THE LAWWAY WITH LAWYERS JOURNAL

VOLUME:-29 ISSUE NO:- 29 , NOVEMBER 26, 2025

ISSN (ONLINE):- 2584-1106

Website: www.the lawway with lawyers.com

Email: thelawwaywithelawyers@gmail.com

Digital Number : 2025-23534643

Authored By :- Tapur , Usha Martin University Ranchi Jharkhand

THE INTERSECTION OF TECHNOLOGY AND CRIMINAL LAW

Abstract

The intersection of technology and criminal law feels less settled than it might appear. Digital tools reshape not only how crimes are committed, but how intent and evidence are understood. A mobile phone, for instance, can quietly map a person's movements, while a simple phishing email can cause serious financial harm. However, the law often responds after the damage is done, struggling with cross-border enforcement and evolving offences. There is also a tension between control and freedom. Stronger regulation may help, yet it risks intruding on privacy. What emerges is not a fixed framework, but an ongoing negotiation shaped by constant technological change.

Keywords

Technology, Intent, Evidence, Jurisdiction, Enforcement, Rights.

Research methodology

This study follows a largely doctrinal approach, though not in a rigid sense. It draws on statutes, case law, and academic writing to understand how criminal law is responding to technological change. At the same time, a comparative glance is taken where useful, especially when dealing with cross-border cyber issues. However, the method is not purely theoretical. Real-world illustrations, such as phishing scams or data breaches, are used to ground the discussion. There is some limitation here. Rapid technological change means the analysis may not capture every emerging trend. Still, it offers a reasoned snapshot of an evolving legal landscape.

Introduction

The intersection of technology and criminal law is not as clear-cut as it first appears. At one level, it seems simple. New technologies emerge, new offences follow, and the law steps in to regulate them. But when you look a little closer, things begin to feel less settled. Technology

does not just create new forms of crime. It changes how actions are carried out, how intent is understood, and even how evidence is gathered.1

Take something as ordinary as a mobile phone. It can record location, store conversations, and reveal patterns of behaviour without the user fully realising it. In a criminal investigation, that device can become more reliable than any human witness. However, this raises uncomfortable questions about privacy and control. The same tools that help solve crimes can also monitor everyday life in ways that feel excessive.2

There is also a deeper issue. Technology is not neutral. It shapes choices, nudges behaviour, and creates environments where certain actions become easier than others. Some scholars argue that these built-in influences complicate how responsibility is assigned in law.3 That claim is persuasive, although perhaps not complete. People still make decisions, even within constrained systems.

The relationship here is not just regulatory. It is ongoing, a kind of negotiation. Law tries to keep pace, while technology quietly redraws the boundaries of what is possible.

Evolution and Nature of Cybercrime

The evolution of cybercrime feels less like a straight line and more like a series of quick adjustments. In its early stages, it was almost tentative. Small intrusions, basic scams, and individuals testing what systems would allow. It is tempting to see those moments as harmless experimentation, but they quietly exposed how fragile digital spaces could be.4

Things have shifted since then. Cybercrime today often looks organised, even structured. Ransomware attacks, data breaches, coordinated fraud schemes. These are not random acts. They are planned, sometimes with a level of precision that resembles legitimate business operations. What is striking, though, is how invisible much of this remains. No physical trace,

1R. Rahardjo et al., The Role of Information Technology in Environmental Sustainability, in E3S Web of Conf. vol. 31, 12011 (2018),

2*Frank Schmalleger,Criminal Law Today* (7th ed. 2021),https://studentebookhub.com/wp content/uploads/2024/preview/9780135970386.pdf

3*Philip Brey, Theorising Technology and Its Role in Crime and Law Enforcement, inThe Routledge Int'l Handbook of Technology, Crime and Justice* 17–34 (M.R. McGuire & Thomas J. Holt eds., 2017),https://www.4tu.nl/ethics/downloads/default/files/brey-2017-theorizing-technology.pdf

