DeepScience

Handbook on the Information Technology Act, 2000

Offences, Penalties, and the Impact of New Criminal Laws

Rahul Kailas Bharati

Handbook on the Information Technology Act, 2000: Offences, Penalties, and the Impact of New Criminal Laws

Rahul Kailas Bharati
Department of Law, Government Institute of Forensic Science,
Chhatrapati Sambhaji Nagar (Maharashtra), India

DeepScience

Published, marketed, and distributed by:

Deep Science Publishing, 2025
USA | UK | India | Turkey
Reg. No. MH-33-0523625
www.deepscienceresearch.com
editor@deepscienceresearch.com
WhatsApp: +91 7977171947

ISBN: 978-93-7185-207-4

E-ISBN: 978-93-7185-183-1

https://doi.org/10.70593/978-93-7185-183-1

Citation: Bharati, R. K. (2025). *Handbook on the Information Technology Act, 2000: Offences, Penalties, and the Impact of New Criminal Laws*. Deep Science Publishing. https://doi.org/10.70593/978-93-7185-183-1

Preface

The relentless march of digital technology has fundamentally reshaped our world, creating a society that is more interconnected and efficient than ever before. This digital revolution, however, has brought with it a new frontier of criminal activity. Cybercrimes, in their myriad forms, now pose a significant and ever-evolving threat to individuals, corporations, and national security. In this landscape, a comprehensive understanding of the legal frameworks designed to combat these offences is not just beneficial—it is essential.

The Information Technology Act, 2000, has been the cornerstone of India's cyber legal jurisprudence for over two decades. It has provided the primary legal scaffolding for addressing a spectrum of digital offences. However, the recent, monumental overhaul of India's criminal justice system, marked by the enactment of the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam, has ushered in a new era of legal interpretation and application. This legislative shift necessitates a fresh and thorough examination of cyber law and its enforcement.

This *"Handbook on the Information Technology Act, 2000"* has been conceived to meet this critical need. It is designed to be a comprehensive and accessible resource for a diverse audience, including legal practitioners, judges, law enforcement agencies, corporate professionals, forensic experts, and students of law. Our objective is twofold: *first,* to provide a detailed, section-by-section analysis of the offences and penalties prescribed under the IT Act, enriched with seminal case studies and judicial precedents. *Second*, and crucially, to dissect the profound impact of the new criminal laws on the existing provisions of the IT Act, offering clarity on the evolving legal landscape.

We have endeavoured to create more than just a commentary; this handbook is a practical tool. Through real-world examples and in-depth case studies, it bridges the gap between theoretical legal provisions and their practical application in investigations and courtrooms. It navigates the intricate interplay between the specialized provisions of the IT Act and the general principles of the new penal code, offering readers a holistic understanding of cyber offence prosecution in India today.

As we stand at this legal crossroads, it is our sincere hope that this handbook will serve as an indispensable guide, empowering its readers to navigate the complexities of Indian cyber law with confidence and clarity. We trust it will be a valuable companion in our collective effort to ensure a just, safe, and secure digital environment for all.

Rahul Kailas Bharati

Table of Contents

II. **Principal Acts:**

i. The Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008 and subsequent amendments).

ii. The Indian Penal Code, 1860 (IPC) (Relevant sections until its repeal and replacement).

iii. The Code of Criminal Procedure, 1973 (Cr.P.C) (Relevant sections until its repeal and replacement).

iv. The Indian Evidence Act, 1872 (IEA) (Relevant sections until its repeal and replacement).

v. The Bharatiya Nyaya Sanhita, 2023 (BNS).

vi. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS).

vii. The Bharatiya Sakshya Adhiniyam, 2023 (BSA).

viii. The Digital Personal Data Protection Act, 2023 (DPDP Act).

ix. The Copyright Act, 1957.

x. The Trade Marks Act, 1999.

xi. The Patents Act, 1970.

xii. The Unlawful Activities (Prevention) Act, 1967 (UAPA).

xiii. The Prevention of Money Laundering Act, 2002 (PMLA).

xiv. The Bankers' Books Evidence Act, 1891.

xv. The Telegraph Act, 1885.

III. **Rules and Regulations:**

i. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).

ii. The Information Technology (Intermediaries Guidelines) Rules, 2011 (and its successor).

iii. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.**

iv. The Information Technology (Certifying Authorities) Rules, 2000.

v. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

vi. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

vii. The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013 (CERT-In Rules).

viii. Directions issued by CERT-In under Section 70B (6) of the IT Act, 2000 (e.g., Direction No. 20(3)/2022-CERT-In dated April 28, 2022).

ix. Reserve Bank of India (RBI) Guidelines on Cybersecurity, Data Protection, and Digital Payments.

x. Securities and Exchange Board of India (SEBI) Circulars and Guidelines related to Cybersecurity.

xi. Ministry of Home Affairs (MHA) Notifications and Advisories on Cybercrime.

