INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DETERRENCE IN THE DIGITAL AGE: A CRITICAL APPRAISAL OF THE CAPACITY OF INDIA'S CYBER-CRIME LAW TO PREVENT CYBER CRIME

AUTHORED BY - ADWAIT SHUKLA
Amity Law School, Amity University Madhya Pradesh, Gwalior
Under the guidance of Dr. Renu Goyal, Associate Professor

Abstract

India does not lack laws against cyber crime. The Information Technology Act, 2000, read with the general penal law and a thickening layer of subordinate rules, forbids a wide range of digital wrongdoing and threatens it with substantial punishment. Yet the recorded volume of cyber crime climbs steeply year after year, with reported cases rising from roughly fifty-two thousand in 2021 to over one lakh in 2024. This paper asks why prohibition on such a scale has so little preventive effect, and answers the question through the classical theory of deterrence, which holds that punishment restrains the rational offender only when it is reasonably certain, reasonably swift, and reasonably proportionate. Applying the three conditions of certainty, celerity, and severity to the Indian setting, the paper argues that the country's cyber law fails to deter not because its penalties are too light but because their imposition is neither sufficiently certain nor sufficiently swift. The digital environment, by its very architecture, defeats certainty and celerity while leaving severity untouched, and the difficulties of attribution, of electronic proof, of cross-border reach, and of institutional capacity are the specific channels through which that defeat occurs. The paper concludes that the reflexive enhancement of penalties is therefore misdirected, and that the restoration of deterrent force depends on the harder, slower work of raising the probability and the speed with which offenders meet a consequence.

Keywords: *cyber crime; deterrence; certainty of punishment; Information Technology Act, 2000; electronic evidence; cyber-crime enforcement; criminal justice.*

ISSN: 2582-6433

1. Introduction

A generation ago, a crime usually required the offender to be somewhere. The burglar had to cross the threshold, the forger had to handle the document, the swindler had to face the person he was cheating. Distance protected most people from most criminals most of the time. The networked computer has quietly removed that protection. A single person at a keyboard can now defraud strangers on three continents before lunch, freeze a hospital's records, or drain the savings of someone he will never meet. The crime has been detached from the criminal's body and from any particular place, and that detachment is what makes cyber crime a distinct problem rather than merely an old problem with new tools.

The law has responded, as legal systems do, by forbidding things. India's statute book now prohibits unauthorised access, the spreading of malicious code, online fraud and personation, identity theft, the violation of digital privacy, cyber terrorism, and a long list of related wrongs, and it attaches to them penalties that range from a few years' imprisonment to imprisonment for life. By the measure of what is forbidden and how heavily, the framework looks formidable. The trouble is that it does not appear to work. The official crime figures record a steep and uninterrupted rise in cyber offending even as the prohibitions have multiplied and the penalties have, in places, grown harsher.

This paper sets out to explain that gap between an imposing law and a rising crime, and it does so by adopting a particular vantage point — the vantage point of deterrence. The choice is deliberate. The distinctive instrument of the criminal law is punishment, and punishment earns its keep, in large part, by preventing the conduct it threatens. To ask whether cyber law deters is therefore to ask whether it is doing the essential thing that criminal law is for. The classical theory of deterrence supplies a precise way of asking: it teaches that punishment prevents crime only when three conditions are met, and that those conditions, in the digital environment, are met very unevenly.

The argument that follows is short to state and the rest of the paper is its elaboration. India's cyber law is severe but neither certain nor swift, and because certainty and speed matter far more to deterrence than severity does, the law threatens much while preventing little. The path to genuine prevention does not run through still harsher penalties; it runs through the unglamorous reconstruction of the machinery that makes punishment probable and prompt.

ISSN: 2582-6433

2. The Theoretical Frame: What Makes Punishment Deter

The intellectual roots of deterrence theory lie in the Enlightenment, in the work of Cesare Beccaria and Jeremy Bentham, and the theory was later sharpened by the economic analysis of crime associated with Gary Becker. Its premise is a model of the offender as a rational calculator who weighs the gain he expects from a crime against the cost he expects to suffer for it, and who refrains when the cost outweighs the gain. The criminal law supplies the cost in the form of punishment. On this account, the law deters by making the expected cost of crime exceed its expected benefit.