4*Lika Chimchiuri, The Evolution of Cybercrime Legislation,Sci. Works Nat'l Aviation Univ. Ser. L. J. Air & Space L.* 2(71), 221–227 (2024),https://www.researchgate.net/profile/Lika Chimchiuri/publication/383555364_THE_EVOLUTION_OF_CYBERCRIME_LEGISLATION/links/691dc699e870980 f18f29637/THE-EVOLUTION-OF-CYBERCRIME-LEGISLATION.pdf

no immediate confrontation. Just systems failing, money disappearing, identities being misused. The harm is real, yet oddly difficult to locate in a traditional legal sense.5

The law has tried to respond, though usually after the fact. New rules emerge once gaps become too obvious to ignore. However, this reactive pattern leaves inconsistencies, especially when crimes cross borders so easily. Enforcement becomes uneven, and jurisdiction itself starts to feel uncertain.6

Moreover, not all cybercrime depends on technical sophistication. A simple phishing email, crafted with just the right urgency, can be more effective than complex code. The nature of cybercrime sits somewhere between human behaviour and technological possibility, which makes it harder to fully contain.7

Types of Technology – Related Offences

When people talk about technology-related offences, they often imagine highly technical crimes carried out by expert hackers. That image is not entirely wrong, but it feels incomplete. The range of offences is much broader, and, in some ways, more ordinary than we might expect. At one end, there are offences like unauthorised access or hacking, where individuals break into systems to extract or manipulate data. These acts can be sophisticated, but sometimes they rely on surprisingly simple vulnerabilities, like weak passwords or outdated software.8

Then there are offences that use technology as a tool rather than a target. Online fraud is a good example. A fake email posing as a bank alert, sent at the right moment, can persuade someone to reveal sensitive details within minutes. It is less about technical brilliance and more about understanding human behaviour. That, perhaps, is what makes such offences so persistent.9

Other forms are harder to categorise neatly. Cyberstalking, identity theft, and the distribution

of harmful content occupy a space between traditional crime and digital innovation. The harm

5*Benoît Dupont, Francis Fortin & Rutger Leukfeldt, Broadening Our Understanding of Cybercrime and Its Evolution,47 J. Crime & Just.* 435 (2024), https://doi.org/10.1080/0735648X.2024.2323872 6Rep.

7*Author(s), Title of Article,Applied Sci.* 15(8), 4156 (2025), https://www.mdpi.com/3504156. 8*R. Ahmad & R. Thurasamy, Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes,11 J. Cyber Sec. & Digital Forensics 405 (2022),*https://journals.riverpublishers.com/index.php/JCSANDM/article/view/12451. 9*Mike McGuire & Samantha Dowling,Cyber Crime: A Review of the Evidence, Home Office Research Report No. 75, ch. 1: Cyber-Dependent Crimes* (Home Office 2013),https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf

is real, often deeply personal, yet the method feels less visible. Moreover, large-scale attacks like ransomware blur the line between criminal activity and organised enterprise, sometimes even resembling structured business models.10

While categories exist, they are not always stable. Technology keeps shifting the boundaries, and the law follows, though not always with complete clarity.

Legal Framework Governing Cybercrime in India

The legal framework governing cybercrime in India feels both deliberate and, at times, slightly strained under pressure. At its centre is the Information Technology Act, 2000, which was introduced when the internet was still finding its place in everyday life. Back then, concerns were relatively narrow. Unauthorised access, data theft, basic forms of online fraud. The law addressed these issues with a certain clarity. However, the digital environment did not remain that simple for long.11

Over the years, amendments and supplementary provisions have tried to keep pace. Sections dealing with identity theft, online impersonation, and obscene digital content reflect this effort. One can see it in cases involving cyber pornography or the circulation of explicit material, where the law attempts to balance regulation with constitutional freedoms. That balance, though, is not always easy to maintain. Questions about overreach and misuse do surface, and not without reason.12

There is also the continued reliance on traditional criminal law, particularly the Indian Penal Code, to fill gaps. This creates a kind of overlap. Sometimes it works well, offering flexibility. At other times, it leads to confusion about applicability and enforcement.

