INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

COMPARISON OF THE CYBERCRIME PREVENTION LAWS IN INDIA AND THE UNITED KINGDOM

AUTHOR - NISHANT SINGH* & MS.ADYA PANDEY**

*STUDENT AT AMITY UNIVERSITY LUCKNOW

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY LUCKNOW CAMPUS

BEST CITATION - NISHANT SINGH & MS.ADYA PANDEY, COMPARISON OF THE CYBERCRIME PREVENTION LAWS IN INDIA AND THE UNITED KINGDOM, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (4) OF 2025, PG. 874-880, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

As global cybercrime rises, strong regulatory frameworks are needed to mitigate digital hazards. We examine the legislative basis, enforcement tactics, and recent modifications of two UK and Indian cybercrime prevention legislation. The Information Technology Act, 2000 (IT Act), India's main cybercrime law, covers unauthorised access, data theft, and electronic fraud. Recent changes and upcoming laws aim to improve data privacy and align it with global standards. However, outdated regulations, strict enforcement, and funding issues persist. Decentralised enforcement institutions like Cyber Crime Cells, CERT-IN, and the National Cyber Crime Reporting Portal handle poorly coordinated activities. The Computer Misuse Act of 1990, Fraud Act of 2006, and Data Protection Act of 2018 (which includes GDPR) expand the UK's legal framework. These guidelines provide a firm framework for fighting various cybercrimes with the support of the National Crime Agency (NCA), Information Commissioner's Office (ICO), and National Cyber Crime Unit (NCCU). UK plan includes modern tools, education, and strong international collaboration. The study reveals similarities and differences in the two nations' legal systems. Both nations struggle with legislative changes, enforcement efficacy, and privacy issues despite their reliance on robust laws and specialist enforcement. Cybercrime prevention requires updating and modernising legislation, strengthening enforcement, improving international collaboration, and raising public awareness. Focussing on cybercrime and digital environment protection may help India and the UK.

Keywords: Cybercrime, Information Technology Act, Computer Misuse Act, Data Protection Act, enforcement mechanisms, international cooperation, legislative frameworks, cybersecurity.

Introduction

Over the past 20 years, cybercrime has skyrocketed, affecting businesses and society worldwide. The expansion of internet connectivity and rapid technological advancement have given criminals new tools. Computer network or internet-related crimes are called "cybercrime". Hacking, cyberfraud, online abuse, and identity theft are examples. These mishaps disclose data protection gaps, damage public faith in digital systems, and need quick cybersecurity reforms. They can also cost money[1407]. Cybercrime costs the global economy billions annually. Financial loss and identity theft hurt individuals, while fraud, theft, and system damage harm enterprises. Governments must invest in cybersecurity and law enforcement to mitigate these threats. Cybercrime is prevalent, thus robust legal frameworks and worldwide coordination are

[1407] Gumbi, D. (2018). Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom'.

needed to secure online spaces and technical infrastructure. Cybercrimes are growing increasingly frequent and complex, requiring robust legal safeguards and prevention. Strong rules and regulations set legal limits, specify prohibited conduct, and punish offenders. They legalise hacker punishment, international collaboration, and victim protection. Without proper regulation, cybercrime protection methods risk becoming fragmented and insufficient, providing hackers easy loopholes. While protecting private data and financial assets is crucial, combating cybercrime is even more crucial for digital network trust[1408]. Well-written laws deter criminals, reduce cybercrime, and improve internet safety. They also help consumers and companies understand cybersecurity and obey legislation. Strict regulations can boost national security, economic stability, and digital safety. Due to its extensive legal history and advanced digital infrastructure, the UK has strong cybercrime legislation and enforcement bodies. This research compares the two nations' legal systems to see how well they tackle cybercrime and where they might improve. This comparison compares the UK and India's legislative frameworks, enforcement methods, and recent advances to show how different countries fight cybercrime[1409]. The idea is to learn from examples. The goal is to contribute to worldwide cybersecurity initiatives and more efficient legislative and regulatory frameworks.