The theory does not treat all punishment as equally deterrent. It identifies three properties on which deterrent force depends. The first is certainty — the likelihood, as the offender perceives it, that he will be caught and made to answer. The second is celerity — the swiftness with which the consequence follows the act. The third is severity — the magnitude of the punishment itself. Beccaria insisted, and modern empirical criminology has broadly confirmed, that of these three it is certainty that does the heavy lifting. A near-certain prospect of a modest penalty restrains far more effectively than a remote prospect of a terrible one, because the rational offender discounts a punishment he does not expect to suffer almost to nothing, however dreadful that punishment may be on paper.

Celerity matters for a related reason. Deterrence works by forging, in the offender's mind, a link between the contemplated act and its expected consequence. A consequence that arrives promptly strengthens that link; one that arrives years later, if at all, dissolves it. Severity, by contrast, is the condition that intuition overrates and evidence deflates: beyond the point of proportionality, raising the penalty adds little to deterrence and may even subtract from it by straining the sense of justice on which the law's authority rests.

This frame is unusually well suited to cyber crime, and not by accident. The digital environment attacks all three conditions at once, but it attacks certainty and celerity hardest. Anonymity and the erasure of distance make the offender difficult to identify and slow to reach, collapsing both the probability and the speed of consequence. Severity alone survives intact, because severity is fixed by the legislature and is indifferent to the medium. A theory that ranks certainty above severity therefore predicts, before any data are consulted, that a digital criminal law heavy on penalties but light on enforcement will deter poorly. The remainder of this paper tests that prediction against the Indian reality.

ISSN: 2582-6433

3. The Nature of the Wrong to Be Deterred

Before assessing whether the law deters cyber crime, one must be clear about what cyber crime is, for its features are precisely what make it hard to deter. The term has no single statutory definition in Indian law; the governing Act lists particular forbidden acts rather than defining a category. For analytical purposes, cyber crime may be understood as any unlawful act in which a computer or network is the target of the wrong, the instrument by which it is done, or the place where evidence of it resides.

Within that understanding, the offences sort into recognisable families. Where the computer is the target, the wrong is done to the machine or its data — unauthorised access, the theft or corruption of data, the deployment of viruses, worms, and ransomware, and attacks that overwhelm a system until it can no longer serve its users. Where the computer is the instrument, a familiar wrong is committed by new means — fraud, cheating by personation, identity theft, stalking, and harassment, transformed by the medium into something with far greater reach and far less risk to the offender. Where the computer is the medium, the wrong lies in the content carried — obscene material, material depicting the sexual abuse of children, defamation, and incitement.

Fraud dominates this landscape. In the most recent year for which figures are available, a fraud motive accounted for roughly three-quarters of all recorded cyber-crime cases, and it is fraud, more than any other form, that drives the rising statistics. This matters for the argument, because fraud is the cyber offence that fits the rational-offender model most snugly: it is deliberate, planned, and committed for gain by people who do indeed weigh risk against reward. If deterrence theory applies anywhere in the digital domain, it applies to the offence that does the most damage.

Several characteristics recur across these families and together explain the deterrent difficulty. The offender is separated from the scene and shielded by anonymity, so the natural deterrent of being seen is absent. The crime ignores borders, so the offender often sits beyond the reach of the law that his victim invokes. The harm scales without effort, so one act of writing a program can victimise thousands. The evidence is electronic — abundant but fragile, and hedged about with demanding requirements of proof. Above all, the probability that any given offence will be traced to an identifiable, reachable, convictable person is very low. That last feature is simply the certainty deficit stated in the language of the crime rather than the language

ISSN: 2582-6433

of the theory, and it is the hinge of everything that follows.

