# CYBER CRIME AND ETHICS: EXAMINING THE BOUNDARIES OF ETHICAL HACKING IN INDIAN JURISPRUDENCE

Tamanna, LL.M, University Institute of Legal Studies, Chandigarh University

**ABSTRACT**

The current research paper examines the role of ethical hacking as a developing concept in the cybersecurity situation and the legal framework that surrounds it in India. It also looks at how practices in digital penetration testing and coordinated vulnerability disclosure are able to meet the provisions of the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023 and procedural protections the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam.

The study is methodologically doctrinal by outlining the line between legal conduct of security research and criminal acts of cyber-crime through consent and proportionality, data protection and the responsible disclosure. It is pointed out in the analysis that the operational mandate of CERT-In was found in Section 70B of the IT Act and the standards of evidence of digital records were found in Section 63 of BSA.

The paper uses the concept of safe harbour in protecting the bona-fide researchers so that concomitant improvement is made towards the sphere of cybersecurity, and personal rights are safeguarded.

**Keywords:** Ethical hacking, Information Technology Act 2000, Digital Personal Data Protection Act 2023, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, CERT-In, cybersecurity law, coordinated vulnerability disclosure, data protection, safe harbour, penetration testing, bug bounty, digital evidence.

## 1. INTRODUCTION

The paper cites ethical hacking as a component of India's changing model for managing cyber crimes and portrays the idea that a permissive and well-governed security research program can contribute to the deterrence of crimes, all the while preserving individual rights and ensuring procedural fairness. The storyline moves across different aspects of the law starting from unauthorized access under the liability line of the "Information Technology Act, 2000" and consent and breach-notice duties under the "Digital Personal Data Protection Act, 2023" as well as evidentiary and procedural safeguards under the "Bharatiya Sakshya Adhiniyam" and the "Bharatiya Nagarik Suraksha Sanhita". Moreover, it also portrays CERT-In as the incident- response regime and logging norms as the risk purview. The research takes a step further and proposes a security research space boundary: research based on consent, necessity, proportion and responsibly disclosed should be free from punitive outcomes and on the other hand, unauthorized and data protection rule-violating acts should be triggering statutory consequences and allowing for evidentiary follow-through. Points to the IT Act sections 43 and 66, DPDP Act sections 4, 7, and 8, BNSS section 105, and the BSA on electronic records as primary evidence are given as references.[1]

The rise in cyber threats in India is reflective of the widespread digitization of payments, e-governance, and platformised services. The transition to the cloud, the application of IoT, and the use of third-party systems have all contributed to the expansion of the attack surfaces. The liability scheme in the IT Act sends a very clear message: any unauthorized access, downloading, introduction of malware, or disruption of systems will lead to civil compensation under "Section 43" and become a criminal offense if done "dishonestly or fraudulently" as per "Section 66". Penetration testing and red-teaming are in a way the hands-on pre-emptive measures through which security flaws that can be, in the near future, used by adversaries are identified. They operate legally in the form of a cooperation issuing an explicit written consent by the owners of the system, containing scoping rules, data handling protocols, and agreed remediation timelines. Moreover, such a policy should reveal the connection between findings and DPDP Act controls: in case of the release of personal data, the security obligations of the fiduciary and breach analysis under "Section 8" and its sub-

[1] *The Information Technology Act, 2000, available at: https://www.indiacode.nic.in/bitstream/123456789/13116/ 1/it_act_2000_updated.pdf (last visited on October 3, 2025)*

sections, will be initiated, as well as internal logging and incident workflows.

Coordinated vulnerability disclosure is the bridge that links the discovery with the removal of the vulnerability. Time-limited disclosure windows, vendor acknowledgments, and public advisories after the release of patches are the main elements of keeping the trust while managing the risk. In cases where incidents affect national cybersecurity, the directions of CERT-In under "Section 70B" of the IT Act provide for the immediate reporting of events and the requirement of retention of logs for 180 days in India that grounds forensic verifiability and strengthens chain-of-custody narratives.[2]

## 2. OBJECTIVES

This subsection states the aims that guide the analysis.

