Hacker by Invitation: Is Bug Bounty Hunting Legal in India? A Doctrinal and Comparative Study

Adv. Prashant Mali
Cyber Law Consulting (Advocates & Attorneys)

Abstract—**Bug bounty hunting is legal in India when, and only to the extent that, the owner of the system has permitted it. That single word, permission, carries the entire weight of the answer. Section 43 of the Information Technology Act, 2000 penalises a list of acts done "without permission of the owner or any other person who is incharge" of a computer resource, and Section 66 criminalises the same acts when done "dishonestly or fraudulently". A published bounty programme supplies the permission; the hunter's good faith answers the mens rea. Step outside the published scope and both protections fall away together.**

This paper tests that proposition against every relevant Indian statute and rule: the IT Act and its subordinate legislation, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and its 2025 Rules, the Copyright Act, 1957, the Telecommunications Act, 2023, the Indian Contract Act, 1872, and the directions of CERT-In, NCIIPC and the sectoral regulators. It reads those provisions through Supreme Court and High Court decisions on access, authorisation, dishonest intent and the primacy of the special statute. It then sets India beside the United States, the United Kingdom, the European Union and its member states, Singapore, China and the two international cybercrime conventions.

The finding is a three-zone model. Research within the owner's published permission is lawful. Research that goes beyond that permission is a contravention as to the excess. Uninvited research, however well meant, is a contravention under Section 43 and sits one prosecutorial inference away from Section 66. India has no statutory safe harbour for good-faith security research, and the paper closes with a draft of one.

Index Terms—**bug bounty; coordinated vulnerability disclosure; ethical hacking; Section 43; Section 66; Information Technology Act, 2000; DPDP Act, 2023; safe harbour; unauthorised access; comparative cyber law.**

I. INTRODUCTION

Volenti non fit injuria. To one who consents, no wrong is done.

A bug bounty is the only arrangement in commerce where a company pays a stranger for doing what would otherwise get the stranger arrested. The same keystrokes that earn a cheque on Monday can earn a First Information Report on Tuesday. The code has not changed between the two days. Only the invitation has.

The locksmith is the familiar analogy, and it is a good one. A locksmith who opens your door at your request sends an invoice. A locksmith who opens it at midnight without being asked, and then leaves a polite note about your weak latch, has still broken in. His note may be accurate. His conscience may be clean. The law of trespass is interested in neither.

Plato put the moral version of the question in the Republic. The shepherd Gyges finds a ring that makes him invisible and promptly uses it to take a kingdom. Glaucon's challenge is whether anyone would stay honest with such a ring. The bug hunter is the rare person who finds the ring, tries it on, and walks it back to the owner. Economists have studied when and how such behaviour should be rewarded and disclosed (Kannan & Telang, 2005; Arora, Telang & Xu, 2008), and empirical work finds that open programmes keep surfacing bugs as new researchers join (Maillart et al., 2017). The law, however, does not ask whether the hunter was virtuous. It asks whether he was permitted.

India sharpens the question for two reasons. First, Indian researchers are among the most active contributors to global bounty platforms, so the exposure is real and daily. Second, the Information Technology Act, 2000 was drafted before the bounty model existed and says nothing about good-faith research.

1.1 Research questions

1. Does participation in a published bug bounty programme amount to a contravention under Section 43 or an offence under Section 66 of the IT Act?
2. Does good faith, without permission, protect an uninvited researcher under Indian law?
3. What is the legal character of the bounty promise, and when is it enforceable?
4. How do comparable jurisdictions protect security research, and what should India borrow?

1.2 Method and sources

The method is doctrinal and comparative. Statutes, rules, regulatory directions and reported judgments are cited as primary sources. Secondary literature is confined to peer-reviewed journals and proceedings indexed in Scopus and to scholarly books from established academic and legal publishers. Blogs, platform marketing and news reports are deliberately left out, however quotable. The exceptions are the case studies in Parts 7.4 and 7.6, where press reports and parliamentary replies are the available record of recent events and are cited as sources of fact, not of law. Part 7.5 draws on an anonymised opinion from the author's own practice.

"Section" is used throughout in the Indian style. References to the Indian Penal Code, 1860 are paired with the corresponding provision of the Bharatiya Nyaya Sanhita, 2023 (BNS), because the reported case law still speaks the older numbering.

II. ANATOMY OF A BUG BOUNTY

A bug bounty programme is a standing public offer: find a qualifying flaw in the listed systems, report it privately under the stated rules, and the organisation will pay. Everything legally interesting lies in the three qualifiers, namely listed systems, stated rules and will pay.

2.1 The actors and the documents

Three parties are usually involved. The organisation owns or controls the target. The hunter tests it. A platform often sits between them, hosting the programme, triaging reports and moving the money. The governing documents are the programme policy (scope, exclusions, rules of engagement, reward table, disclosure terms) and the platform's own terms of use. Empirical work shows how uneven these documents are. A study of programme rules on a leading platform found wide variation in how clearly scope, prohibited conduct and legal assurances were stated (Laszka et al., 2018). Later work on policy documents and programme operators reports the same unevenness (Walshe & Simpson, 2022, 2023), and hunters themselves report poor communication, disputes and unclear scope among their main grievances (Akgul et al., 2023). Elazari Bar On (2019) describes the result as private ordering: contract terms doing the work that statute has left undone.

2.2 Bounty, disclosure policy, and neither

A vulnerability disclosure policy (VDP) and a bug bounty programme are often confused. A VDP says "tell us and we will not sue". A bounty adds "and we will pay". Both grant permission. Only the second promises consideration. ISO/IEC 29147 and ISO/IEC 30111 standardise the disclosure and handling process but leave legal protection to local law.

The typology below is used for the rest of this paper.

Category	What the hunter has	Typical example	Core legal question
A. Invited, rewarded	Published scope and a promise to pay	A fintech's public programme on a bounty platform	Did the hunter stay within scope?
B. Invited, unrewarded	A VDP with a no-action assurance	A company's security.txt and disclosure page	Is the assurance binding without consideration?
C. Uninvited, good faith	Nothing but good intentions	A student finds an exposed database and emails the CEO	Does motive excuse lack of permission?
D. Uninvited, with a demand	A finding and a price	"Pay me or I publish"	Is this extortion?
E. State and critical systems	Sometimes a governmen	A flaw in a notified	Do Sections 66F and 70 apply?

Category	What the hunter has	Typical example	Core legal question
	t channel, never a bounty contract	protected system	

Categories A and B are the invited zones. Category C is where most Indian controversies arise. Category D is the so-called "beg bounty", which the security community dislikes almost as much as the police do. Category E is where the sentence, if things go wrong, is measured in decades.

2.3 What a "safe harbour" clause really is

In a bounty policy, "safe harbour" means a promise by the organisation that it will treat in-scope research as authorised and will not sue or complain. It is a contractual assurance by a private party. It is not an immunity granted by law. That distinction matters in India because Section 66 is a cognizable offence, and a private promise cannot bind the investigating agency. What the clause can do, and does do, is supply the permission on which Section 43 turns. Part 3 explains why that is usually enough.

III. THE INDIAN STATUTORY FRAMEWORK

No Indian statute mentions bug bounties, and none prohibits them. Legality therefore has to be assembled from provisions written for other purposes. The assembly starts with the IT Act and then moves outward.

