International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

Criminal Liability in the Digital Age: A Comparative and Behavioural Framework for Cybercrime in an AI-Driven World

Cumaran Nadaradjan
B.A., LL.B., LL.M. (Criminal & Cyber Law), Ph.D. (Criminal & Cyber Law)
Sabarmati University, Ahmedabad, Gujarat, India

Abstract
This advanced international-journal article develops a multidisciplinary framework for criminal liability in the digital age, with a particular focus on AI-enabled cybercrime, human behavioural vulnerability, and cross-jurisdictional legal fragmentation. Drawing on behavioural science, cyberpsychology, digital forensics, and comparative criminal law, the paper argues that cybercrime is best understood as a behaviourally scripted, technologically amplified phenomenon rather than a purely technical offence. Traditional doctrines of mens rea, actus reus, causation, and evidence, designed for physical acts in territorial spaces, face significant strain when applied to autonomous malware, deepfakes, botnets, crypto-ransomware, and large-scale social engineering campaigns. Using a mixed-methods approach that combines doctrinal analysis, cross-cultural behavioural insights, and case-law examination from India, the United States, the United Kingdom, the European Union, and Sweden, the article identifies recurring gaps in attribution, intent assessment, and evidentiary reliability. It then proposes a Hybrid Behavioural–Technological–Legal Liability Framework, incorporating a Behavioural Vulnerability Index, an Algorithmic Autonomy Spectrum, and a Multi-Actor Cyber Liability Grid. The conclusion calls for incremental harmonisation of cyber liability standards, integration of behavioural science into cyber legislation, and robust international cooperation to safeguard justice in an AI-driven digital ecosystem.

Keywords:- Cybercrime, Artificial Intelligence, Criminal Liability, Behavioural Vulnerability, Comparative Cyber Law

Introduction

Cybercrime has evolved from sporadic acts of digital mischief into a pervasive structural threat that implicates national security, financial stability, democratic integrity, and everyday privacy. The emergence of artificial intelligence (AI), machine learning, big data analytics, and deepfake technologies has transformed the scale, precision, and psychological impact of cyber offences. In contrast, criminal law in most jurisdictions remains anchored in paradigms crafted for tangible acts, localised harm, and clearly identifiable offenders. Doctrines such as mens rea (guilty mind), actus reus (guilty act), causation, and evidentiary standards were not designed to contend with

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

self-propagating malware, anonymised networks, algorithmically tailored phishing, or synthetic media that can convincingly impersonate anyone. This doctrinal–technological gap has practical consequences: many cyber offences are under-reported, under-investigated, or under-prosecuted, and even when offenders are identified, courts struggle to evaluate intent, foreseeability, and responsibility.

At the same time, cybercrime is fundamentally rooted in human behaviour. Social engineering attacks, business email compromise, romance fraud, spear-phishing, and deepfake voice scams all exploit predictable cognitive shortcuts, emotional states, and social norms. A bank employee in Mumbai, a nurse in Stockholm, or a small business owner in Texas may all respond similarly when confronted with urgent, authority-framed digital instructions. These offences rarely require highly sophisticated technical exploits; instead, they weaponise fear, trust, curiosity, and fatigue. Legal systems that implicitly assume the "reasonable person" model in victim behaviour risk overlooking the systemic, predictable, and often engineered nature of digital manipulation.

This article advances three core arguments. First, that cybercrime should be conceptualised as a behaviour–technology hybrid in which psychological manipulation and technological mediation operate together. Secondly, that existing doctrines of criminal liability require context-sensitive adaptation rather than wholesale abandonment; concepts such as intention and causation can be refined to account for autonomous systems and distributed harm. Thirdly, that comparative and cross-cultural analysis offers valuable lessons for harmonising cyber liability and fostering mutual legal assistance in cyber investigations. By synthesising legal, psychological, and technological insights, this paper aims to contribute a nuanced framework suitable for international discourse on cyber liability.

Theoretical Framework

The theoretical foundation of this article rests on the intersection of behavioural science, technological autonomy, and comparative criminal law. Four interlocking models are proposed.

