



# Iot, AI And Block-Chain Driving The Refurbishment Of IT Legislation In India

Chetan Prakash<sup>1\*</sup>, Dr. Jasjeet Singh<sup>2</sup>

<sup>1\*</sup>Assistant professor, Gitarattan International Business School, Delhi, Email: [chetan.prakash@gitarattan.edu.in](mailto:chetan.prakash@gitarattan.edu.in)

<sup>2</sup>Assistant professor, Gitarattan International Business School, Delhi, Email: [jasjeet.singh@gitarattan.edu.in](mailto:jasjeet.singh@gitarattan.edu.in)

**Citation:** Chetan Prakash (2024), Iot, AI And Block-Chain Driving The Refurbishment Of IT Legislation In India, *Educational Administration: Theory and Practice*, 30(1), 597-602  
*Doi:* 10.53555/kuey.v30i1.5004

## ARTICLE INFO

## ABSTRACT

Humans possess a unique attribute of being superior to other organisms. They possess this supremacy not alone due to their capacity for reasoning and rationalizing, but also because of their inclination to organize themselves as a collective, capable of functioning well in huge groups. The innate human inclination to creatively adapt and modify its own creations has led to the transformation of our world, progressing from the use of simple counting devices like the abacus to the current age of advanced robotics. In order to prevent disorder and preserve their independence, every nation endeavors to eliminate the apprehension of control by a privileged few, therefore necessitating the implementation of legislation and the rule of law. The purpose of this study is to emphasize the ambiguous aspects and constraints present in Information Technology Laws, with a specific focus on the expanding realms of cyberspace. It also seeks to capture the attention of policymakers and legislators in order to make them comprehend the necessity of updating the Information Technology Act, 2000 to incorporate legislative provisions pertaining to emerging concerns in cyberspace.

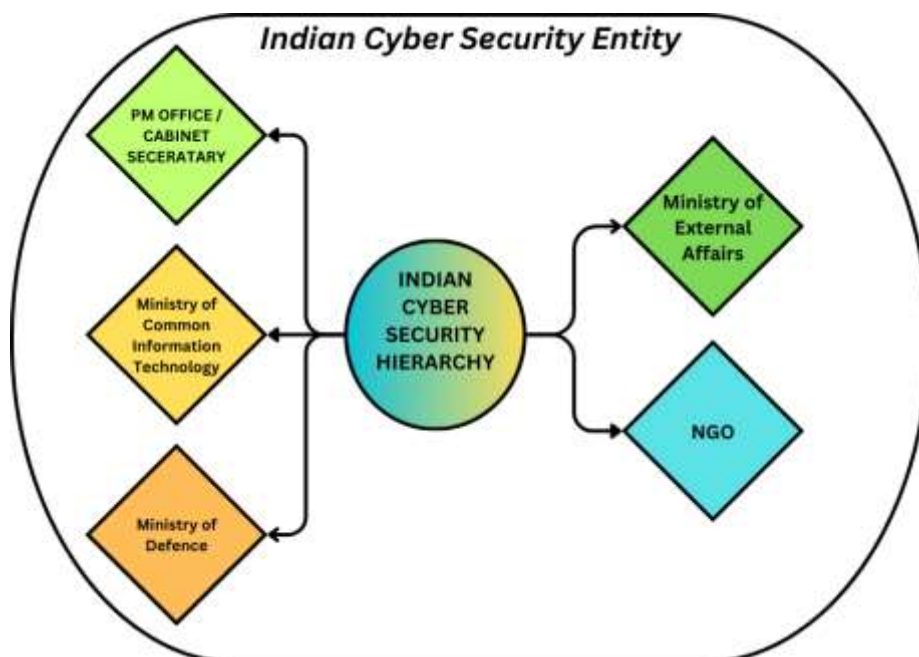
The quantitative research method involves systematically reviewing historical sources of information and using qualitative research techniques to analyse the findings.

The conclusions and recommendations of this article will undoubtedly provide valuable assistance in the creation or revision of a complete law pertaining to information technology, taking into account the ever-changing technologies and their practical applications.

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

## Introduction

Internet and the concept of World Wide Web are profoundly transforming the world in which we reside. Today, the level of anxiety regarding poverty, famine, and conflicts is no longer larger than that of a cyber-attack on a defense department or the economic infrastructure of a nation. Never before has the utilization of the internet and computer systems reached such a prominent role as it has during the COVID-19 era. All aspects of administration, academics, and governance are now communicating exclusively utilizing electronic and digital means. [1, 2]



**Figure 1: Indian Cyber Security Hierarchy**

The Indian Cyber Security Hierarchy is shown in the figure 1 where the various entities of the Ministry of Defense (MoD), Non-Government Organization, Ministry of External Affairs (MoEA), Ministry of Common Information Technology (MoCIT) and Cabinet Minister are the controlling authorities of the various law and policy makings.