- Establish a clearly defined fault line, by which a cyber conduct is considered punishable under the "Information Technology Act, 2000" and at the same time considered as a permissible security research when structured through authorization, data protection safeguards under the "Digital Personal Data Protection Act, 2023", and procedural–evidentiary controls in the "Bharatiya Nagarik Suraksha Sanhita" and "Bharatiya Sakshya Adhiniyam".

- Introduce standards for legitimate penetration testing, bug bounty involvement, and disclosure management that comply with the provisions of the DPDP Act, sections 4, 7, and 8, CERT-In's regime under Section 70B of the IT Act, and the BNSS section 105 and BSA section 63 based recording and admissibility framework.

## 3. METHODOLOGY

This research paper takes a doctrinal approach to primary materials and uses authoritative commentary for guidance. The legal frame of reference comprises various statutes like the "Information Technology Act, 2000", "Digital Personal Data Protection Act, 2023", "Bharatiya Nagarik Suraksha Sanhita", and "Bharatiya Sakshya Adhiniyam" along with an emphasis on "Section 43", "Section 66", "Section 70B", "Section 4", "Section 7", "Section 8", BNSS "Section 105", and BSA "Section 63". The study also looks at policy instruments

[2] *CERT-In Directions on Cybersecurity: An Explainer, available at: https://internetfreedom.in/cert-in-guidelines-on-cybersecurity-an-explainer/ (last visited on October 2, 2025).*

such as the CERT-In directions for the purpose of providing an operational context. A constrained comparative scan is used to highlight features of safe harbor and disclosure design, but it is still largely Indian sources and statutory text that inform the study. No case law is referred to here.

## 4. HISTORY AND CONSTITUTIONAL CONTEXT

India's interaction with ethical hacking has been a complicated and somewhat contradictory tale that is deeply rooted in the various laws and regulations it had to undergo. It has to do with the criminal law which is dealt with by the Information Technology Act, 2000, with data/ privacy-centric regulations under the Digital Personal Data Protection Act, 2023, and with changes in the procedures for criminal and civil courts, as per the latest amendments in the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023.

### 4.1 Early Phase

The initial period, which was between the day the IT Act was passed in 2000 and the 2008 amendments, embodied the legal terminology for computer misuse and intermediary responsibility and had an impact on security testing by the way they were understood. In the pre-amendment structure, only unauthorised access and data interference were punishable, but the 2008 changes enhanced the criminal exposure by confirming "Section 66" along with other offenses and also putting structured obligations on intermediaries and preparing a national incident-response backbone through "Section 70B" for CERT-In. Penetration testing and red teaming, in this context, were required to greatly indicate documented authorization, minimal data handling, and show proof-of-concept restraint so as not to cross the statutory line from civil wrong under "Section 43" to criminal conduct under "Section 66". The issue of intermediarial liability also developed further as it helped the ways how platforms were influenced by the reports from researchers and how the takedowns or remediation would be done without overbroad suppression. The overall impact was that while the environment was cautious, it was still not one that either completely shut down responsible security work or offering total protection; the selection design of ethical hacking depended on explicit authorization letters, bounded methodologies, and disclosure mechanisms that were in accordance with organisational incident workflows and privacy-by-design guardrails under the DPDP Act's "Section 8".