3.1 Information Technology Act, 2000: the two hinges

Section 43 lists ten acts, clauses (a) to (j), that attract liability to pay compensation when done "without permission of the owner or any other person who is incharge" of the computer resource. They include accessing or securing access, downloading or copying data, introducing a contaminant, causing damage or disruption, denying access, and assisting another to gain access. Liability is civil and strict. No intent is required.

Section 66 converts any Section 43 act into an offence when it is done "dishonestly or fraudulently", with up to three years' imprisonment or a fine up to five lakh rupees, or both. The Explanation borrows the Penal Code meanings of both words, now found in BNS Section 2(7) and 2(9).

Four features of these two provisions decide most bounty questions.

1. "Access" is defined very widely. Section 2(1)(a) covers gaining entry into, instructing or communicating with the logical, arithmetical or memory functions of a computer resource. Sending a crafted request to a server is access.
2. Permission has no prescribed form. The Act does not require writing, a signature or a contract. A published programme policy is permission, given in advance, to anyone who acts within it.
3. Permission is divisible. Each clause of Section 43 is separately qualified by "without permission". Permission to access under clause (a) is not permission to download under clause (b) or to disrupt under clause (e). This is the statutory basis for treating scope as a legal boundary and not a courtesy.
4. "Damage" includes harmless change. Explanation (iv) to Section 43 defines damage to include adding or modifying data by any means. A test record inserted to prove an injection flaw is, in statutory terms, damage.

3.2 Other IT Act provisions a hunter can trip over

Provision	What it covers	Why it matters to bounty work
Section 65	Tampering with computer source documents	Altering or concealing source code during testing
Section 66B	Dishonestly receiving a stolen computer resource	Buying or accepting leaked data or credentials to "verify" a bug
Section 66C	Dishonest or fraudulent use of another's password or unique identifier	Account-takeover proofs using a real user's credentials
Section 66D	Cheating by personation using a computer resource	Social-engineering tests, usually out of scope
Section 66E	Capturing or transmitting private images	Proofs on camera or media endpoints

Provision	What it covers	Why it matters to bounty work
Section 66F	Cyber terrorism, up to life imprisonment	Clause (1)(B) reaches knowing unauthorised access to data restricted for State security, without any terror motive
Section 70	Unauthorised access to a notified protected system, up to ten years	Critical information infrastructure; no bounty policy by a vendor can waive it
Section 72A	Disclosure of personal information in breach of a lawful contract	Publishing findings in breach of programme confidentiality terms
Sections 84B and 84C	Abetment and attempt	A failed exploit can still be an attempt; see Part 3.9
Section 75	Extraterritorial reach where an Indian computer is involved	Foreign hunters testing Indian targets

Procedure softens the picture a little. Under Section 77B, offences punishable with three years are bailable, and the Supreme Court confirmed in Maharaj Saran v. State of Punjab, 2026 SCC OnLine SC 1378, that Section 66 is bailable on that basis. Section 77A allows compounding. Section 78 requires investigation by an officer not below the rank of Inspector. Section 81 gives the Act overriding effect, though Part 4 shows that this does not always keep the Penal Code out.

The Jan Vishwas (Amendment of Provisions) Act, 2023 formally omitted Section 66A and converted the punishments in Sections 72 and 72A into monetary penalties. It did not touch Sections 43 or 66, and it added no research exception.

3.3 Subordinate legislation and agency policy

- CERT-In Rules, 2013 and Directions of 28 April 2022. Service providers, intermediaries, data centres, bodies corporate and government organisations must report specified incidents to CERT-In within six hours of noticing them. Unauthorised access and data leaks are on the list. An uninvited researcher's email can therefore start a statutory clock for the recipient.
- CERT-In Responsible Vulnerability Disclosure and Coordination Policy (2021). CERT-In coordinates disclosure with vendors. Clause 7 of the policy states that reporting a vulnerability does not exempt the discloser from legal compliance and that the discloser remains responsible for the acts by which the flaw was found. The channel is a mailbox. It is not a shield.
- NCIIPC Rules, 2013, the Protected System Rules, 2018 and the NCIIPC disclosure programme. NCIIPC accepts reports on critical infrastructure from researchers and acknowledges contributors. It offers no immunity from Section 70 of the Information Technology Act.
- SPDI Rules, 2011 and Intermediary Rules, 2021. The first set the "reasonable security practices" standard under Section 43A, which the DPDP Act will replace. The second require intermediaries to report incidents to CERT-In.

3.4 Bharatiya Nyaya Sanhita, 2023

The BNS supplies the mental-element vocabulary and a set of offences that sit alongside the IT Act.

- Definitions. "Dishonestly" means intending wrongful gain or wrongful loss (Section 2(7)). "Fraudulently" means with intent to defraud (Section 2(9)). Nothing is done in "good faith" that is done without due care and attention (Section 2(11)).
- Extortion (Section 308, formerly IPC Section 383). A report coupled with a threat to publish unless paid falls here. This is the legal line between Category C and Category D.
- Cheating, breach of trust, mischief, criminal intimidation (Sections 318, 316, 324, 351). These are the provisions that are generally attracted in an FIR against an insider or a rogue tester.
- General exceptions. Section 19 (formerly IPC Section 81) excuses an act done without criminal intent and in good faith to prevent other harm. Section 33 (formerly IPC Section 95) excuses trivial harm. Both are arguable for a careful researcher. A constitutional court has tested neither on these facts.

- Concealment (Sections 238 and 239, formerly IPC Sections 201 and 202). These are aimed at the organisation, not the hunter. A "bounty" paid to bury a breach is the risk.

3.5 Digital Personal Data Protection Act, 2023 and the 2025 Rules

The DPDP Rules were notified on 13 November 2025. The security-safeguard and breach-intimation obligations in Rules 6 and 7 take effect on 13 May 2027. Three consequences follow for bounty programmes.

1. Incentive. Section 8(5) requires reasonable security safeguards, with a penalty of up to 250 crore rupees for failure. A well-run bounty programme is evidence of diligence, though the Act does not name it.
2. Is a hunter's access a "personal data breach"? Section 2(u) defines breach to include unauthorised processing that compromises confidentiality. In-scope access is authorised, so the better view is that it is not a breach. Out-of-scope or uninvited access to personal data is, and it triggers intimation to the Data Protection Board of India and to each affected Data Principal under Section 8(6) and Rule 7.
3. What is the hunter? A hunter who copies customer records to prove a flaw decides the purpose and means of that processing. Without a programme, that makes the hunter a Data Fiduciary with no lawful ground under Section 4. Within a programme, the hunter is better characterised as a Data Processor acting on the fiduciary's behalf, which Section 8(2) permits only "under a valid contract". The Bounty Programme terms should therefore be drafted to serve as that contract.

3.6 Copyright Act, 1957

Parliament has already recognised authorised security testing once. Section 65A, inserted in 2012, criminalises circumvention of technological protection measures but exempts, in sub-section (2), acts done for "testing the security of a computer system or a computer network with the authorisation of its owner". Section 52(1)(ac) protects observing, studying, or testing the functioning of a program to determine the underlying ideas/principles, provided the copy was lawfully obtained.