The rapid development of the planet has left us uncertain about the structure of our society and how it operates in conjunction with algorithms. This pandemic signifies the commencement of a more advanced phase in the development of digital India. [3,4] Even after years of adjusting to the evolving aspects of cyberspace, we still have concerns about the potential loss of our personal and sensitive data to an unidentified and powerful entity. When an excessive amount of matter is present in space, or when an excessive amount of information is circulating in the networks of cyberspace, it becomes necessary to establish regulations. The purpose of regulation is to organize and control the disorderly elements of bits and bytes, in order to prevent chaos. This necessitates the creation of rules and the reinforcement of enforcement mechanisms. It is imperative to implement or enhance the Information Technology legislation in the country as it serves as the fundamental support system for the social, cultural, and economic functions of the nation. It is crucial to have a robust legal framework for Information Technology due to the inability to apply physical world rules to cybercrimes. The internet requires a legal architecture that is both supportive and enabling of transgressions.[5-7]

### **Resources and Techniques**

The Information Technology Act, 2000 was enacted by the legislature to regulate the virtual space due to its vulnerabilities and societal dependency. This act was based on the United Nations Commission on International Trade Law (UNCITRAL) Model, which focused on granting legal recognition to electronic documents and online transactions. The 2008 Amendment to the Information Technology Act, 2000 placed further emphasis on and made a concerted effort to priorities Information Security. The current legislation regarding the Information Technology Act clearly acknowledges the absence of necessary updates or a flexible approach needed for digital rulemaking in India. Although the Information Technology Act, 2000 is the sole regulated law in India pertaining to digitalization, it has only been revised once in 2008. [8,9]

In certain locations, there may be a perceived necessity to revise existing regulations, while in other instances, one may observe the inadequacy of the law to address emerging cyber space issues. Additionally, there may be a desire for the creation of an entirely new legislation on the subject due to the magnitude of the concerns. [10, 11] The utilization of informal interviews and open-ended questions allowed for flexibility in certain elements of the study. Engaging with individuals in the legal profession provided valuable insights into the real-world challenges and potential remedies for enhancing the execution and enforcement. The qualitative study also included participant observations for data collection, based on systematic planning, validity, and dependability. The authors have examined the legal precedents and drafts from many countries about laws and regulations related to information technology and cyberspace in order to gain insight into the principles and frameworks that can be effectively implemented. The paper employed data sourced from main documents such as the UNCITRAL Model Law, Budapest Convention, and Information Technology Act. [12]

### **a. Insufficient delineation of Cyber Crime**

The primary flaw in the statute is that the terms "Cyber Crime" or "Information Technology Offences" are not defined in either the Information Technology Act, 2000 or its revised version of 2008. This demonstrates the legislators' lack of assurance or clarity in adhering to any universally accepted definition of the term, as well as their inability to identify the specific circumstances or components that would constitute the accomplishment of a cybercrime. Therefore, it is necessary to comprehend the phrase in a broad manner, by considering that any illegal act carried out using a computer system will be classified as a Cyber Crime or an Information Technology crime. [13, 14]

### **b. Insufficient Legal Framework for Addressing Cyber Offences**

It is important to note that the Information Technology Law of 2000 and its revised edition of 2008 do not constitute a standalone Cyber Security law. The inadequacy of the statute lies in its failure to encompass all forms of cyber-attacks, breaches, and violations, notwithstanding the inclusion of further cybercrimes in the list of Information Technology crimes in 2008. Furthermore, technology is advancing rapidly, undergoing both revolutionary and transformative changes with technological advancements. [15] A rigid legislation will be insufficient to address this situation, given that cybercrime is a significant problem in India. Consequently, the cyber security system is still in its early stages of development and is not yet completely equipped to handle the problems posed by cyber threats. The primary factor contributing to the lack of reporting of infractions and offences in cyberspace is the key reason. The legislative framework fails to clearly define the specific duties and responsibilities that define the roles of the players in the digital and electronic ecosystem. When the laws are insufficient in both substance and essence to safeguard the residents of a specific geographical region, how can the governmental institutions and organizations be shielded from such international monstrosities. [16]

### **c. Responsibility of the Intermediary**

It is crucial to maintain confidence in a nation's legislative efforts, else optimism would diminish. An instance of proactive rule-making can be observed in the matter concerning the accountability and legal obligations of intermediaries, commonly referred to as Internet Service Providers. This initiative was prompted by fatalities resulting from mob violence, which were instigated by messages disseminated on social media. These occurrences compelled the government to reduce the level of security provided to intermediaries and hold them accountable for failing to regulate the content uploaded online. [17, 18]