2. Overview of Cybercrime Prevention Laws in India

Legislation

The Information Technology Act, 2000 (IT Act) is India's main cybercrime law, legitimising and enabling electronic transactions and e-commerce. The IT Act's cybercrime sections cover hacking, data theft, and electronic fraud. Hacking and other computer crimes are banned under Section 66 of the IT Act. This portion establishes the legal foundation for penalising unauthorised access to computer systems and data, a major advance in cyber security[1410]. Section 66C criminalises identity theft through fraudulent use of another's electronic identity. The provision discourages phishing and unethical use of personal information. Section 66D criminalises computer fraud, which involves deception for financial gain. These elements form a comprehensive foundation for combating cybercrime. The IT Act also protects privacy and data, such as Section 72, which prohibits intermediaries from disclosing information without permission. This area is important for avoiding data abuse by individuals and organisations. The IT Act creates Adjudicating Officers and Cyber Appellate Tribunals to handle cybercrime issues.

Amendments and Updates

Since its adoption, the IT Act has been updated multiple times to reflect cybercrime and technology advances. The Information Technology (Amendment) Act, 2008 was the most significant modification, revising the initial Act. This amendment expanded cybercrime crimes and added sections to address rising concerns. Section 66A of the 2008 amendment addresses online harassment and hate speech via electronic means. Because of its misuse and limitation on free expression, the Supreme Court struck down this article in 2015. The IT Act was updated by the Information Technology (Amendment) Act, 2018 to improve cybersecurity and data protection. This amendment reinforced the need for businesses to secure consumer data when data protection laws were passed[1411]. In addition, the Personal Data Protection Bill, 2019 attempts to build a comprehensive data protection framework in

[1408] Eboibi, F. E. (2021). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, *47*(1), 113-142.

[1409] Syngle, T. (2017). An overview of corporate cybercrime in India and US. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *6*(2), 49-59.

[1410] Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 305-326.

[1411] Al Hosani, H., Yousef, M., Al Shouq, S., Iqbal, F., &Mouheb, D. (2019, November). A comparative analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

India in line with international standards like the GDPR. This initiative seeks to close data protection and privacy gaps by enhancing cybercrime prevention laws and data management standards.

Enforcement Agencies

Indian cybercrime laws are enforced by many important authorities. Many governments and union territories have Cyber Crime Cells that investigate and prosecute cybercrime. Local police agencies oversee these cybercrime units, which may handle hacking and online fraud. The Ministry of Home Affairs created the National Cyber Crime Reporting Portal to centralise cybercrime reporting. This site streamlines reporting and expedites case registration and resolution[1412]. It also helps victims and provides cybercrime prevention information. India's CERT-IN monitors and responds to cybersecurity events. Organisations need CERT-IN to coordinate cyber threat response, provide technical assistance, and share cybersecurity best practices. It collaborates with international partners to combat cross-border crimes and improve cybersecurity collaboration.

Challenges and Criticisms

India has several cybercrime challenges despite its legal framework and enforcement. Some elements of the IT Act are outdated and may not address modern cyber threats, which is an issue. The legal framework must be revised to accommodate for new cybercrimes as technology advances rapidly. Enforcement issues are another problem. Cybercrime enforcement includes several federal and state agencies, which may cause inefficiencies and coordination issues. Another concern is the gap between law and practice[1413]. The IT Act provides a comprehensive legal framework, but enforcement is inconsistent. Cybercrime cases can drag on due to process, knowledge, or judicial system issues. India's cybercrime prevention laws and enforcement mechanisms have improved, however they still require improvement. These issues require a coordinated effort to modernise legislation, increase enforcement, and ensure cybercrime law enforcement.

3. Overview of Cybercrime Prevention Laws in the United Kingdom

Legislation

UK cybercrime laws are tough and diversified, proactively addressing digital threats. The UK's cybercrime laws are based on the 1990 Computer Misuse Act. Hacking and other illicit access computer systems and data are criminalised under this law. The Act criminalises unauthorised computer system access under Section 1 to deter illicit access and data breaches. Section 2 includes unlawful access to conduct or help illegal crimes, including spying and planning. The later Section 3 amendment made it illegal to change computer content without authorisation, including installing viruses or malware[1414]. The Computer Misuse Act's broad approach allows prosecution of several cyberattacks. In addition to the Computer Misuse Act, the 2006 Fraud Act addresses cyber fraud. Especially for electronic and online fraud, this Act makes fraud by false representation a felony. Since the 2018 Data Protection Act, which adapts the GDPR for the UK, data protection and privacy laws have improved. The Act's personal data provisions highlight consent, correct data, and the right to access personal information. Data controllers and processors must protect personal data reasonably[1415]. According to the Act's strict provisions, organisations must inform the ICO of data breaches within 72 hours. Under the General Data Protection Regulation (GDPR),