3.7 Telecommunications Act, 2023 and sector rules

Section 42 of the Telecommunications Act punishes unauthorised access to a telecommunication network or to the data of an authorised entity with up to three years' imprisonment, a fine up to two crore rupees, or both. The Telecom Cyber Security Rules, 2024 add a six-hour incident-reporting duty for telecom entities. A hunter testing a telecom operator faces this Act in addition to the IT Act.

The Aadhaar Act, 2016 (Section 38) criminalises unauthorised access to the Central Identities Data Repository. The Official Secrets Act, 1923 remains available where sovereign or protected government information is obtained.

3.8 Financial-sector regulators

RBI's cyber security framework for banks (2016) and its 2023 Master Direction on IT governance, SEBI's Cybersecurity and Cyber Resilience Framework (2024) and IRDAI's 2023 information security guidelines all mandate periodic vulnerability assessment and penetration testing, generally through qualified or CERT-In empanelled auditors. They neither prohibit voluntary public bug bounties nor shield uninvited external researchers from criminal liability under the IT Act or BNS.

3.9 Attempts: when a failed test is still an offence

Most security testing consists of attempts that fail, so the law of attempt matters more to a hunter than to almost any other accused. In most professions failing at the job is not a crime. In this one it can be, at half the sentence. Two general provisions govern it, and a third group of express clauses overrides both.

Provision	What it reaches	Punishment	Where it meets bounty work
IT Act, Section 84C	An attempt to commit any offence under the IT Act, where the Act makes no express provision	Up to half the longest term provided for the offence, or the fine, or both. For	A dishonest intrusion that fails

Provision	What it reaches	Punishment	Where it meets bounty work
	for that attempt	Section 66, up to eighteen months	
BNS, Section 62 (formerly IPC Section 511)	An attempt to commit an offence under the Sanhita punishable with imprisonment, where no express provision exists	Up to half the longest term provided for the offence, or the fine, or both	Attempted cheating or theft charged alongside the IT Act
Express attempt clauses: IT Act, Sections 66F and 70(3); BNS, Section 308(3)	Attempting to penetrate with the cyber-terrorism intent; attempting to secure access to a protected system; putting a person in fear in order to extort	The full punishment for the offence, with no halving	Critical infrastructure; the demand that goes unpaid

The two general provisions do not overlap. Section 84C applies only to offences "punishable by this Act", and Section 62 only to offences punishable by the Sanhita. A failed intrusion is charged under the first. A failed attempt to cheat by means of that intrusion is charged under the second.

Five consequences follow for the analysis in this paper.

1. Neither provision reaches Section 43. Section 43 creates civil liability and not an offence, so there is no such thing as an attempted contravention. The comfort is thinner than it looks. Because "access" includes merely communicating with a computer resource, a request that the server receives and answers may already be completed access. The space for a pure attempt at access is small.
2. Intention is an essential ingredient. In Abhayanand Mishra v. State of Bihar, AIR 1961 SC 1698, the Supreme Court held that an attempt needs an intention to commit the offence and an act done towards it, which need not be the last act before completion. Since Section 66 requires dishonest or fraudulent intent, an attempt at Section 66 requires the same. A good-faith hunter whose exploit fails has not attempted the offence, for the same reason that one whose exploit succeeds has not committed it. Section 84C removes the need for success. It does not remove the need for a guilty mind.
3. Preparation is not attempted. Malkiat Singh v. State of Punjab, (1969) 1 SCC 157, asks whether the acts already done would be harmless if the accused changed his mind. State of Maharashtra v. Mohd. Yakub, (1980) 3 SCC 57, looks to how close the acts came to completion. Preparation constitutes reading documentation, studying client-side code and building tools. Attempt connotes ending the crafted payload at the target, provided the intent is present. Reconnaissance scanning occupies a legal gray area; under a broad interpretation of "access", probing a system may cross the threshold from mere attempt to a completed unauthorized entry.
4. Impossibility is no defence. The illustrations to Section 62, carried over from the old Code, include the pickpocket who finds the pocket empty and is guilty all the same. A hacker with malafide intentions who gets blocked by a firewall is still guilty of an attempt. For ethical security researchers, though, the logic flips. "Nothing broke" does not remain a valid defense. Instead, the defense must hinge entirely on establishing that there was authorisation to test the system and lacked any dishonest intent.
5. For protected systems, the attempt is the offence. Section 70(3) punishes securing access and attempting to secure access in the same breath, with up to ten years for either. Section 84C and its halving do not apply. This is why the Meera example in Part 7.3 ends with advice to test nothing further.

The practical effect varies by zone. In the Green zone there is nothing to attempt, because the completed act would be lawful. In the Amber and Red zones Section 84C means the police need not show a successful entry. To register a case, logs of blocked requests suffice, and intent is argued afterwards. After Awadhesh Kumar Parasnath Pathak, an attempt to cheat under Section 318 read with Section 62 of the BNS can be added to the same FIR.

One example fixes the point. A hunter enrolled in a programme for one host fires injection payloads at a second, out-of-scope host, and a firewall blocks every request. If he was honestly testing, there is no attempt at Section 66 and, at most, an arguable civil contravention for the requests that reached the server. If the intention was to take data and sell it, the offence of attempt is complete although despite no tangible gain.

3.10 What the statute book adds up to

Read together, these provisions give a consistent answer. Authorisation by the owner is the dividing line in the IT Act, the Copyright Act, the Telecommunications Act and the Aadhaar Act alike. Indian law has no concept of "authorised by good intentions".

IV. JUDICIAL INTERPRETATION

The Supreme Court of India or any High Court has not ruled on a bug bounty dispute to date. Key judicial precednts however, already establish the essential legal framework. Nuances such as the intent required under section 66, the scope of unauthorised access, the role of motive, and the permissibility of layering criminal code charges alongside IT Act offenses have been deliberated upon by courts. This section synthesizes those foundational principles.

4.1 Mens rea is an ingredient of Section 66

In Shreya Singhal v. Union of India, (2015) 5 SCC 1, the Supreme Court struck down Section 66A for vagueness and, in doing so, contrasted it with Section 66. The Court noted that mens rea is an essential element of every computer-related offense under section 66, emphasizing that terms like 'dishonestly' and 'fraudulently' have well-established legal definitions.

Ramesh Rajagopal v. Devi Polymers Pvt. Ltd., (2016) 6 SCC 310, applied the principle. A director was prosecuted under Sections 65 and 66 for creating a website said to misrepresent the company. The Supreme Court quashed the proceedings on two key determinations: there was no proof of unauthorised access to the coporate systems, and no dishonest intent was established. Taken together, valid authorization and an honest purpose were sufficient to invalidate the prosecution precisely the dual protections provided by a bug bounty program and an ethical researcher.

Regarding the historical standards under the Indian Penal Code, Dr. Vimla v. Delhi Administration, AIR 1963 SC 1572, remains the leading precedent. "Defraud" requires deceit together with injury to the person deceived or an unlawful advantage to the deceiver. A hunter who discloses vulnerabilities transparently and abides by the program's reward structure commits no deception and receives no unlawful benefit.