1. **Cyber-Behavioural Vulnerability Model (CBVM)**

The CBVM posits that cybercrime succeeds primarily by exploiting cognitive biases and emotional states. Drawing from social psychology and cyberpsychology, it emphasises authority bias, urgency bias, trust and familiarity heuristics, confirmation bias, and decision fatigue. These factors reduce critical scrutiny and promote compliance with malicious digital prompts. The model challenges the traditional legal assumption that victims act as rational agents capable of consistently resisting deception.

2. **Algorithmic Autonomy Spectrum (AAS)**

The AAS conceptualises digital tools on a spectrum from fully controlled instruments (e.g., manually executed scripts) to highly autonomous systems (e.g., self-learning malware that adapts without human input). Liability analysis must consider where on this spectrum an offending tool

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

lies. At one end, intention tracks closely to human action; at the other, questions arise about foreseeability, risk-taking, and constructive intent.

3. **Multi-Actor Cyber Liability Grid (MAC-LG)**

Cyber offences often involve multiple actors: coders, operators, infrastructure providers, money mules, and unwitting intermediaries. The MAC-LG offers a matrix for mapping each actor's contribution to the offence—design, deployment, facilitation, monetisation—and aligning it with gradated forms of liability (principal, accomplice, conspirator, negligent enabler).

4. **Cross-Border Digital Harm Principle (CDHP)**

The CDHP builds on emerging scholarship that treats cyber harm as inherently transnational. It argues that jurisdiction, attribution, and liability should be guided not only by territorial presence, but by the locus of harm, the targeting of victims, and the role of states in hosting critical infrastructure. This principle underpins calls for greater alignment between national cybercrime statutes and international frameworks such as the Budapest Convention.

Expanded Literature Review

Early cybercrime scholarship largely focused on technical exploits and network vulnerabilities. Over time, however, researchers have increasingly recognised the behavioural and legal dimensions of digital offences. Brenner (2010) describes the "jurisdictional maze" faced by prosecutors when attacks span multiple countries, arguing that traditional territorial assumptions are ill-suited to cyberspace. Kerr (2018) examines how the Computer Fraud and Abuse Act (CFAA) in the United States has generated inconsistent case law, particularly around the concept of "unauthorised access," prompting debates about over-criminalisation and vagueness. European scholars, by contrast, have emphasised rights-based approaches under instruments such as the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directives, which link cybersecurity obligations to data protection and digital autonomy.

On the behavioural side, Hadlington (2017) and Parsons et al. (2019) highlight that human error and risky online habits are central to most data breaches. Their work shows that security training alone is insufficient; emotional regulation, workload management, and organisational culture play critical roles in determining whether individuals adhere to secure practices. Mitnick and Simon (2002) popularised the idea of humans as the "weakest link," while later empirical studies by Vishwanath and colleagues refined our understanding of how stress, multitasking, and habituation erode individuals' capacity to distinguish legitimate requests from fraudulent ones.

Criminological literature, including Holt, Bossler, and Seigfried-Spellar (2015), situates cybercrime within broader theories of opportunity, routine activities, and social learning. Offenders are shown to leverage online forums, encrypted messaging platforms, and darknet markets to share tools, techniques, and criminal "scripts." McGuire and Dowling (2013) describe

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

cybercrime as a "hyper-connected risk," noting the blurring boundaries between organised crime, state actors, and freelance hackers-for-hire.

Legal-technology scholarship has increasingly focused on AI and autonomous systems. Citron and Chesney (2019) assess the societal and legal implications of deepfakes, warning that synthetic media can erode trust in evidence, facilitate extortion and harassment, and create plausible deniability for wrongdoers ("the liar's dividend"). Casey (2011) and later digital forensics researchers warn that traditional evidentiary assumptions about integrity, authenticity, and chain-of-custody are challenged by the malleability of digital artefacts.

Comparative studies, including work commissioned by UNODC and Europol, document uneven capacities across jurisdictions to investigate and prosecute cyber offences. Nordic countries, including Sweden, tend to exhibit higher digital literacy, stronger institutional trust, and more integrated cybersecurity strategies, while rapidly digitising countries, including India, face surging cybercrime alongside incomplete legal frameworks and resource constraints. This literature points towards the need for both domestic reform and international coordination.