### 4.2 Privacy Turn

Privacy recognition as a fundamental right had an impact on setting the normative balance between the control of cybercrime and security research, and it required the state as well as private actors to observe the necessity and proportionality in surveillance, data processing, and investigation. The nine-judge bench in "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[3], made privacy a constitutional identity under Articles 14, 19, and 21, which in turn demands a check on measures that interfere with an individual's bodily integrity, informational self- determination, and decisional freedom. Consequently, the researcher controller relationships have to adapt to the change with lawful testing being accountable, limited data collection with storage discipline, and remediation that is accountable while organisational controllers have to incorporate notices, consents, and legitimate uses under "Section 4" and "Section 7" of the DPDP Act and implement security safeguards under "Section 8". Moreover, the investigatory powers that are now subject to stricter justificatory demands ensure that the officials' access to the researcher-generated artifacts, logs, or exploit code due process with calibrated scope. The BSA's "Section 63" on the admissibility of electronic records facilitates courts in this by providing a straightforward proof path; as a result, researchers and controllers are encouraged to keep disciplined documentation. The S.105 of BNSS on audio-video recording of search and seizure also appears to reduce the problem of how the collection and authenticity of the seized digital media are ensured. Overall, the constitutional recognition of privacy does not prevent intrusive conduct; instead, it advocates security research to go on under the conditions of consent, minimalism, and transparency and at the same time requires the state and firms to prove that the intrusion was the least harm pathway or the one that made the network more secure.

### 4.3 Free Speech and Due Process Online

As a result of the invalidation of vague offences related to online speech and the refinement of standards for intermediary liability, the environment for responsible disclosure, public advisories, and open technical discussion has significantly changed. The Supreme Court's decision in "*Shreya Singhal vs. Union of India*[4], not only struck down "Section 66A" of the IT Act for overbreadth and vagueness but also clarified that intermediary takedown

[3] *(2017) 10 SCC*
[4] *(2015) 5 SCC 1*

obligations had to be linked to lawful orders, thus reducing the number of private censorship incentives and arbitrary content removal. This decision for the security community meant fewer risks of vulnerability notes, proof-of-concept narratives, or coordinated disclosure statements being chilled by amorphous offences that were framed around annoyance or inconvenience. Accordingly, while the powers for blocking under "Section 69A" could still be exercised, they were accompanied by procedural checks that ensured precision and transparency in rare cases. The DPDP Act's model integrates a privacy focus to speech: if the technical writing is about personal data or shows exploits on live datasets, the controllers must ensure that the disclosure is in accordance with the laws of processing of data and security. Needless to say, the courts along with agencies get the help of "Section 63" of the BSA when they supervise electronic records that show the timelines of disclosure and commits of a repository and "Section 105" of the BNSS is there to help reliable capturing of seizures which are linked with alleged exploit misuse. The post-Shreya setting allows for an open security discourse as well as coordinated disclosure that respects user rights without falling into the vagueness trap which once was a threat to legitimate technical speech.

## 5. LEGISLATIVE FRAMEWORK

India's way of dealing with ethical hacking is fundamentally situated between the fight against cybercrime and the facilitation of security research. In many ways, the legislative framework mirrors this ambiguity that exists between these two areas. The "Information Technology Act, 2000" outlines the main illegal activities and the powers that the government will have; the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" define rights and roles and ways of appeal for platforms; the "Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules" 2009 regulate blocking; and the "CERT-In Directions" make the time for incident reporting shorter from days to hours. In these "Digital Personal Data Protection Act, 2023" parallel scenarios, the code of conduct of researchers is designed considering the fact that they might come across personal data during the tests. The risk of criminal activities overlapping with the "Bharatiya Nyaya Sanhita, 2023" persists in phishing, credential stuffing, or document forgery cases, while the "Bharatiya Nagarik Suraksha Sanhita, 2023" and the "Bharatiya Sakshya Adhiniyam, 2023" take care of the

process and proof.[5]