IV. Books

i. Rahul Kailas Bharati and Dr. Shobha Kamalakar Bawiskar, *Cyber Law and Cyber Crime Detection*, Namya Press Publication, New Delhi, 2023
ii. Dr. Rahul Kailas Bharati, *A Comprehensive Guide to New Criminal Laws*, Vinod Publications, 2024.
iii. Apar Gupta, *Commentary on the Information Technology Act* (LexisNexis).
iv. N.S. Nappinai, *Technology Laws Decoded* (LexisNexis).
v. Karnika Seth, *Computers, Internet and New Technology Laws: A Comprehensive Reference Work with Special Focus on Developments in India* (LexisNexis).
vi. Pavan Duggal, *Textbook on Cyber Law* (Universal Law Publishing).
vii. Vakul Sharma, *Information Technology: Law and Practice* (LexisNexis).
viii. Rodney D. Ryder, *Guide to Cyber Laws* (LexisNexis).
ix. S.R. Bhansali, *Commentary on the Information Technology Act, 2000*
x. Gibson, W. (1984) Neuromancer, Ace Books
xi. Kerr, O. S. (2005). Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. New York University Law Review, 78(6), 1596–1668

xii. United Nations Commission on International Trade Law (UNCITRAL). (1996). *Model Law on Electronic Commerce*
xiii. Ministry of Electronics and Information Technology (MeitY). (2023). *The Information Technology Act, 2000* [PDF]. Government of India.
xiv. "Safe Harbour Clause in IT Law," 2023; Cyril Amarchand Mangaldas, 2022; iPleaders, 2022
xv. The Indian Computer Emergency Response Team [CERT-In], 2025; Vajiram and Ravi, 2025; MyLawRD, 2025
xvi. Reserve Bank of India [RBI], 2022; CERT-In, 2023; Singh, 2024
xvii. Kumar, 2023; Brookings Institution, 2020; Ministry of Electronics and Information Technology [MeitY], 2024.
xviii. Online Legal India, 2025; AsianLaws.org, 2024
xix. National Crime Records Bureau [NCRB], 2024; Europol, 2023; Chainalysis, 2025
xx. Nelson, B., Phillips, A., & Steuart, C. (2020). *Guide to computer forensics and investigations* (6th ed.). Cengage Learning.
xxi. CERT-In. (2017). *Advisory on WannaCry ransomware attack* [Security Advisory]. Indian Computer Emergency Response Team.
xxii. AIIMS Ransomware Cybercrime: A Complete Case Study. (2024, October 26). Data Galaxy.
xxiii. Orissa High Court. (2024). *Order granting bail in cryptocurrency Ponzi scheme case* (Criminal Appeal No. 303 of 2024)
xxiv. Buckels, E. E., Trapnell, P. D., & Paulhus, D. L. (2014). *Trolls just want to have fun*. *Personality and Individual Differences*, 67, 97–102.
xxv. World Pulse. (2015, January 21). *Cyber stalking: A "virtual" crime with real consequences*
xxvi. Women Press Freedom. (2024, November 8). *India: Malicious doxing by right-wing trolls' targets Rana Ayyub, incites harassment*.
xxvii. CrowdStrike. (2025, January 16). *Most common AI-powered cyberattacks*. CrowdStrike
xxviii. Indian Computer Emergency Response Team (CERT-In). (2024). *Advisory on cloud storage misconfigurations and data leaks*
xxix. Narcotics Control Bureau. (2025, July 1). *Operation MELON busts India's largest darknet drug syndicate*. Government of India.
xxx. Information Commissioner's Office (ICO). (2025, February 6). *TalkTalk cyber-attack – how the ICO's investigation unfolded*

V. **Reports and Official Publications**

i. Law Commission of India Reports (Relevant reports on IT Act, evidence, criminal law reform).
ii. National Crime Records Bureau (NCRB) – "Crime in India" Reports
iii. CERT-In Annual Reports and Advisories.

iv. Ministry of Electronics and Information Technology (MeitY) Reports and Publications.
v. Ministry of Home Affairs (MHA) Reports and Publications on Cybercrime.
vi. Parliamentary Standing Committee Reports on IT, Home Affairs, or Law & Justice
vii. Reports by international bodies like UNODC, INTERPOL, Council of Europe (Budapest Convention) on cybercrime trends and legal frameworks.

VI. **International Conventions and Model Laws**
    i. Council of Europe Convention on Cybercrime (Budapest Convention).
    ii. UN Model Law on Electronic Commerce.
    iii. UN Model Law on Electronic Signatures