10*Siniša Franjić, Cybercrime is Very Dangerous Form of Criminal Behavior and Cybersecurity,4 Emerging Sci. J. 18 (2020),*https://doi.org/10.28991/esj-2020-SP1-02.

11*Juneed Iqbal & Bilal Maqbool Beigh, Cybercrime in India: Trends and Challenges,6 Int'l J. Innovations & Advancement Comput. Sci. 187 (2017),https://www.researchgate.net/profile/Juneed Iqbal/publication/322245372_Cybercrime_in_India_Trends_and_Challenges/links/5a4e040c458515a6bc6ea9e 3/Cybercrime-in-India-Trends-and-Challenges.pdf*

12*Saquib Ahmed & Rishikesh Faujdar, An Overview of Cyber Pornography in India, inCyber Crime, Regulation and Security: Contemporary Issues and Challenges* 264 (Pradeep Kulshrestha, Anita Singh & Ritu Gautam eds., 2022),https://www.researchgate.net/profile/Rishikesh Faujdar/publication/367095979_An_Overview_of_Cyber_Pornography_in_India/links/69023789368b49329fa8 0d34/An-Overview-of-Cyber-Pornography-in-India.pdf

Moreover, practical challenges remain. Limited technical expertise, underreporting, and jurisdictional complications often weaken implementation.13

So while India's legal framework is certainly evolving, it does not feel entirely settled. It reflects an ongoing attempt to adapt older legal thinking to a space that resists being neatly defined.

Landmark case laws :

Shreya Singhal v. Union of India14 in this case it was held that concern was strongly addressed in Shreya Singhal v. Union of India (2015), where

the Supreme Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional. The Court held that vague and overbroad provisions regulating online speech violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution. This judgment highlights the risk of excessive state control in digital spaces and reinforces the need for precise legal drafting in cybercrime legislation.

K.S. Puttaswamy v. Union of India15 it was held that The Supreme Court in K.S. Puttaswamy v. Union of India (2017) recognised the right to privacy as a fundamental right under Article 21 of the Constitution. This landmark judgment has significant implications for digital surveillance, emphasising that any state action involving data collection or monitoring must satisfy tests of legality, necessity, and proportionality. In the context of cybercrime regulation, this decision serves as a critical safeguard against unchecked surveillance.

Anvar P.V. v. P.K. Basheer16 it was held that the issue of electronic evidence has been clarified in Anvar P.V. v. P.K. Basheer (2014), where the Supreme Court held that electronic records are admissible only if they comply with the requirements under Section 65B of the Indian Evidence Act, 1872. This ruling underscores the technical and procedural challenges

13*Savannah Tuscany Smit, A Look at Victim Experiences of Cybercrime in South Africa and Whether the Current Legislative Framework Is Equipped to Deal with This Issue* (LL.M. thesis, University of Cape Town 2024),https://open.uct.ac.za/server/api/core/bitstreams/32bd3c47-a689-4d92-a303-0a89d9b6fae6/content 14 "Manupatra Academy" <https://www.manupatracademy.com/LegalPost/MANU_SC_0329_2015> accessed April 4, 2026.

15 "JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA – South Asian Translaw Database – PRIVACY" (South Asian Translaw Database, October 7, 2018) <https://translaw.clpr.org.in/case-law/justice-k-s puttaswamy-anr-vs-union-of-india-ors-privacy/> accessed April 4, 2026.