### 5.1 Information Technology Act, 2000

The "Information Technology Act, 2000" fundamentally marks out boundaries that ethical hackers are not allowed to cross without specific permission. "Section 43" establishes accountability for the acts of access, download, or disruption without authorization; however, by the virtue of an engagement letter, the same action becomes a consented "access", thus, the hacker is no longer liable but rather providing a contractual service. "Sections 66, 66C, 66D, and 66F" describe the escalation of the offenses: unauthorized access with a dishonest purpose, identity theft by using the victim's credentials or tokens, cheating by personation through computer resources, and cyber-terrorism, respectively. "Section 69A" allows for the blocking of content via a rule-based process, whereas "Section 70" identifies and protects the critical information infrastructure that hard-coded security is not allowed to be tampered with by ethical hackers without explicit, documentable authorization. "Section 70B" sets up CERT-In and lays the foundation of coordinated vulnerability disclosure interfaces. "Sections 72 and 72A" impose punishments for leak of confidentiality done even with consent in lawful contracts, which becomes important if testers are in possession of client data. "Sections 79 and 85" deal with the safe harbour for intermediary due diligence and company-officer vicarious liability, respectively, thus, indicating how platforms could operate bug bounties programs whereas corporate approvals should be defined. In consonance with these clauses, written authorization, scoping to defined systems, and data-minimised methods are the ones that take the testing to be a legitimate security service rather than an unlawful intrusion.[6]

### 5.2 Data Protection Overlay

"Digital Personal Data Protection Act, 2023" stitches the ethical hacking landscape with several obligations which come up whenever the testing process has an impact on the personal data. Lawful processing should be based on a valid ground such as consent or a documented contractual necessity with the client as "Data Fiduciary", and the act highlights purpose limitation, data minimisation, accuracy, security safeguards, and breach notification to affected individuals and the Data Protection Board. In such a test, the researchers have to

[5] *Supra Note 1*
[6] *Section43 of the Information Technology Act, available at: https://cis-india.org/internet-governance/resources/section-43-it-act.txt (last visited on September 30, 2025).*

design the tooling in a way that personal data are not collected unless it is absolutely necessary for the test objective, synthetic or anonymized datasets should be used, and any incidental personal data should be segregated in controlled repositories with deletion protocols on closure.[7]

### 5.3 Criminal Law Cross-Overs

Ethical hacking, which is beyond the scope of authorization, is often classified as conventional offences under the "Bharatiya Nyaya Sanhita, 2023". "Section 318" of the cheating acts describes fraud, which is the inducement of a victim to part with their property or to do something against their interest, and in the case of a phishing test that is performed without consent, it is quite relevant. "Section 319" dealing with cheating by personation can be reinterpreted to impersonation based intrusions, while "Section 324" regarding mischief can combine the aspect of damage to physical property with the new frame that extends to digital property or service availability. "Section 336" on forgery, in particular, refers to electronic records, thus being highly relevant to the forgery of invoices, certificates, or access tokens that are created to escalate privileges in a test beyond the scope of the agreed one.[8]

### 5.4 Civil and Contractual Dimensions

The legal layer of the private law establishes whether a penetration test is a service delivered with the consent of the test or a tortious interference. In general, standard terms of service prohibit such actions as probing, scraping, or reverse engineering, so the scope of work specifically designed with the asset owner is the tool that provides authorization and allocates risk. Non disclosure agreements must be aimed at limiting researcher access to client data, thereby coordinating with "Section 72A of the Information Technology Act, 2000" that imposes a penalty for the disclosure of information in violation of a lawful contract; this works in conjunction with "Section 72" concerning confidentiality obtained in official capacities. Properly constructed statements of work define the parameters of IP addresses, domains, time windows, attack classes excluded, data handling, vulnerability rating standards, remediation windows, and disclosure timelines. Civil offenses such as trespass to chattels and passing off may be among the charges in cases of abusive probing, especially

[7] *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 2, 2025)*

[8] *https://uppolice.gov.in/site/writereaddata/siteContent/ThreeNewMajorActs/20240628171056482 3BNS_IPC_Comparative.pdf.*

when automated scans result in the degradation of the service, or counterfeit credentials are used to simulate trust marks. The intermediary safe harbour under "Section 79" is the place where platforms are given support to run bug bounty programs which establish permitted techniques and a good faith safe harbour, provided there is a reporting channel and remediation cooperation; the exposure of corporate officers under "Section 85" serves as a motivation for documented approvals and oversight.[9]