4. The Framework on Paper: A Law Rich in Prohibition

India's principal cyber statute, the Information Technology Act, 2000, began life not as a crime-control measure but as an instrument to enable electronic commerce, modelled on an international template concerned with the legal recognition of electronic records. Criminal prohibition was, in the original design, almost an afterthought, grafted onto a commercial structure. That origin left a lasting mark: the penal provisions are extensive but unsystematic, and the Act says a great deal about what is forbidden and remarkably little about how the prohibitions are to be enforced.

The penal architecture was substantially enlarged by the amendment of 2008, which introduced offences of identity theft, cheating by personation through a computer resource, the violation of bodily privacy, and cyber terrorism, and which conferred on the executive the powers of interception, monitoring, and the blocking of content that have figured so prominently in the subsequent constitutional debate. Later amendments have continued to adjust the Act by indirect routes; among them, the Jan Vishwas legislation of 2023 formally removed from the statute book the much-criticised provision on "offensive" messages that the Supreme Court had already struck down years earlier, and the data-protection statute of the same year recast parts of the framework governing personal data.

Surveying the penalties as a whole establishes a fact essential to the argument: the framework is not deficient in severity. Many offences carry imprisonment of two or three years; cyber terrorism may attract imprisonment for life; offences involving child sexual abuse material attract heavy custodial terms. A person who consulted only the text would reasonably conclude that cyber crime is firmly deterred. The contradiction between that paper severity and the lived reality of rising crime is the puzzle the next section resolves.

Around the Act sits a growing body of subordinate regulation, most importantly the rules governing online intermediaries, which impose duties of diligence, require the removal of unlawful content on authoritative notice, and have been amended repeatedly, most recently with effect from late 2025 and with a tentative reach towards synthetically generated content. The general criminal law, freshly recast in 2023 into new codes, continues to apply alongside the special statute, and the institutional response is distributed across an emergency-response

ISSN: 2582-6433

team, a national coordination centre and reporting portal, state cyber cells, forensic laboratories, and sectoral regulators. The apparatus, in short, is elaborate. The question is whether it functions.

5. The Framework in Operation: A Law Poor in Consequence

Tested against the three conditions of deterrence, the Indian framework reveals a sharp imbalance. It satisfies severity amply and fails certainty and celerity gravely, and the failure is not incidental but structural, produced by identifiable breaks in the chain that runs from offence to consequence.

Certainty fails first at the stage of reporting. A large but unmeasurable share of cyber offences never enters the official record at all — victims of fraud may not realise their loss until the money is gone, victims of harassment may be silenced by shame, and businesses may suppress news of breaches to protect their reputation. What is never reported can never be punished, and the offender who observes that his victims do not complain learns that his risk is lower still. Certainty fails again at investigation, where anonymity, the use of intermediary servers, and the sheer volume of cases overwhelm the limited number of trained investigators and the limited capacity of forensic laboratories, so that most offences are never traced to a person. It fails a third time at prosecution and trial, where the demanding and, for a period, unsettled law governing the admissibility of electronic records has defeated otherwise sound cases on technical grounds. The cumulative product of these successive failures is a conviction rate that is very low in relation to the volume of offending — and a low conviction rate is simply low certainty expressed as a number.

Celerity fails for overlapping reasons. Digital investigation is slow; the courts carry a vast backlog; and where the trail crosses a border, the formal machinery of mutual legal assistance can consume years, during which evidence is lost and the trail goes cold. Against an offence that may be completed in seconds and its proceeds dispersed within minutes, a consequence that arrives, if at all, a decade later forges no deterrent link whatever. The offence is swift and the answer is glacial, and in the gap between them the law's preventive force leaks away.

Severity, meanwhile, sits intact and largely irrelevant. Here lies the paradox the theory dissolves: a severe punishment that is almost never imposed, and that arrives long after the act when it is imposed at all, is to the rational offender a remote and discountable risk. He surveys

ISSN: 2582-6433

a landscape in which the chance of being caught is small and the chance of a swift consequence smaller, and against that the nominal severity of a punishment he does not expect to suffer weighs very little. He offends. The rising statistics are not evidence that the theory is wrong; they are exactly what the theory predicts when severity is high but certainty and celerity are low.