[1412] Kabha, R., Kamel, A., Elbahi, M., & Narula, S. (2019). Comparison study between the UAE, the UK, and India in dealing with WhatsApp fake news. *Journal of Content, Community and Communication*, *10*, 176-186.
[1413] Sethu, S. G. (2020, July). Legal protection for data security: a comparative analysis of the laws and regulations of European Union, US, India and UAE. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.
[1414] Ralarala, S. (2020). *The Impact of cyber crime on e-commerce and regulation in Kenya, South Africa and the United Kingdom* (Doctoral dissertation, Strathmore University).
[1415] Abiodun, A. (2021). A comparative analysis of the legal framework for the criminalization of cyberterrorism in Nigeria, England and the United States. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, *12*(1), 99-112.

corporations must comply and individuals' rights to control their personal data are increased.

Enforcement Agencies

Several key UK authorities police cybercrime and cybersecurity legislation. National Cyber Crime Unit (NCCU) of the National Crime Agency (NCA) combats large and organised cybercrime. The NCCU focusses on large cybercrimes include coordinated attacks on critical infrastructure, enormous fraud, and complex hacking operations. It collaborates with law enforcement and overseas partners to improve UK cybersecurity and combat global cyber threats. The independent UK Information Commissioner's Office (ICO) protects data and upholds information rights. According to the GDPR and the Data Protection Act of 2018, the Information Commissioner's Office (ICO) ensures firms comply with data protection laws and don't infringe privacy rights[1416]. The Information Commissioner's Office (ICO) investigates complaints, audits, and penalises data breaches and non-compliance to protect data security and privacy. In addition to fighting big and organised crime, the National Crime Agency (NCA) prevents cybercrime. The NCA works with the NCCU to investigate and punish cybercrime and other crimes. The NCA's collaboration helps the UK fight and investigate cybercrime.

4. Comparative Analysis

Legal Frameworks

There are several similarities and differences between UK and Indian cybercrime prevention laws. The IT Act, 2000 is India's main cybercrime law. Data theft, computer fraud, and unauthorised access are among its many crimes. This Act punishes cybercriminals, although many of its provisions, such as those on hacking and identity theft, are outdated due to the rapid development of new technology. Recent changes like the Information Technology (Amendment) Act, 2018 and the anticipated Personal Data Protection Bill, 2019 aim to enhance the legal framework by aligning data protection with worldwide standards. Enforcement challenges include shifting cyber threats and filling legal gaps[1417]. However, the UK's legal system is strong and contains landmark laws. The Fraud Act of 2006 covers several sorts of cyber fraud, although the Computer Misuse Act of 1990 prohibits computer hacking. The 2018 Data Protection Act incorporates the UK's GDPR and sets strict privacy and data protection standards. This comprehensive law addresses cybercrime by targeting fraud, data breaches, and unauthorised access. The UK's proactive cybercrime and data protection plan is considered stronger and more in line with global best practices than India's.

Enforcement Mechanisms

UK and Indian cybercrime enforcement methods are equally vital, but their efficiency vary due to differences in resources, knowledge, and collaboration. India implements through cyber crime cells, CERT-IN, and the National Cyber Crime Reporting Portal. Coordination, resources, and specialist training are issues for these entities, which investigate cybercrimes, respond to incidents, and answer complaints. Decentralised enforcement may mishandle cybercrime cases and ignore difficult issues. In contrast, the UK's centralised cybercrime policy has worked. The National Cyber Crime Unit (NCCU) of the National Crime Agency (NCA) oversees and offers expertise in high-level cybercrime investigations nationally[1418]. The ICO monitors data protection, whereas the NCA handles more complex criminal investigations, including cybercrime. Their specialist nature and better resources and training help them

[1416] Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: a cross-country study. *Journal of Global Information Technology Management*, *23*(2), 112-137.