The Inter-Ministerial Committee, led by Rajiv Gauba, the Home Secretary in 2018, presented its findings to the Home Minister about instances of mob-lynching that occurred in the nation. The reason of such inciting was determined to be the dissemination of counterfeit statements on social media. The Committee denounced these acts of provocation and incitement resulting from the dissemination of false information and rumours, and established specific recommendations. [19] For example, the Committee suggested appointing a Superintendent of Police in each district as the nodal authority responsible for taking legal action against those who commit acts of mob violence. The Committee also addressed the issue and engaged in discussions with representatives from Google, Facebook, and Twitter to implement all available procedures to eliminate or filter out undesirable content. In addition, the Committee is currently developing standards that would expedite the process of addressing a complaint within a few hours.

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

The III-T Laws (Amendment) Bill, 2020 is currently the most significant legislation awaiting approval in the parliament. This bill aims to modify the III-T (Public-Private Partnership) Act, 2017. The Act designates specific institutions as institutes of national significance. The proposed revisions aim to facilitate increased research in the field of Information Technology, hence fostering the development of a robust cyber community and skilled workforce capable of thriving in this industry. Once the Bill is enacted, it has the potential to address multiple disparities in relation to the enhancement of technology infrastructure and human resources. [20-22]

### **e. IoT: Data Protection and Privacy**

The term 'Big Data' is becoming highly popular in the cyber world, surpassing even the frequency of data packets on a network. Big data analytics is a rapidly emerging technological innovation. The task of analyzing and keeping data carries significant weight as it poses a risk to privacy. The concepts of Accountability, Accessibility, and Security necessitate that a privacy law include crucial components such as supervisory assignments and a method for redressed. Currently, India lacks a robust regulatory authority as well as a privacy or data commissioner. Furthermore, there is a lack of available independent statistics on individual cybercrime, making it impossible to determine. However, the National Crime Record Bureau does publish an overall data on cybercrimes. Additionally, specific data must be created, such as statistics concerning the national expenditure on cyber security, data regarding enterprises affected by crimes like phishing, or data on thefts of finances or information from governmental entities. [23,24]

The Personal Data Protection Bill, 2019, now awaiting approval in parliament, is a legislative document that aims to safeguard the privacy of individuals as a fundamental right and defend their privacy as an integral aspect of information privacy. 14. The Insurance Regulatory and Development Authority of India also issued cyber

security guidelines for insurance companies in 2017. In addition, the Security Exchange Board of India (SEBI) also introduced the Cyber Security and Cyber Resilience Framework for Stock Exchanges, Clearing Corporations, and Depositories in 2016. In addition, the Ministry of Health and Family Welfare has issued a notification regarding the draft of the Digital Information Security in Healthcare Act and has requested the public to provide comments. [25]

Furthermore, the concept of IoT is emerging as a network that connects humans, objects, and information technology systems, which can respond to both physical and virtual forms of data. Its objective is to optimize and refine the communication among persons, systems, and other entities. If such an interaction occurs between them, it would inevitably lead to the sharing of personal information and the interchange of a large amount of data, which will result in privacy and data protection concerns. In 2015, the government produced a draft on IoT Policy. These principles are leading to the emergence of a 'Machine to Machine' ecosystem and introducing concepts such as Machine learning. Each instance of progress is built upon preexisting information and data that circulate in the digital realm. Therefore, ensuring the privacy and security of people's information becomes a paramount responsibility in this domain. [26]

#### **f. Legal Compliances in AI**

Indian law lacks provisions to address the ethical, legal, and regulatory consequences of Artificial Intelligence. Additionally, there are no specific provisions in the Information Technology Act (2000) that protect privacy. Elsewhere in the world, there is scrutiny surrounding the explosion of the Space X Falcon 9 and regulations are being implemented to address incidents involving Tesla's driverless cars, following the laws of the western world. India continues to face challenges in effectively regulating aggregators like Uber and Ola when legal issues or conflicts develop. In India, there is currently a lack of literature on product liability and a lack of established legal principles regarding the tort of wrongful death. [27]

In the event of any such wrongdoing, we utilize Section 43A of the Information Technology Act, 2000 (amended in 2008) and pursue legal action in Consumer courts, either for product defects or service deficiencies. Despite the Ministry of Electronics and Information Technology releasing four Artificial Intelligence Committee Reports in 2019, which cover topics such as platforms and data on Artificial Intelligence, the use of Artificial Intelligence in national missions and programmes in key sectors, the analysis and mapping of technological capacity for adopting Artificial Intelligence technology, and cyber security issues, there is still a significant amount of progress needed to catch up with other countries in the world. [28] The National programme on Artificial Intelligence is required to be established by NITI Aayog in the 2018-2019 budget. While it is a wonderful and praiseworthy action, it also highlights our lack of preparedness and inexperience in dealing with this matter.