6. The Channels of Failure: Why Certainty and Celerity Collapse

It is worth naming precisely the mechanisms through which certainty and celerity are eroded, because they are the points at which reform must be aimed. They are not separate problems alongside a deterrence problem; they are the anatomy of the deterrence problem itself.

The first is the problem of attribution. Connecting an offence to a reachable person is the indispensable first link in the chain, and the digital environment makes it hard at every level. Yet the offender's concealment is usually pseudonymity rather than true anonymity — penetrable, in principle, by sufficient investigative effort — which means the attribution deficit is to a large degree a remediable failure of capacity rather than an immovable fact of nature. That is, on the whole, an encouraging conclusion, for it implies that investment in the means of attribution can genuinely raise certainty.

The second is the evidentiary problem. Cyber offences leave their traces in electronic form, and electronic evidence must be collected, preserved, and authenticated to a demanding standard before a court will rely on it. The jurisprudence on the admissibility of such evidence has oscillated — strict, then briefly relaxed, then strict again — and every period of uncertainty has imperilled prosecutions. Where investigators and prosecutors lack the training to satisfy the rules, sound cases fail not because the accused is innocent but because the proof is wanting, and each such failure is a failure of certainty.

The third is the jurisdictional problem. The Act asserts an extra-territorial reach, but assertion is not exercise. The cross-border offender can be identified, evidenced against, and surrendered only with the cooperation of the state where he is found, and the machinery of that cooperation is slow, formal, and uncertain. As cyber crime becomes ever more international, an increasing share of it lies, in practice, beyond domestic reach — which is to say beyond both certainty and celerity at once.

ISSN: 2582-6433

The fourth is the capacity problem, which underlies the other three. The specialised investigators, forensic facilities, prosecutors, and judges on whom enforcement depends are too few, too thinly resourced, and too unevenly distributed to match the volume and complexity of the crime. The national reporting portal has improved the intake of complaints, but intake is not enforcement, and the machinery behind it struggles to convert complaints into investigations, investigations into prosecutions, and prosecutions into convictions. These channels interact and compound one another, so that none can be closed in isolation; the deficits of certainty and celerity are the joint product of the whole system of weaknesses, and they must be addressed as a system.

7. The Constitutional Boundary

The pursuit of certainty cannot be unconditional, for some of the law's instruments against cyber crime press against fundamental rights. The leading authority is the Supreme Court's decision in Shreya Singhal v. Union of India, which struck down the provision criminalising "offensive" online messages as unconstitutionally vague and over-broad, read down the safe- harbour provision so that an intermediary's duty to remove content is triggered only by a court order or a governmental direction rather than any private complaint, and upheld the power to block content subject to its procedural safeguards.

That decision carries a double lesson for a study of deterrence. The first is that prevention purchased by chilling lawful expression is bought too dearly; a law that deters crime by deterring speech does more harm than the crime it prevents. The second, less obvious, is that vagueness is a deterrent failing as well as a constitutional one. A law whose contours the citizen cannot discern invites arbitrary and selective enforcement, which the rational offender quickly learns to discount, so that clarity in the definition of offences serves prevention as much as it serves liberty.

The recognition of a fundamental right to privacy deepens the same tension on the investigative side. The powers of surveillance and interception that certainty may require must now be confined within safeguards that respect privacy, and the data-protection regime has begun, but only begun, to work out the balance. The constitutional setting is thus not merely a constraint on cyber law but a guide to its proper shape: certainty is to be pursued, but within limits that the pursuit must not overrun.

ISSN: 2582-6433

8. Towards Restoration: The Direction of Reform

If the diagnosis is sound, the prescription follows from it. Because the deterrent failure is a failure of certainty and celerity rather than of severity, reform must be directed at raising the probability and the speed of consequence, and not at the enhancement of penalties that are already ample. The reforms that matter share a single test: do they make consequence more likely or more prompt?