### 5.5 Boundary Rules for Ethical Hacking

In India, the limit to ethical hacking can be legally defined by outlining five operational lines. First, the documented authorization by the system owner, connected to named assets, time boxes, and an explicit permission to test, is what neutralises the "Section 43" exposure and avoids "Sections 66/66C/66D" characterizations; vague or inferred consent is unsafe. Second, strict scope limitation and non exploitation ensure that discovered flaws are validated with least intrusive methods, thus avoiding a service disruption that could be interpreted as "mischief" under "Section 324 of the Bharatiya Nyaya Sanhita, 2023". Third, data minimisation and segregation reduce "DPDP Act" risk when test traffic or logs contain identifiers; deletion and retention clauses should be in line with the act's principles. Fourth, the responsible disclosure timelines should be in line with CERT In's six hour reporting culture for incidents and platform rule pathways under the Intermediary Rules, while at the same time respecting the "Section 69A" framework if content level blocking is involved. Fifth, safe harbour through published vulnerability disclosure or bug bounty policies gives predictability to researchers and platforms, thus linking coordinated disclosure channels to CERT In and making it clear that good faith testing within the policy will not cause legal action.[10]

## 6. CASE LAW ANALYSIS

The Indian judiciary has, in a very careful manner, managed to draw a line between, on the one hand, control of cybercrime and, on the other hand, the preservation of the space available for security research conducted in good faith. Such a boundary line can be best gleaned by scrutinizing those decisions in tandem with the "Section 69A of the Information

[9] *Will You Be Charged for Data Breach and Misuse: Section 72A of the IT Act, available at: https://www. apnilaw.com/legal-articles/acts/will-you-be-charged-for-data-breach-and-misuse-section-72a-of-the-it-act/ (last visited on October 3, 2025)*

[10] *Supra* note 6

Technology Act, 2000", the Blocking Rules, and the safe harbour architecture for intermediaries. The path in "*Shreya Singhal v. Union of India*[11], eliminated vague prohibitions of speech while still maintaining a structured takedown mechanism, which hence becomes the baseline against which later portal based powers are measured. Judgments on electronic evidence in "*Anvar P.V. v. P.K. Basheer*[12], and "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[13], require procedural rigor in authenticating logs and forensics, a matter that also supports ethical testers who do it methodically. In "*National Association of Software and Service Companies v. Ajay Sood*[14], the Delhi High Court's acknowledgment of phishing carved out civil boundaries around trickery in cyberspace, and the Supreme Court's interpretation of the IT Act as a special code in "*Sharat Babu Digumarti v. Govt. (NCT of Delhi)*[15], redefines the possibilities of charging while investigations are crossing over into general penal law. The stories of the Sahyog Portal in the recent orders of the Karnataka High Court and a 2025 Bengal conviction in a large "digital arrest" scam, occurring simultaneously, suggest together as one such judiciary that is not only ready to give a green signal to powerful responses against cyber harm but also to expect the due process and the discipline of evidence which, in turn, redefines the space where researcher disclosures and proof of concept sharing must lie.[16]

### 6.1 Speech, Takedown, and Due Process

"*Shreya Singhal vs. Union of India*, abolished "Section 66A of the Information Technology Act, 2000" and partially interpreted "Section 79" as non-binding, while confirming the "Section 69A" blocking system and its procedural safeguards. That configuration shifts the State's control over the Internet content into a more regulated and step by step process that requires explanation, documentation, and review. This model is significant for moral hacking when researchers disseminate the details of a breach, the demonstration code, or the compromise indicators that a platform or a law enforcement agency may consider as a source of harm. The legal way refers to depending on the Blocking Rules rather than random instructions, and it also defines the responsibility of the intermediaries in the coordination of