4.2 Good-faith testing: the Himachal e-pass case

The closest Indian deliberation on uninvited security research is Aman Kumar Bhardwaj v. State of Himachal Pradesh, 2022 LiveLaw (HP) 16. During the second Covid wave a television journalist doubted the State's claim that inter-State e-passes were issued only after verification. He applied for two passes, one in the name of Amitabh Bachchan and one in the name of Donald Trump, using his own Aadhaar number and phone. Both were issued. He broadcast the result and was booked for personation and forgery under the Penal Code and under Section 66D of the IT Act.

The High Court quashed the FIR. It found that he had acted to verify how the system worked, had never used or intended to use the passes, had brought the flaw to the authorities' notice, and was therefore "neither dishonest nor fraudulent". Consequently, a government database briefly reflected a valid entry pass to Shimla issued to Donald Trump, giving Indian jurisprudence its initial precedent on good faith-security testing.

While useful, the limitations of this single-judge ruling must be acknowledged: it addressed only fraud-based offenses and ignored section 43 of the IT Act, where intent is legally irrelevant. Further, because the tester merely submitted a public web form without accessing third-party records, the ruling offers weak protection for researchers who bypass authentication or extract sensitive data.

4.3 Motive mitigates; it does not authorise

At the civil level the position is stricter. In Vinod Kaushik v. Madhvika Joshi, the Adjudicating Officer for Maharashtra dealt with a spouse who had accessed email accounts to gather evidence for a matrimonial prosecution. After a remand by the Cyber Appellate Tribunal in 2011, the access was held to be without permission under Section 43. The intruder's intent was treated strictly as a mitigating factor to lower damages, resulting in only a nominal fine. Although this quasi-judicial ruling lacks the binding weight of a High Court precedent, its rationale aligns squarely with the statutory text: a noble motive may reduce financial liability, but it never supplies missing authorization.

4.4 Permission is bounded by purpose

The insider cases show that Indian courts already treat authorised access as limited by what it was given for.

- Abhinav Gupta v. State of Haryana, 2008 Cri LJ 4536 (P&H): An engineer holding valid system access emailed confidential design data to his personal account before moving to a rival firm. The court denied anticipatory bail, holding that general access privileges do not cover unauthorized data transfers.
- A. Shankar v. State (Madras High Court, 2010): The High Court refused to quash an IT Act prosecution against an employee accused of accessing a colleague's workstation without permission.
- Syed Asifuddin v. State of Andhra Pradesh, 2005 Cri LJ 4314 (AP): Reprogramming network-locked mobile devices was ruled to potentially constitute source code tampering under Section 65, reflecting a broad judicial interpretation to safeguard owner interests.

For a hunter, the lesson transfers directly. Scope is the bounty equivalent of an employee's job description. Access granted for testing app.example.in is not access to payroll.example.in.

4.5 The Penal Code can still be added

It was once thought that an IT Act charge displaced the Penal Code entirely. Sharat Babu Digumarti v. Government (NCT of Delhi), (2017) 2 SCC 18, held that where the IT Act specifically covers an electronic offence, the general law gives way. A Division Bench of the Bombay High Court extended this in Gagan Harsh Sharma v. State of Maharashtra, 2018 SCC OnLine Bom 17705, quashing cheating and breach-of-trust charges where Sections 43 and 66 covered the data theft alleged.

A Full Bench of the same Court has since narrowed that view. In Awadhesh Kumar Parasnath Pathak v. State of Maharashtra, 2024 SCC OnLine Bom 1074, it held that Sections 43 and 66 do not define the same offences as cheating and criminal breach of trust, because the Penal Code offences have additional ingredients such as deception and entrustment. An accused can be tried under both.

The practical consequence is serious. Section 66 is bailable and compoundable. Cheating with delivery of property under BNS Section 318(4), formerly IPC Section 420, is non-bailable and can be compounded only with the court's leave. A hunter who strays outside scope cannot assume that the gentler statute is the ceiling.

4.6 Technology-sensitive interpretation

In State of Punjab v. Amritsar Beverages Ltd., (2006) 7 SCC 607, the Supreme Court accepted that statutes must be read in a manner that keeps pace with technological change. That approach supports reading "permission" to include a standing public authorisation such as a programme policy. Requiring written consent for each individual researcher would impose a formal restriction on Section 43 that Parliament never intended to include.

4.7 The constitutional overlay

Three key precedents anchor any constitutional case for security researchers:

- Shreya Singhal establishes that vague criminal provisions causing a chilling effect on constitutionally protected activities are subject to legal challenge.
- K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 recognizes informational privacy as a fundamental right and obligates the State to safeguard it, an objective directly advanced by vulnerability research.
- Anuradha Bhasin v. Union of India (2020) 3 SCC 637 affirms that practicing a trade or profession over the internet is protected under Article 19(1)(g), subject only to proportionate restrictions.

While these rulings offer a compelling policy narrative, they form a weak strategy in courtroom

litigation. The phrase "without permission" is not legally vague, and requiring third parties to secure authorization before probing a system easily satisfies the test of proportionality. Consequently, the true solution to a researcher's legal exposure rests with legislative reform rather than judicial interpretation, prompting the statutory text proposed in Part 8.

4.8 Proof

A hunter's defence will rest on logs, timestamps, request captures and the programme policy as it stood at the time. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, require electronic records to be accompanied by the statutory certificate, now under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. A hunter who keeps clean records and an archived copy of the policy is preserving evidence of permission.

4.9 What the cases establish

1. Section 66 cannot be made out without dishonest or fraudulent intent (Shreya Singhal; Ramesh Rajagopal).
2. Authority to access plus honest purpose is a complete answer to Section 66 (Ramesh Rajagopal).
3. Testing a system in good faith to expose a flaw, without using the result, is not fraud (Aman Kumar Bhardwaj).
4. Good motive does not supply permission under Section 43 (Vinod Kaushik).
5. Permission is limited by its purpose (Abhinav Gupta).
6. Penal Code offences may be charged alongside the IT Act (Awadhesh Kumar Parasnath Pathak).

The open question, on which there is no reported authority, is whether exceeding the scope of a published programme makes the whole exercise "without permission" or only the excess. The divisibility of Section 43, discussed in Part 3.1, points to the second answer.

V. THE BOUNTY AS A CONTRACT

A unilateral contract such as a bounty programme is offered to the world and accepted by the performance of the conditions of the offer. Reward cases, decided by the Indian courts over the last hundred years or so, are surprisingly similar to bounty disputes.

5.1 Offer to the world, acceptance by performance

Section 8 of the Indian Contract Act, 1872 treats performance of the conditions of a proposal as acceptance. Carlill v. Carbolic Smoke Ball Co. [1893] 1 QB 256 is the English root. The company promised one hundred pounds to anyone who used its smoke ball and still caught influenza, and was held to its word. A bounty policy makes the same kind of promise in reverse: money to anyone who catches the company's illness before it spreads.

Indian courts adopted the principle in Har Bhajan Lal v. Har Charan Lal, AIR 1925 All 539, where a reward offered by handbill for tracing a missing boy was held enforceable by the person who found him. No prior communication of acceptance was needed. A hunter who submits a qualifying in-scope report has accepted the offer by doing what it asked.