[1417] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820.

[1418] Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 17488958221128128.

fight cybercrime and respond to emerging threats.

International Cooperation

Cybercrime affects governments worldwide, thus they must collaborate to fight it. India and the UK collaborate globally in different ways. India participates in the International Telecommunication Union (ITU) and the Global Forum on Cyber Expertise (GFCE) to share knowledge and improve cybersecurity worldwide. India collaborates with other nations on joint investigations and capacity-building. Bilateral agreements matter too. However, coordination and legal issues may limit these worldwide efforts. UK cybersecurity cooperation is well-established[1419]. The UK's engagement in Europol and ENISA, the European Union Agency for Cybersecurity, shows its commitment to international collaboration. Joint actions and information sharing with foreign allies help the UK combat global cyber threats. The government leads worldwide cybersecurity programs and sets international regulations and standards, making cybercrime response more structured and effective.

Recent Developments

The Indian and British governments have amended their cybercrime laws to reflect new concerns. The IT Act amendments and anticipated Personal Data Protection Bill, 2019 demonstrate India's commitment to data protection and worldwide standards. These reforms aim to strengthen India's cybersecurity, combat growing threats, and improve data protection laws. These reforms depend on how successfully they are implemented and how enforcement agencies adapt to the new laws. A new UK law, the Data Protection Act of 2018, applies the General Data Protection Regulation (GDPR) and sets strict privacy and data protection obligations. The UK's data protection reputation is due to strong data processor and controller rules[1420].

5. Case Studies

India

High-profile cybercrime cases in India have highlighted the country's justice system's strengths and faults. For instance, Pune's Cosmos Bank was hacked in 2018. The cyber group used stolen cards and exploited security weaknesses to steal over ₹94 crore (nearly $13 million) from ATMs worldwide. The crooks used malware to get into the bank's system and steal financial data. The case highlighted banking sector flaws and the need for effective cybersecurity. The Pune Police Cyber Crime Cell investigated the Cosmos Bank attack with help from CERT-IN. Multiple people were arrested in this case and indicted under the Information Technology Act, 2000 (IT Act), including data theft and illegal access. This case showed how the IT Act may be utilised to investigate complex cybercrimes, but it also highlighted the need for international coordination. Data breaches at Indian e-commerce giant BigBasket in 2019 were another notable event[1421]. Cybercriminals stole almost 2 crore (20 million) names, emails, and phone numbers. A hack on the company's database prompted the breach, raising concerns about data security and privacy. After notifying the Cyber Crime Cell, the business fixed the security flaw and informed affected consumers. Due to inadequate data security processes, the case highlighted the need of IT Act data protection.

United Kingdom

These high-profile UK cybercrime cases demonstrate the country's strong legal system and enforcement. In 2017, WannaCry ransomware attacked many NHS hospitals in

[1419] P., Shwetha. (2021). Comparative Analysis of Privacy and Data Protection Laws in E-Commerce. *Indian JL & Legal Rsch.*, *3*, 1.

[1420] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*, 971.

[1421] Jain, M. J., & Chaudhary, M. R. (2019). Understanding the concept of cybercrimes in India Vis-a-Vis cyber laws of USA. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *6*(2), 427-438.

the UK. Ransomware encrypts files and demands money on hacked systems. The attack damaged infrastructure and disrupted healthcare. The NCA and NCCU investigated WannaCry. Cybersecurity officials collaborated with global peers to mitigate the threat. These case studies demonstrate the necessity for international collaboration and cybersecurity preparation in the face of large-scale cyber attacks. Another notable event was the 2020 hack of Boots, the UK's largest pharmacy retailer. Hackers took client data and login passwords from the business's computers. The ICO investigated the event[1422]. After the lawsuit, the company reevaluated its data protection policies and realised how important GDPR compliance is for customer data. BT Group's 2021 hack was another high-profile case. Hackers used enterprise network weaknesses to steal private data and disrupt service. The NCCU led the investigation to secure the compromised networks and identify the criminals with other law enforcement authorities. This incident showed that telecoms infrastructure has trouble implementing strong cybersecurity measures. Bitrue, a British cryptocurrency exchange, was another 2019 highlight. Hackers exploited system weaknesses to steal about $4.5 million in bitcoin from the exchange. According to the NCA, bitcoin sector security should be tightened and digital currencies are dangerous.