Raising certainty begins with narrowing the reporting gap, through reporting channels that are simple, accessible, and responsive, through the sensitive handling that encourages victims of personal offences to come forward, and through measured obligations of disclosure on businesses that suffer breaches. It continues with the building of investigative and forensic capacity — more trained investigators, better-equipped laboratories, stronger means of attribution, and processes for the rapid preservation of fragile evidence — which is the foundation on which all certainty must rest. It extends to the training of prosecutors and judges and the settling of clear, stable rules of electronic evidence, so that sound cases are not lost on technical grounds. And it reaches, finally, to international cooperation, without which the cross-border offender retains his practical impunity.

Raising celerity overlaps substantially with these measures, for the capacity that makes investigation reliable also makes it prompt; but it depends additionally on compressing the timelines of investigation and on the dedicated, expedited adjudication of cyber cases by personnel equipped to understand them. A particular and underused lever is the financial response: mechanisms that detect, freeze, and reverse fraudulent transfers before the proceeds are dispersed strike directly at the profitability of the dominant offence, and they do so with a speed and at a scale that the case-by-case criminal process cannot match. Denying the offender his gain may deter the profit-seeking fraudster more effectively than the remote threat of a conviction.

Two further measures complete the programme. The constitutional balance must be preserved by defining offences with precision and confining investigative powers within safeguards, so that the pursuit of certainty does not erode the liberty it is meant to protect. And prevention must complement deterrence: public awareness, directed especially at the inexperienced users who are the fraudster's favoured prey, denies the offender his victims and so reduces crime by a route that the threat of punishment cannot reach. None of this is cheap or quick, which is precisely why it is so often neglected in favour of the cheap and conspicuous gesture of penalty

ISSN: 2582-6433

enhancement. But there is no shortcut: certainty and celerity are bought only by sustained investment in the capacity to detect, to prove, and to punish, reliably and promptly.

9. Conclusion

The question with which this paper began — why a country with so many cyber laws suffers so much cyber crime — has a clear answer. India's cyber law is built the wrong way round for deterrence. It is strong in the condition that deters least, severity, and weak in the two that deter most, certainty and celerity. The offender, calculating rationally, sees a small chance of a slow consequence and is not restrained, and the rising statistics are the aggregate of millions of such calculations.

The deterrent perspective offers not only a diagnosis but a discipline. It insists that every proposed reform be judged not by how tough it sounds but by whether it raises the probability or the speed with which an offender meets a consequence. By that standard, much of what passes for cyber-law reform — the multiplication of offences, the raising of penalties — misses the point entirely, while the real work lies in the patient, expensive, unglamorous reconstruction of the machinery of enforcement.

Cyber crime will not be abolished; no crime ever has been. But it can be deterred, in the only sense in which any crime is deterred — reduced to a level at which the would-be offender, facing a real and reasonably swift risk of consequence, more often chooses not to act. India has written the prohibitions and prescribed the punishments. What remains, and what this paper has argued is the true task, is to make those punishments certain and prompt. Until that is done, the statute book will go on threatening much and preventing little, and the figures will continue their melancholy climb.

References

[1] Cesare Beccaria, On Crimes and Punishments (Henry Paolucci trans., Bobbs-Merrill 1963) (originally published 1764).

[2] Jeremy Bentham, An Introduction to the Principles of Morals and Legislation (1789).

[3] Gary S. Becker, "Crime and Punishment: An Economic Approach", 76 Journal of Political Economy 169 (1968).

[4] Daniel S. Nagin, "Deterrence: A Review of the Evidence by a Criminologist for

ISSN: 2582-6433

Economists", 5 Annual Review of Economics 83 (2013).

[5] The Information Technology Act, 2000 (Act 21 of 2000).

[6] The Information Technology (Amendment) Act, 2008.

[7] The Jan Vishwas (Amendment of Provisions) Act, 2023.

[8] The Digital Personal Data Protection Act, 2023.

[9] The Bharatiya Nyaya Sanhita, 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023.

[10] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by the Amendment Rules, 2025.

[11] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[13] Sharat Babu Digumarti v. Government (N.C.T. of Delhi), (2017) 2 SCC 18.

[14] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[15] National Crime Records Bureau, Crime in India (Ministry of Home Affairs, Government of India), reports for 2021, 2022, 2023 and 2024.