16 Amartya Bag, "Presentation of Electronic Evidence in Court in Light of the Supreme Court Judgment in Anvar P. K. vs. P.K Basheer & Ors." (iPleaders, September 22, 2014) <https://blog.ipleaders.in/presentation-of electronic-evidence-in-a-court-in-light-of-the-supreme-court-judgment-in-ansar-p-k-vs-p-k-basheer-ors/> accessed April 4, 2026.

involved in proving cyber offences, as improper handling of digital evidence can render it inadmissible in court.

International Framework :

The global nature of cybercrime necessitates international cooperation, as offences frequently transcend national borders and involve multiple jurisdictions. In this context, the Budapest Convention on Cybercrime (2001) represents the first and most comprehensive international treaty addressing cybercrime. It seeks to harmonise national laws, improve investigative techniques, and promote cooperation among states in tackling cyber offences. The Convention categorises cybercrimes into offences against the confidentiality, integrity, and availability of

computer systems, as well as computer-related fraud and content-related offences. It also establishes procedural mechanisms, such as expedited preservation of data and cross-border access to stored information, to facilitate effective investigation. Although India is not a signatory to the Convention, it often draws upon its principles in shaping domestic cyber law policy and international cooperation strategies. The Convention thus serves as an important benchmark in understanding the global legal response to cybercrime, even for non-member states.

Challenges in Investigation and Enforcement

The investigation of cybercrime rarely gives the kind of clarity that traditional criminal cases sometimes offer. There is no obvious crime scene to secure, no physical trail to preserve in the usual sense. Instead, everything depends on digital traces that can be copied, altered, or quietly erased.17 An investigator may start with a suspicious login attempt or a fraudulent transfer, only to discover that the data has passed through several servers across different countries. At that point, the process becomes less about finding answers and more about piecing together fragments that may or may not fit neatly.

Attribution, in particular, feels like one of the most persistent difficulties. It is not enough to show that a system was compromised. The law demands a connection to a specific individual, and that connection is often obscured. Offenders use proxy networks, stolen identities, or

17*Mariam Nouh, Jason R. C. Nurse, Helena Webb & Michael Goldsmith, Cybercrime Investigators Are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement,* arXiv:1902.06961 (2019), https://arxiv.org/abs/1902.06961.

even hijacked devices belonging to ordinary users.18The evidence exists, but it can point in multiple directions at once, which complicates prosecution.

Jurisdictional issues make things even more uncertain. A single cyber incident might involve a victim in one country, infrastructure in another, and a suspect somewhere else entirely. Cooperation between states is possible, but it is rarely quick. Legal procedures differ, priorities vary, and sometimes political considerations quietly shape the outcome. Meanwhile, digital evidence does not wait. It can disappear or lose relevance before formal processes are completed.19

There is also the question of capacity. Not all enforcement agencies are equally equipped to handle technically complex cases. Some have advanced cyber units, while others rely on limited resources and general training. One might assume that better technology alone will resolve this imbalance. However, the issue seems broader than that. It involves coordination, legal clarity, and, perhaps, a shift in how institutions approach crime in a digital environment.

Emerging Technologies and Future Challenges in Criminal Law

Emerging technologies are beginning to test the limits of criminal law in ways that feel both subtle and disruptive. It is not always obvious where the problem lies. Sometimes the technology itself seems neutral, even

useful, until it is placed in the wrong hands. Consider how easily a realistic fake video can be created now. A person's face, voice, even mannerisms can be replicated with unsettling accuracy. The harm, when it occurs, is immediate and personal, yet the legal response often feels slightly delayed, as if it is still trying to name the offence properly.

At the same time, not every challenge is purely technical. Some of the most troubling issues, such as online exploitation or cyber pornography, show how digital platforms can intensify existing social harms rather than invent entirely new ones.20 That makes regulation more

18*E. F. G. Ajayi, Challenges to Enforcement of Cyber-Crimes Laws and Policy,6 J. Internet & Info. Sys. 1 (2016),*https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210 19*Maggie Brunner, Challenges and Opportunities in State and Local Cybercrime Enforcement,10 J. Nat'l Sec. L. & Pol'y 563 (2020),*https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2020/05/Challenges-and Opportunities-in-State-and-Local-Cybercrime-Enforcement.pdf.