5.2 The hunter must know of the offer

Lalman Shukla v. Gauri Dutt, (1913) 11 All LJ 489, supplies the limit. A servant sent to look for his master's nephew found the boy, learned afterwards that a reward had been announced, and sued for it. He failed. One cannot accept an offer one does not know about.

The bounty version arises regularly. A researcher finds a flaw in January and reports it. The company launches a programme in March and the researcher asks for a reward. On Lalman Shukla, there is no contract. The same result follows where the company has no programme at all. Whatever is paid in those cases is a gift.

5.3 Formation online

Section 10A of the IT Act confirms that contracts formed through electronic records are not unenforceable for that reason alone. Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1, accepted that a concluded contract can arise from an exchange of emails without a signed document. Programme terms accepted by a click or by submission are binding on ordinary principles.

5.4 "At our sole discretion"

Most policies reserve to the organisation the final say on validity, severity, duplicates and amount. Two doctrines limit how far that can go.

First, Section 29 voids agreements whose meaning is uncertain. A promise to pay "whatever we think fit, if anything" comes close to no promise at all. A published reward table with ranges by severity is certain enough.

Second, Central Inland Water Transport Corp. v. Brojo Nath Ganguly, (1986) 3 SCC 156, allows courts to refuse enforcement of unconscionable terms in standard-form contracts between parties of unequal bargaining power. A solo hunter facing a large company's take-it-or-leave-it terms fits the description. The doctrine has mostly been applied in employment and consumer settings, so its use here would be an extension, but a clause allowing a company to use a report and pay nothing would be a fair candidate.

5.5 Lawful object: when a "bounty" is hush money

Section 23 of the Contract Act voids any agreement that breaks or bypasses the law. A legitimate bug bounty serves a lawful purpose, but dressing up a hush-money payment as a "bounty" to hide a real data breach does not. Covering up a breach defeats mandatory incident-reporting duties—including the 6-hour CERT-In reporting mandate and the breach notification requirements under the DPDP Act taking full effect in May 2027.

A stark warning comes from the US case United States v. Sullivan. In 2022, Uber's former Chief Information Security Officer was convicted of obstruction and misprision of felony for routing a payment to hackers through the company's bug bounty program to buy their silence—a conviction the Ninth Circuit affirmed in 2025. In India, an executive attempting a similar cover-up would face criminal charges under BNS Sections 238 and 239 alongside severe regulatory fines.

This principle also applies to gag clauses. Contract terms that permanently ban a security researcher from reporting a vulnerability to regulatory authorities or CERT-In are legally void as against public policy. However, requiring reasonable confidentiality while a patch is being deployed is standard, lawful, and fully enforceable.

5.6 No programme, no claim in restitution

Can an uninvited researcher claim reasonable payment for a benefit conferred? Section 70 of the Contract Act allows recovery where a person "lawfully does anything for another person" without intending it as a gift, and the other enjoys the benefit. State of West Bengal v. B.K. Mondal & Sons, AIR 1962 SC 779, treats lawfulness of the act as a condition of the claim and stresses that the recipient must have had the choice to refuse the benefit.

The uninvited researcher fails on both. Access without permission is not lawful, and a company that never asked to be tested had no opportunity to decline. The moral claim may be strong. The legal claim does not exist.

5.7 The seventeen-year-old hunter

A noticeable share of talented hunters are minors, which raises a point of capacity. Mohori Bibee v. Dharmodas Ghose, (1903) ILR 30 Cal 539 (PC), holds a minor's agreement void. That protects the minor from obligations. It does not prevent the minor from taking a benefit. In Raghava Chariar v. Srinivasa Raghava Chariar, (1916) ILR 40 Mad 308 (FB), a minor who had fully performed was allowed to enforce the promise made to him.

A minor who submits a valid report has performed fully, so the reward promise should be enforceable on the minor's behalf. The confidentiality and indemnity terms, however, cannot be enforced against the minor. Organisations that want those terms to bind should contract through a guardian. Criminal liability is governed separately by the Juvenile Justice (Care and Protection of Children) Act, 2015.

5.8 The platform's terms

Where a foreign platform hosts the programme, its terms usually choose foreign law and arbitration. That governs the payment dispute. It does not govern Section 43, which asks a factual question: did the owner permit this act? Permission given through a foreign platform by the Indian owner is permission. Permission given by the platform for a target the listing organisation does not own is not, and hunters should check that the party listing an asset is the party entitled to authorise testing of it.

5.9 Tax and foreign exchange, briefly

Bug bounty earnings are subject to tax under the Income-tax Act, 2025. They are classified as professional income for full-time researchers or as "income from other sources" for occasional bug hunters. Payouts from overseas companies are treated

as cross-border service exports under GST law, meaning researchers must comply with the Foreign Exchange Management Act (FEMA), 1999 by receiving funds through authorized banking channels. While failing to report bounty income creates serious tax liabilities, it affects tax compliance—it does not retroactively turn a legally authorized test into a criminal hack.

VI. COMPARATIVE AND INTERNATIONAL LAW

Every major jurisdiction criminalises access "without authorisation" or "without right", and every one of them has had to decide what to do about the well-meaning intruder. The answers fall into four models: prosecutorial restraint, statutory safe harbour, coordinated disclosure through a State body, and no protection at all. India currently sits in the fourth.

Jurisdiction	Core offence	Protection for good-faith research	Legal form
United States	Computer Fraud and Abuse Act, 18 U.S.C. Section 1030	Yes, for federal criminal charges	Prosecutorial policy (2022) and a copyright exemption
United Kingdom	Computer Misuse Act 1990, Sections 1 to 3A	None yet; statutory defence under consideration	None
Belgium	Criminal Code computer offences	Yes, including uninvited research, on strict conditions	Statute (2023; tightened 2024)
Netherlands	Criminal Code, computer trespass	Yes, case by case	Prosecutorial guideline
France	Criminal Code, fraudulent access	Limited: for good-faith reports to the national agency	Statute (Defence Code)
European Union	Directive 2013/40/EU	Encouraged, not required	NIS2 Directive, Article 12 and Recital 60
Singapore	Computer Misuse Act 1993, Section 3	Only within government programmes	Programme terms
China	Cybersecurity Law and 2021 vulnerability regulations	State-directed disclosure	Administrative regulation
India	IT Act, Sections 43 and 66	Only where the owner permits	Private contract

6.1 United States

The Computer Fraud and Abuse Act punishes access "without authorization" or in excess of it. For three decades the scope of those words was the central question of American computer crime law (Kerr, 2003; Kerr, 2016; Bellia, 2016).

Van Buren v. United States, 593 U.S. 374 (2021), gave a narrow answer. A police officer who ran a licence-plate search for a bribe had used access he was entitled to, for a bad purpose. The Supreme Court held that this did not exceed authorised access. The test is whether the gate is up or down for that part of the system, not why the person walked through it. Lower courts have reasoned similarly for breaches of website terms

(Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C. 2020)) and for public data (hiQ Labs v. LinkedIn, 31 F.4th 1180 (9th Cir. 2022)).

In May 2022 the Department of Justice revised its charging policy to direct that good-faith security research should not be prosecuted under the Act. The definition of good faith was borrowed from the security-research exemption to Section 1201 of the Digital Millennium Copyright Act, first granted in the 2015 rulemaking. Both protections are real, and both are limited. The policy binds federal prosecutors only. It does not stop a civil suit or a State prosecution, which is why Bambauer and Day (2011) argued for statutory immunity.