[11] *AIR 2015 SC 1523.*
[12] *(2014) 10 SCC 473.*
[13] *(2020) 7 SCC 1*
[14] *119 (2005) DLT 596.*
[15] *(2017) 2 SCC 18*
[16] *Shreya Singhal v. Union of India — Case Analysis, available at: https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/ (last visited on September 30, 2025)*

the disclosure. When disclosure becomes content restriction, the due process system from Shreya Singhal is still guiding a lawful reaction, and it provides a terminology for disputing excessive takedowns while co operating in risk reduction.[17]

### 6.2 Electronic Evidence Standards

"*Anvar P.V. v. P.K. Basheer*, and "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* combined raised the bar for the admission of electronic records, a standard that is reflected in the certificate and authenticity framework under the "Bharatiya Sakshya Adhiniyam, 2023". Their judgements mandate that a contemporaneous certificate for secondary electronic evidence be produced, which in reality implies that packet captures, log exports, screenshots, and disk images, which are being used to defend a good faith testing, must be created and preserved with a chain that is auditable for the detailed activities."[18]

### 6.3 Phishing and Tort Recognition

"*National Association of Software and Service Companies v. Ajay Sood*, recognized phishing as one of the violated civil rights, i.e., as passing off and deceit, and the court's rationale has a long lasting value in today's red teaming context. In case a tester fabricates identities and uses logos to trick credentials without having proper authorization, then the civil liability can be brought by this line of authority even if the criminal standards under "Sections 66C and 66D of the Information Technology Act" are not exceeded. The decision's focus on the use of deception for the extraction of the data makes it clear why social engineering performed by client approved must be guarded by explicit written consent, well defined scenarios, and destruction or hand back of the captured information.[19]

### 6.4 Recent Cybercrime Jurisprudence with Policy Signals

A 2025 Bengal conviction of a massive "digital arrest" fraud, nine life sentences being the most prominent, for an extortion through the simulated custodial threats, reflects the current stance of the judiciary against the use of technology for coercion, and indicates their readiness to consider cyber enabled fraud as aggravated economic harm. The case description

[17] *Supra note 16*
[18] *https://aphc.gov.in/docs/imp_judgements/Anvar PV case.pdf.*
[19] *Uncovering the Legal Consequences of Copycat Websites, available at: https://blackandwhite.legal/post/uncovering-the-legal-consequences-of-copycat-websites (last visited on October 1, 2025).*

illustrated the details of the cross state arrests, high value proceeds, and the method of intimidation using VoIP masking and screen shares, while the sentencing speech referred to such operations as the ones that destroy public order.[20]

## 7. CHALLENGES

Drawing on the same inquiry into lawful and ethical security research under India's cyber laws, the following friction points merit anticipation and disciplined mitigation.

- Ambiguous consent boundaries risk exposure under Section 43 of the IT Act. Obtain written authorization identifying systems, timelines, and permissible tools before initiating any probe.

- Overlap between IT Act offences and general penal provisions may cause duplicative charges. Cite Sharat Babu Digumarti to confine allegations to the IT Act when conduct squarely concerns digital access or transmission.

- Delayed breach reporting can breach Section 8 of the DPDP Act and CERT-In directives. Integrate six-hour notification triggers and automated alerts in incident-response playbooks.

- Unclear data-minimisation practice can create DPDP Act non-compliance. Use anonymised test data, limit captures to metadata, and define erasure rules in scope documents.

- Portal-based takedown orders may suppress coordinated disclosures. Preserve full communication logs and assert Shreya Singhal's due-process requirement when contesting informal removals.

- Weak evidentiary trails reduce protection for ethical testers. Generate hash-verified logs and BSA-compliant Section 63 certificates contemporaneously with each test.

- Third-party systems touched incidentally may trigger cross-jurisdictional claims. Insert indemnity and notification clauses covering external dependencies in every

[20] *In a First, 9 Sentenced to Life by Court in Bengal for 'Digital Arrest' Fraud, available at: https://timesofindia. indiatimes.com/india/in-a-first-9-sentenced-to-life-by-court-in-bengal-for-digital-arrest-fraud/articleshow/ 122773681.cms (last visited on October 2, 2025).*

authorization letter.

