural Development in India. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.523823

34. Sinha, S. (2006). Evidence for power-law tail of the wealth distribution in India. *Physica A: Statistical Mechanics and Its Applications*, *359*(1–4), 555–562. https://doi.org/10.1016/J.PHYSA.2005.02.092
35. Xiang, B. (2001). Structuration of Indian Information Technology Professionals' Migration to Australia: An Ethnographic Study. *International Migration*, *39*(5), 73–90. https://doi.org/10.1111/1468-2435.00172