6. Conclusion

The UK and India's cybercrime prevention laws have certain similarities and some differences, reflecting their varied approaches to cybercrime. Both the UK and India understand the need for robust laws and focused enforcement to combat cybercrime. The IT Act (Amendment) Act, 2018 and the planned Personal Data privacy Bill, 2019 aim to increase data privacy and align India's legislation with international norms. The 2000 IT Act covers cybercrimes such unauthorised access and data theft. Despite these efforts, resource constraints, enforcement concerns, and outdated rules limit cybercrime prevention and response in India. Decentralised enforcement by CERT-IN, state-level Cyber Crime Cells, and the National Cyber Crime Reporting Portal sometimes lacks resources and coordination. The UK benefits from a more comprehensive and unified legal system. Computer Misuse Act 1990, Fraud Act 2006, and Data Protection Act 2018, which contains GDPR, give a strong foundation to combat cybercrimes such hacking, fraud, and data breaches. Both nations may improve cybercrime prevention laws in several ways. India must accelerate the Personal Data Protection Bill and modernise the IT Act to keep up with technology and outdated laws. Implementing specialist training programs, increasing Cyber Crime Cell and CERT-IN cooperation and resources, etc. can boost enforcement efficiency. The UK should invest in training and technology to be prepared. Both nations should collaborate on global cybersecurity initiatives, share information, and investigate cyber threats that cross borders. To prevent cybercrime, both nations must educate the public and companies about cybersecurity and data protection. Finally, privacy problems must be resolved and cybersecurity measures balanced with individual rights to build confidence and avoid criminality. These proposals can help India and the UK fight cybercrime and secure digital ecosystems.

7. Reference

1. Gumbi, D. (2018). Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom'.
2. Eboibi, F. E. (2021). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive

[1422] Arab, M. S. (2020). Global surge in cybercrimes-Indian response and empirical evidence on need for a robust crime prevention system. *International Journal of Cyber Criminology*, *14*(2), 497-507.

enforcement measures. *Commonwealth Law Bulletin*, *47*(1), 113-142.

3. Syngle, T. (2017). An overview of corporate cybercrime in India and US. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *6*(2), 49-59.
4. Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 305-326.
5. Al Hosani, H., Yousef, M., Al Shouq, S., Iqbal, F., &Mouheb, D. (2019, November). A comparative analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.
6. Kabha, R., Kamel, A., Elbahi, M., & Narula, S. (2019). Comparison study between the UAE, the UK, and India in dealing with WhatsApp fake news. *Journal of Content, Community and Communication*, *10*, 176-186.
7. Sethu, S. G. (2020, July). Legal protection for data security: a comparative analysis of the laws and regulations of European Union, US, India and UAE. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.
8. Ralarala, S. (2020). *The Impact of cyber crime on e-commerce and regulation in Kenya, South Africa and the United Kingdom* (Doctoral dissertation, Strathmore University).
9. Abiodun, A. (2021). A comparative analysis of the legal framework for the criminalization of cyberterrorism in Nigeria, England and the United States. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, *12*(1), 99-112.
10. Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: a cross-country study. *Journal of Global Information Technology Management*, *23*(2), 112-137.
11. Arab, M. S. (2020). Global surge in cybercrimes-Indian response and empirical evidence on need for a robust crime prevention system. *International Journal of Cyber Criminology*, *14*(2), 497-507.
12. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820.
13. Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 17488958221128128.
14. P., Shwetha. (2021). Comparative Analysis of Privacy and Data Protection Laws in E-Commerce. *Indian JL & Legal Rsch.*, *3*, 1.
15. Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*, 971.
16. Jain, M. J., & Chaudhary, M. R. (2019). Understanding the concept of cybercrimes in India Vis-a-Vis cyber laws of USA. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *6*(2), 427-438.