Methodology

Given the normative and cross-disciplinary objectives of this article, a mixed-methods approach was adopted. First, a doctrinal analysis was conducted of key statutory instruments and policy documents, including the Indian Information Technology Act 2000 and its amendments, relevant provisions of the Indian Penal Code, the U.S. Computer Fraud and Abuse Act, the UK Computer Misuse Act, EU directives and the GDPR, and Sweden's cyber-related legislation. Case law was reviewed to trace judicial reasoning on intent, access, harm, and intermediary liability.

Second, a synthesis of behavioural and cyberpsychology research was undertaken, focusing on empirical studies that examined susceptibility to phishing, social engineering, and digital fraud. These findings were mapped against doctrinal requirements for reasonableness, consent, and victim responsibility.

Third, a comparative case-study method was applied, selecting illustrative judgments from India, the United States, the United Kingdom, Germany, EU institutions, and Sweden. Cases were chosen to reflect a diversity of offence types (e.g., unauthorised access, denial-of-service, deepfake fraud, business email compromise) and to highlight different judicial approaches to cyber liability.

Finally, the insights from doctrinal, behavioural, and comparative analysis were integrated into a conceptual Hybrid Behavioural–Technological–Legal Liability Framework, designed to support future legislative and policy reform.

Key Findings and Discussion

The analysis yields several key findings. First, behavioural vulnerabilities are systematically exploited across jurisdictions, yet legal doctrine often treats victim behaviour as idiosyncratic

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

rather than predictable. Court judgments occasionally imply that victims "should have been more careful," without recognising the engineered nature of social engineering attacks. Second, AI-enabled tools such as deepfakes and autonomous malware complicate traditional notions of intention and causation. Offenders may deploy tools whose subsequent evolution exceeds their precise foresight, but not necessarily their awareness of risk. Third, cross-border fragmentation in cybercrime statutes, evidentiary rules, and mutual legal assistance procedures creates gaps that offenders actively exploit.

In light of these findings, the article argues for a recalibrated understanding of mens rea that accounts for risk-taking with powerful autonomous tools; an expanded concept of actus reus that includes code deployment and configuration as legally significant acts; and a more nuanced approach to causation in distributed, multi-actor digital environments. Behavioural science should inform judicial interpretation of victim behaviour, reducing unfair victim-blaming and emphasising the foreseeability of manipulation in high-pressure digital contexts.

Conclusion

Cybercrime in an AI-driven era presents one of the most serious tests for criminal law's adaptability. This article has argued that meaningful reform must recognise the hybrid behavioural–technological nature of digital offences, refine existing liability doctrines to address autonomous systems and distributed harm, and embrace comparative and international perspectives. The proposed Hybrid Behavioural–Technological–Legal Liability Framework is not a final solution, but a starting point for legislators, judges, and scholars seeking to align legal responsibility with the realities of contemporary cybercrime. As technology continues to evolve, the legitimacy of criminal justice systems will depend on their ability to protect individuals from digital harm while safeguarding due process, proportionality, and human dignity.

References

1. Brenner, S. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
2. Kerr, O. (2018). The Law of Cybercrime. Journal of Criminal Law & Criminology, 108(2).
3. McGuire, M., & Dowling, S. (2013). Cyber Crime: A Review of the Evidence. UK Home Office.
4. Citron, D., & Chesney, R. (2019). Deepfakes and the New Disinformation War. California Law Review, 107(6).
5. Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.
6. Hadlington, L. (2017). Human Factors in Cybersecurity. Cyberpsychology, Behavior, and Social Networking, 20(10).
7. Parsons, K., et al. (2019). The Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 87.

8. Mitnick, K., & Simon, W. (2002). The Art of Deception. Wiley.
9. Vishwanath, A., et al. (2016). Suspicion, Cognition, and Automaticity: Phishing Vulnerability. Journal of Computer-Mediated Communication, 21(1).
10. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. (2015). Cybercrime and Digital Forensics. Routledge.
11. UNODC. (2023). Global Cybercrime Trends Report.
12. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA).
13. NCRB. (2023). Crime in India: Cybercrime Statistics.
14. Halder, D., & Jaishankar, K. (2011). Cyber Crimes Against Women in India. Sage.
15. Goodman, M. (2015). Future Crimes. Random House.