20Saquib Ahmed & Rishikesh Faujdar, *An Overview of Cyber Pornography in India*, in **Cyber Crime, Regulation and Security: Contemporary Issues and Challenges** 264 (Pradeep Kulshrestha et al. eds., The Law Brigade Publishers 2022).https://www.researchgate.net/profile/Rishikesh Faujdar/publication/367095979_An_Overview_of_Cyber_Pornography_in_India/links/69023789368b49329fa8 0d34/An-Overview-of-Cyber-Pornography-in-India.pdf

complicated than it appears. It is not just about controlling software or networks, but about addressing behaviour that adapts quickly to new environments.

There is also a quiet tension in how far the law should go. Stronger regulation might prevent misuse, yet it can also affect privacy and innovation in ways that are difficult to reverse.21Therefore, the future of criminal law seems less about finding a final solution and more about constant adjustment, responding to technologies that refuse to stay still.22

Balancing Rights, Regulation, and the Future of Criminal Law

Balancing rights and regulation in the digital age feels less like applying clear rules and more like making careful, sometimes uneasy choices. On one hand, there is a strong push for tighter control. Governments want better surveillance tools, faster access to data, and broader powers to prevent cybercrime before it escalates. That instinct is understandable. If a coordinated online attack can disrupt banking systems or critical infrastructure overnight, waiting too long can carry real consequences.

Yet the other side of the picture is harder to ignore. Expanding state power, especially in digital spaces, does not come without cost. A system designed to monitor potential offenders can just as easily track ordinary individuals going about their daily lives. Think of location tracking or mass data collection. It may help solve crimes, but it also raises quiet

concerns about privacy and autonomy. The line between protection and intrusion becomes difficult to define.23

Moreover, emerging technologies like artificial intelligence complicate this balance even further. Automated decision-making in policing or sentencing promises efficiency, but it also risks embedding bias in ways that are not immediately visible. Some argue that better design and oversight can fix this. Perhaps. Still, the concern lingers.

21Olukunle Oladipupo Amoo et al., *The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System*, 21(2) **World J. Advanced Rsch. & Rev.** 205 (2024)

22Alan Mills, Jonathan White & Phil Legg, *GoibhniUWE: A Lightweight and Modular Container-Based Cyber Range*, 4(3) **J. Cybersecurity & Priv.** 29 (2024),https://www.mdpi.com/2624-800X/1/4/29 23Daniel Epps, *Checks and Balances in the Criminal Law*, 74 **Vand. L. Rev.** 1 (2021), available at https://openscholarship.wustl.edu/law_scholarship/1155.

The future of criminal law does not lie in choosing one side over the other. It lies in constant adjustment. Rights and regulation are not opposing forces so much as competing priorities that must be negotiated, again and again, as technology continues to evolve.24

Conclusion

When you step back, the relationship between technology and criminal law feels less like a problem to be solved and more like something we keep negotiating. The law still looks for clear intent, clear harm, clear responsibility. Technology, however, tends to blur those lines. A fake video ruining someone's reputation or a quiet data breach draining accounts does not fit comfortably into older legal categories. It almost asks the law to rethink its own assumptions.

At the same time, stronger rules are not a perfect answer. More surveillance might prevent harm, but it also changes how ordinary people live and behave, often in ways we barely notice at first. That trade-off is not easy to measure.

The future here seems uncertain, maybe inevitably so. The task is not to catch up once and for all, but to keep adjusting, carefully, knowing that both overreach and inaction carry their own risks.

24Maureen S. Hopbell, *Balancing the Protection of Children against the Protection of Constitutional Rights: The Past, Present and Future of Megan's Law*, 42 **Duq. L. Rev.** 813 (2004), available at https://dsc.duq.edu/dlr/vol42/iss2/