The comparison with India is instructive. Van Buren reads authorisation narrowly in favour of the accused. Indian insider cases such as Abhinav Gupta read it by purpose. An Indian court considering a hunter who had valid credentials but tested beyond scope would not be bound to follow the American gate.

6.2 United Kingdom

The Computer Misuse Act 1990 was enacted after R v. Gold and Schifreen [1988] AC 1063, where the House of Lords found that the Forgery Act did not fit two journalists who had got into a Prestel mailbox, the Duke of Edinburgh's among them. Section 1 makes unauthorised access an offence. Section 17(5) defines access as unauthorised where the person is not entitled to control access and lacks consent from someone who is. There is no public-interest or research defence.

The case law is unsympathetic. In R v. Bow Street Metropolitan Stipendiary Magistrate, ex parte Government of the United States (Allison) [2000] 2 AC 216, the House of Lords held that an employee authorised to view some accounts was not authorised to view others. In R v. Cuthbert (2005, unreported), a security consultant who had donated to a tsunami appeal site and then probed it, fearing it was fake, was convicted under Section 1. The court accepted his motive and convicted him anyway.

Reform has been promised for years. A Home Office review ran from 2021 to 2023. In December 2025 the security minister announced that the Government was looking at a statutory defence for researchers. Amendments to that effect were tabled to the Cyber Security and Resilience Bill and withdrawn in committee in February 2026 on ministerial assurances. India's provisions share the structure of this Act, and they share its gap.

6.3 European Union and its member states

Directive 2013/40/EU requires member states to criminalise access "without right". The NIS2 Directive (EU) 2022/2555 adds the constructive half. Article 12 requires each member state to designate a CSIRT as coordinator for vulnerability disclosure, and Recital 60 encourages guidelines on non-prosecution of researchers. The Cyber Resilience Act, Regulation (EU) 2024/2847, obliges manufacturers of products with digital elements to operate a disclosure policy and to report actively exploited vulnerabilities.

EU law therefore mandates the channel and leaves the immunity to national choice. The national choices differ sharply (Vostoupal et al., 2024; Rampášek et al., 2026).

- Belgium went furthest. Since February 2023 a person who investigates a Belgian system without prior consent commits no offence if four conditions are met: no fraudulent intent or intent to harm, prompt notification to the national cybersecurity centre and the organisation, conduct limited to what is necessary and proportionate, and no public disclosure without the centre's agreement. The 2024 law transposing NIS2 tightened the timing, with a simplified notice required within 24 hours.
- The Netherlands relies on a public prosecutor's guideline that asks three questions: was the motive a public interest, was the conduct proportionate, and was there a less intrusive way.
- France protects the good-faith reporter who informs the national agency, which may keep the reporter's identity confidential and is relieved of its usual duty to refer offences to the prosecutor.
- Germany published a draft in 2024 to exempt good-faith research from its data-espionage offences.
- Malta shows the cost of doing nothing. Students who reported a flaw in a popular student app in 2022 were arrested and charged, and were pardoned only in 2025 after sustained public criticism.

A criminological study written from the Dutch experience argues that clear disclosure channels and credible assurances steer finders toward reporting and

away from misuse (Weulen Kranenbarg, Holt & van der Ham, 2018).

6.4 Singapore, Australia and China

Singapore's Computer Misuse Act 1993 mirrors the British model. In Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin [1999] 3 SLR(R) 653, a teenager who had broken into servers and claimed he was exploring their security had his probation order replaced with imprisonment on appeal; the High Court prioritised deterrence. Singapore has since built government bounty and disclosure programmes, and protection exists only inside them.

Australia's Criminal Code Act 1995 (Cth), Part 10.7, does not prescribe a research defence.

China takes a State-centric path. Regulations in force since 1 September 2021 require vendors to report vulnerabilities in their products to the industry ministry within two days and restrict researchers from publishing details before a patch or passing them to overseas parties other than the vendor. The model secures the State's knowledge of vulnerabilities. It does little for researcher autonomy.

6.5 The two conventions

The Council of Europe's Budapest Convention on Cybercrime (2001) requires criminalisation of access "without right" in Article 2 and, in Article 6(2), excludes authorised testing from the offence of misusing devices. India is not a party.

The United Nations Convention against Cybercrime was adopted by the General Assembly on 24 December 2024 and opened for signature at Hanoi on 25 October 2025. India signed it in New York on 25 September 2026. It is not yet in force and India has not ratified it. Article 7 requires criminalisation of illegal access and lets parties confine the offence to cases involving breach of security measures or dishonest intent. Article 11 carries forward the authorised-testing carve-out for devices. The Convention contains no general protection for good-faith research, a gap that was criticised during negotiation.

For India this is an opening. Ratification will require a review of domestic cybercrime law. The Convention's own optional qualifier, dishonest intent, is the element Section 66 already uses. A research safe harbour can be added at the same time without departing from the treaty.

6.6 Lessons for India

1. A channel without immunity is not enough. CERT-In's reporting framework provides a channel for researchers, much like Article 12 of the EU's NIS2 Directive, but it lacks statutory safe-harbor backing like Belgium's legislation.
2. Prosecutorial guidelines work where prosecution is centralised. In India, where any police station may register an FIR, a guideline would need to bind State police forces, which points toward statute.
3. The conditions used abroad are convergent: good faith, proportionality, prompt confidential reporting, no data retention, no demand. They can be legislated in a paragraph.
4. Judicial approaches like the US Supreme Court's Van Buren decision protect credentialed insiders who misuse access, but do little for independent, uninvited security researchers. Outside researchers require an explicit statutory safe harbor.

VII. THE ANSWER: A THREE-ZONE TEST

Bug bounty hunting in India is legal inside the owner's permission, a civil wrong outside it, and a crime when dishonest intent is added. The three zones below turn that sentence into a working test.

Zone	Facts	Section 43	Section 66	Other exposure	Position
Green	Published programme or VDP; hunter stays within scope and rules	Not applicable: permission exists	Not applicable: no contravention, no dishonesty	None, if personal data is not retained	Lawful
Amber	Active policy exists, but testing exceeds defined boundaries.	Applicable to the unauthorised access.	Depends on intent; hard to prove against a prompt, candid reporter	DPDP breach intimation by the company; loss of reward; possible BNS add-ons	Unlawful as to the excess
Red	Uninvited testing without consent, financial extortion/demands, or	Attracted	Attracted where dishonesty is	BNS Section 308 (extortion); IT Act Sections 66F and 70;	Unlawful; may be criminal

Zone	Facts	Section 43	Section 66	Other exposure	Position
	probing critical national infrastructure.		shown; a demand supplies it	Telecommunications Act Section 42	

7.1 Why the Green zone is lawful

Three propositions, each already established, combine to produce the result.

1. Section 43 applies only to acts done without the owner's permission (Part 3.1).
2. A published policy constitutes advance permission to anyone operating strictly within its terms. (Part 4.6).
3. Section 66 additionally requires dishonesty or fraudulent intent (mens rea). A researcher acting transparently under a published policy lacks this criminal mental element. (Ramesh Rajagopal).