- Corporate officers may face vicarious liability under Section 85 IT Act. Document board-level approval for bounty or penetration programs and maintain oversight minutes.

- Misclassification of social-engineering exercises as deception can invite civil suits. Align scenarios with NASSCOM v. Ajay Sood by obtaining client-signed scripts and post-test destruction certificates.

- Absence of unified CVD guidance leaves disclosure timing uncertain. Adopt internal 90-day remediation clocks and mirror ISO 29147 to structure acknowledgments and Advisories.

## 8. CONCLUSION

This research illustrates that the design of the cybercrime framework in India is capable of including ethical hacking if authorization, proportionality, and documentation are the legal pivots on which the system operates. The study demonstrates, by reading the sections 43, 66, and 70B of the IT Act in conjunction with sections 4, 7, and 8 of the DPDP Act, and the BSA and BNSS as the evidentiary backbone, how to achieve the coexistence of deterrence and privacy. The responsible testing, when it is limited by consent, minimal data use, and prompt reporting, turns from a potential intrusion into a compliance support. The operational rendition of law from Puttaswamy's privacy reasoning to Shreya Singhal's due process rights gives the legal and moral grounds for a defensible distinction between investigation and taking advantage. There are, however, some methodological constraints: the absence of an empirical case base, enforcement data that is not evenly distributed, and the possibility that pending subordinate rules under the DPDP Act might affect the extent of generalisation of the doctrinal synthesis. Yet, this synthesis still serves to illuminate the permissible perimeter.

Ethical hacking is reimagined through the practical aspect of the framework as a form of governance that can be measured: compliance artefacts such as authorisation letters, CERT In timelines as metrics of responsiveness, and log integrity under the BSA as the proof of good faith. Subsequent policy may define success by the decrease of incident under reporting, shorter patch cycles, and documented collaboration between researchers and fiduciaries.

Finally, this article is holding the position of ethical hacking as an accountability tool which is not a criminal law loophole but rather one that fosters deterrence and at the same time complies with India's constitutional and privacy commitments.

## REFERENCES / BIBLIOGRAPHY


- Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy, *available at:* https://cyber.dhs.gov/assets/report/bod-20-01.pdf (last visited on October 3, 2025).

- CERT-In Directions on Cybersecurity: An Explainer, *available at:* https:// internetfreedom.in/cert-in-guidelines-on-cybersecurity-an-explainer/ (last visited on October 2, 2025).

- Extension of Timelines for Enforcement of Cyber Security Directions of 28 April 2022, *available at:* https://www.cert-in.org.in/PDF/CERT-In_directions_extension_MSMEs_and_validation_27.06.2022.pdf (last visited on October 1, 2025).

- https://aphc.gov.in/docs/imp_judgements/Anvar PV case.pdf.

- https://uppolice.gov.in/site/writereaddata/siteContent/Three New Major Acts/ 20240628171056482 3BNS_IPC_Comparative.pdf.

- In a First, 9 Sentenced to Life by Court in Bengal for 'Digital Arrest' Fraud, *available at:* https://timesofindia.indiatimes.com/india/in-a-first-9-sentenced-to-life-by-court-in- bengal-for-digital-arrest-fraud/articleshow/122773681.cms (last visited on October 2, 2025).

- Justice K. S. Puttaswamy (Retd.) v. Union of India, *available at:* https://cdnbbsr. s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/

- Section 43 of the Information Technology Act, *available at:* https://cis-india.org/ internet-governance/resources/section-43-it-act.txt (last visited on September 30, 2025).

- Sharat Babu Digumarti v. Government (NCT of Delhi) — Supreme Court of India Judgment, *available at* https://www.casemine.com/judgement/in/ 5854174353bee7171745b2c0 (last visited on September 30, 2025).