Currently, there are multiple provisions in the current laws that provide both civil and criminal solutions. Section 66E of the Information Technology Act, 2000 deals with deepfake offences that involve privacy infringement. These crimes can result in a prison sentence of up to three years or a fine of INR 200,000. Section 66D specifically addresses the intentional and harmful use of communication devices or computer resources. Violators can face consequences such as imprisonment and/or monetary fines. In addition, Sections 67, 67A, and 67B of the IT Act can legally charge individuals for disseminating or transmitting explicit deepfake content. Social media sites are required under the IT Rules to promptly remove such content, or else they may lose their 'safe harbour' protection. [29-31]

The Indian Penal Code offers additional legal options to address cybercrimes linked to deepfakes, including Sections 509 (offences against the modesty of a woman), 499 (criminal defamation), and 153 (a) and (b) (inciting hatred on communal grounds), among others. The Copyright Act of 1957 specifically deals with instances where copyrighted material is used without authorization to create deepfakes. Section 51 of the Act explicitly prohibits these actions. Moreover, recent examples illustrate how law enforcement has been utilising forgery-related provisions in instances involving deepfake technology. [32, 33]

#### **g. Advanced Digitalization: Crypto currency and BlockChain Technology**

The majority of blockchain-based projects in India encounter obstacles in progressing due to the absence of legislation and regulatory deficiencies. Due to the requirements of the IT Act, the use of digital signatures is not allowed for transactions or documents related to immovable property. This imposes constraints and confines the use of block chain based solutions in a nation where the majority of legal matters and disputes revolve around property. Regarding crypto currencies, the Supreme Court of India has provided legal recognition to Bit Coins. [34] However, the country still lacks a comprehensive legal framework for this matter. In July 2019, the Government introduced a draft legislation called the 'Banning of Crypto currency and Regulation of Official Digital Currency Act, 2019'. This legislation aims to prohibit any individual from engaging in activities such as mining, generating, holding, selling, dealing in, issuing, transferring, disposing of, or using crypto currency within the territory of India. In September 2019, the Ministry of Finance classified crypto currencies into distinct categories, namely Utility tokens and Security tokens. As there are no specific laws in place, the responsibility of issuing warning circulars in this matter lies with the Reserve Bank of India.

Conceptual jurisprudence is insufficient in the national context regarding upcoming disruptive technologies such as block chain or the implementation of Artificial Intelligence techniques in the industrial sector. [35, 36] Specific provisions of the Information Technology Act, 2000 and 2008, such as Section 69A, 43A, and 67C, require thorough scrutiny. The research must be conducted with careful consideration for the fragile

equilibrium between new technology and the constitutional rights outlined in Article 19 and 21. Given the significant gaps in our current research, it is questionable if we are adequately prepared to handle the complexities of drone technology, bit coin, dome systems in military applications, or the challenge of slaughter bots.

### CONCLUSION AND SUGGESTIONS

In conclusion, the laws adopted or altered today must align with the essential requirements of the future world. It is not possible to completely eliminate faults in a constantly expanding field, but standards can be established by incorporating language such as 'technology collateral or incidental thereto' in every relevant clause. This will signify any progress made in technology. Strategic formulation of laws in the rapidly evolving realm of networks and technology will reduce the need for excessive legislation, repeated enactment, and endless modifications. The government will always play a fundamental and crucial role in the development of policies, rules, and regulations. Nevertheless, at present, it is imperative that the government promptly and urgently focuses on revising the laws, given that the entire nation is predominantly residing and operating in the virtual realm rather than the physical world. The state should implement strict legislation on intermediary liability, digital ethics, and prompt resolution of cyber-related grievances. Additionally, it is imperative that the state expeditiously addresses privacy concerns by advancing the Data Protection Bill. It is imperative to establish a legislative framework for developing technologies such as blockchain, cryptocurrencies, and drones. We have implemented Artificial Intelligence and Real-time intelligence to proactively prevent cyber invasions and infractions. In addition, research is considered incomplete unless it include an element of creativity. To address regulatory ambiguities, targeted innovations can be implemented, such as: Intuitive Intrusion Detection System. This application provides robust protection against malicious cyber-attacks, without requiring 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](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%3Ascholar&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-Bracers: 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](http://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](http://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>