A private "safe harbour" clause cannot bind the police. It does not need to. With permission in place, there is no contravention for the police to investigate.

7.2 Why good faith alone is not enough

In the Red Zone, an uninvited researcher has one defense but lacks another. Good faith defeats criminal prosecution under Section 66 (Aman Kumar Bhardwaj), but it provides no protection against Section 43 civil liability, which imposes strict liability without regard to state of mind.

That is an uncomfortable place to stand. Holmes advised that to know the law one should look at it as a bad man would, caring only for consequences (Holmes, 1897). The honest researcher is in the odd position of needing the bad man's caution. Fuller's requirement that law be capable of guiding conduct in advance is not met by a rule whose application depends on an after-the-fact reading of motive (Fuller, 1969).

7.3 Six worked examples

Ananya and the in-scope flaw. A payments company lists api.example.in on a bounty platform. Ananya creates two test accounts and shows that one can read the other's transaction list. She reports within the hour. Green. She had permission, touched only her own test data and reported as required. The reward is contractually due (Har Bhajan Lal).

Rohan and the fifty thousand records. Under the same program, Rohan discovers the same vulnerability. To "prove impact," he writes an automated script and extracts 50,000 customer KYC records. Amber, shading to Red. The policy authorised testing, not bulk extraction. Section 43(b) is attracted for the download. The company now has a personal data breach to intimate. A proof of concept needs two records, not the table.

Kabir and the open hospital database. Kabir, a student, stumbles upon an exposed, unauthenticated patient database belonging to a hospital with no disclosure policy. He views a few rows to confirm accessibility, immediately emails the hospital and CERT-In, and asks for no compensation. Red at the civil level; unlikely to be criminal. Access was without permission. Dishonest intent is absent on the reasoning in Aman Kumar Bhardwaj. The hospital must report to CERT-In within six hours. Kabir's safest course was to stop at the directory listing and report without opening records.

Kabir adds a deadline. Suppose his email had ended: "Pay five lakh rupees in 48 hours or I post this publicly." Red, and criminal. The demand introduces extortion under BNS Section 308 and supplies the explicit intent to cause wrongful gain required by Section 66. One sentence converts a civil trespass into two criminal offenses.

Meera and the power utility. Meera notices a login bypass on a State electricity distribution portal that has been notified as a protected system. Red, at its most serious. Section 70 punishes even an attempt to access with up to ten years. No vendor policy can authorise it. The only prudent step is to report what was observed to NCIIPC and test nothing further.

Dev, aged sixteen. Dev finds a valid in-scope flaw in an Indian retailer's app listed on a foreign platform. Green. Permission came from the owner, and his age does not affect that. The reward is enforceable for his benefit (Raghava Chariar). The confidentiality terms are not enforceable against him unless a guardian has agreed to them.

7.4 The test applied: the CBSE On-Screen Marking disclosures, 2026

The 2026 CBSE episode illustrates the Red Zone at its most sympathetic: uninvited research, reported same-day without financial demands, yet lacking formal statutory safe harbor protections. It involved two

individuals whose legal standing differs fundamentally under Indian law. Nisarga Adhikary tested an active system; Sarthak Sidhant analyzed public documents. Only the former engages the IT Act.

The account below rests on press reports and on the researcher's own published statements. CBSE disputes part of it, and no court has made findings on these facts.

Date	Event	Source
7 September 2026	Delhi High Court declines a public interest petition on the On-Screen Marking (OSM) system, noting that the Supreme Court had already refused similar relief	Bar and Bench
July 2026	Supreme Court, hearing a student's petition, is told that a one-member commission is reviewing the OSM system, and calls for a status report	Ommcom News
June 2026	Adhikary is hired by the cybersecurity hub at IIT Kanpur	The Week
6 June 2026	In an agency interview Adhikary says he was able to open evaluator scripts and generate grades, and that after publication he found a cloud store exposing a very large number of scanned answer sheets. He says the FIR lodged by CBSE concerns a separate denial-of-service attack	IANS via Siasat
30 May 2026	Sidhant, a Class 12 student, publishes a comparison of successive tender documents and alleges that eligibility terms were changed to the vendor's benefit	The Quint
27 May 2026	CBSE states that the portal named was an internal testing site holding sample data and not the live evaluation system	Telangana Today
26 May 2026	The Internet Freedom Foundation writes to the Ministry of Education and CERT-In seeking an investigation	IFF
22 May 2026	Adhikary publishes a technical write-up, 86 days after his report	IFF
25 February 2026	Adhikary, aged 19, reads the JavaScript served by the public OSM portal, finds five flaws including a master password in plain text, and reports to CERT-In the same day. CERT-In acknowledges	IFF

Date	Event	Source
	and, on his account, takes no visible action	

Adhikary: four acts, four answers. His conduct has to be taken in stages, because the law treats each stage differently.

1. Reading the code. The server delivered JavaScript to the client browser. Inspecting code intentionally made public does not constitute unauthorized access under Section 43.
2. Using the credentials. Submitting that password or altering session state to reach internal evaluator screens constituted a distinct, unauthorized act under Section 43(a). Explanation (iv) treats altering test data as statutory damage; CBSE's "testing site" defense goes to quantum of harm rather than authorization.
3. Criminal liability. Section 66 requires dishonest or fraudulent intent. A same-day report to the national agency, a video walkthrough supplied on request, no demand and an 86-day wait all point the other way. On the reasoning in Aman Kumar Bhardwaj, a prosecution should fail. Section 70 would matter only if the portal were a notified protected system, and nothing public suggests it was.
4. Publishing, and going further. No Indian statute explicitly prohibits disclosing a security flaw. However, publishing working exploit details of an unpatched system risks exposure under Sections 43(g) and 84B. Accessing stored student answer sheets presents the greatest legal risk under data minimisation and proportionality principles, as student scripts contain sensitive personal data.

The same facts produce different results under different regimes.

Regime	Result on the reported facts
India today	Civil contravention under Section 43(a) from the moment internal screens were accessed. Criminal prosecution under Section 66 unlikely to succeed but procedurally possible.
Draft Section 43B (Part 8)	Conditions on intent, prompt reporting and no demand are met. Publication at 86 days is protected only if the prescribed period is shorter than that. The later exploration is doubtful on necessity
Belgium	Testing and prompt report protected; publication without the national centre's agreement forfeits protection
United States	Falls within the DOJ's 2022 CFAA Charging Policy for good-faith research; federal prosecution highly unlikely.
United Kingdom	Section 1 offense under the Computer Misuse Act 1990 completed upon unauthorized entry (R v Cuthbert).

Sidhant: a speech case. He tested nothing. He compared published versions of a public tender and drew conclusions. The IT Act is not engaged, and calling him a hacker misdescribes what he did. His position is governed by Article 19(1)(a) and the law of defamation.

His exposure is a complaint under BNS Section 356, which the Supreme Court upheld in principle in Subramanian Swamy v. Union of India, (2016) 7 SCC 221, or a civil suit by the vendor. His defences are truth published for the public good and fair comment on the public conduct of a public body. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632, holds that government and public authorities cannot sue for defamation over their official conduct, so the Board itself has no such claim.

The Whistle Blowers Protection Act, 2014 gives him nothing. It has not been brought into force, and it covers only disclosures made to a designated authority

about public servants. A blog post is outside it. He was reported to be 17 at the time, so any proceedings would run through a guardian.

What the episode shows.

- The CERT-In channel worked as a mailbox and not as a coordinator. On the researcher's account, nothing was fixed in 86 days.
- The organisation's own duties were engaged. Once apprised through CERT-In, CBSE came under the six-hour reporting duty in the 2022 Directions. Whether it complied is not public.
- Neither student faced formal prosecution, and Adhikary was subsequently recruited by a national cybersecurity hub. In India today, public goodwill often serves as the most effective practical defense—though it remains an uncertain substitute for clear statutory safe harbor laws.

7.5 The view from the other side: a vendor's opinion, 2020

To understand both sides of vulnerability disclosure, consider a mirror image of the CBSE case: a written legal opinion provided by the author in February 2020 to a listed Indian technology enterprise facing an uninvited security researcher.

Instructed Facts

An individual in India tested a company's infrastructure without consent, claimed to have identified a critical flaw, made direct contact with executives, and visited corporate premises without signing a non-disclosure agreement (NDA). He cited the Carnegie Mellon CERT Coordination Center Guide to Coordinated Vulnerability Disclosure (Householder et al., 2017) as his legal justification. The company instructed that the individual was acting in bad faith and sought counsel on two points:

1. What legal standing does the foreign guide hold in India?
2. What legal mechanisms exist to prevent unauthorized public disclosure?

The Legal Opinion Summary

1. No Statutory Force: The Carnegie Mellon guide carries no legal authority in India. Neither the IT Act nor its rules recognize external framework guides as legal authorization.
2. Framework Terms Exceeded: Paragraph 4.1.2 of the guide itself specifies that testing must be conducted on systems the finder is authorized to use. Absent a published policy, no authorization exists.
3. Statutory Trespass: Access without permission violates Section 43(a); accompanying dishonest intent triggers criminal liability under Section 66. Sections 1(2) and 75 confirm extra-territorial jurisdiction where Indian systems are impacted.
4. Parallel Legal Remedies: The company possessed three concurrent avenues: filing an FIR under criminal law, lodging a claim before the Adjudicating Officer under Section 43 (for damages up to ₹50,000,000), or seeking a civil court injunction restraining disclosure.

The opinion also made an observation that this paper now develops. It recorded that for coordinated disclosure "to operate in India" there would have to be a proviso or exception to Section 43(a), and that the legislature had not enacted one.

How the opinion reads in 2026.

Point in 2020	Position in 2026
FIR under Section 154 of the Code of Criminal Procedure	Now Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023
CERT-In had only a reporting page	CERT-In adopted a disclosure policy in 2021; its clause 7 confirms that reporting gives the finder no legal cover
The matter was the companies to pursue or not	Since April 2022 the company must itself report the unauthorised access to CERT-In within six hours
Section 66 as the deterrent	Confirmed bailable in Maharaj Saran (2026); Penal Code offences may be added after Awadhesh Kumar Parasnath Pathak (2024)
No data protection statute	From May 2027, intimation to the Board and to Data Principals if personal data was reached
No exception in Section 43(a)	Still none

Reading the two cases together.

- The same provision, opposite outcomes. Both finders acted without permission and both fell within Section 43(a). The CBSE researcher reported to the national agency the same day and asked for nothing. In the 2020 matter the instructions were of mala fides. That difference is the one Section 66 is built to detect, and it explains why one finder was hired and the other faced the prospect of a complaint.
- A foreign guide is not a defence. The finder's reliance on an American best-practice document shows a common misunderstanding in the research community. Community norms describe how to disclose. They do not create permission to test.
- The confidentiality point. A company cannot impose a non-disclosure agreement on a stranger, since a contract needs assent. It does not need one. The cause of action is the access, and information obtained by unauthorised access can be protected in equity without any contract.
- The limits of the injunction. A court asked to restrain publication will apply the usual tests of prima facie case, balance of convenience and irreparable injury (Dalpat Kumar v. Prahlad Singh, (1992) 1 SCC 719). An order can properly restrain public release of exploit details. It should not restrain a report to CERT-In, for the reasons in Part 5.5.
- Both sides want the same section. The 2020 opinion, written for a complainant, noted the missing exception. Part 8 of this paper, written with the researcher in mind, drafts it. It is not often that counsel for the company and counsel for the hacker would vote for the same amendment. A provision like draft Section 43B would not have protected a finder acting in bad faith, because its first condition is honest intent. It would have told both parties on the first day where they stood.

The opinion records advice and not the result. What followed is outside this account.

7.6 Four earlier episodes: disclosure, theft and attack

Four prominent Indian episodes illustrate the legal spectrum between legitimate research, data theft, and cyberattacks:

Episode	What the record shows	Actor and Motivation	Legal character
Aadhaar app disclosures, 2018 (FactorDaily)	A French researcher using the handle "Elliot Alderson" decompiled the mAadhaar Android app and published findings on its data storage and on third-party handling of Aadhaar data. UIDAI disputed parts of his account. It had no disclosure policy or bounty at the time	An outside researcher, to force a fix	Uninvited research with public-first disclosure
The Tribune's Aadhaar report, January 2018 (Legally India)	A reporter paid 500 rupees to an anonymous seller for login credentials that opened demographic records, and published the fact. UIDAI	Investigative journalist testing public security assurances.	Access without permission; no dishonest intent on the reported facts

Episode	What the record shows	Actor and Motivation	Legal character
	lodged an FIR citing cheating and forgery provisions, Section 66 of the IT Act and Sections 36 and 37 of the Aadhaar Act		
Cyberabad data-broker arrests, March and April 2023 (Business Today)	Police arrested persons for holding and selling data said to cover 66.9 crore individuals and organisations in 104 categories, including defence personnel, government employees and PAN holders, and issued notices to 11 organisations. Some experts thought the figure inflated	Commercial data brokers operating for illicit profit. This was a police investigation and not a researcher's disclosure.	Theft and sale of data
AIIMS Delhi ransomware attack, November 2022 (Lok Sabha reply)	Five servers were affected and about 1.3 terabytes of data encrypted. An FIR was registered for extortion and under Sections 66 and 66F. CERT-In's analysis, reported to Parliament, attributed the compromise to improper network segmentation	Unknown attackers. The findings came from the national agency's own investigation	Attack; the investigation was fully authorised

The foreign researcher. The Aadhaar app disclosures raise a point the other cases do not. Section 75 extends the IT Act to a foreigner abroad where an Indian computer is involved, so the Act applied to him on paper. In practice France does not generally surrender its own nationals, and no proceedings against him have been reported. Indian law therefore deters the researcher within reach of an Indian police station and leaves the one abroad untouched. The predictable effect is to push disclosure about Indian systems offshore and onto social media, which is the least coordinated form there is.

Decompiling an application package on one's own device does not constitute unauthorized remote access under Section 43. Instead, it engages copyright law,

where Section 52(1)(ac) provides limited exceptions for interoperability testing. Conversely, querying live remote servers falls directly under Section 43(a).

The journalist. The Tribune matter is the nearest Indian example of criminal process against a tester. Buying a credential and logging in is access without permission, and using another person's password engages Section 66C on its face. The reporter did it to test an official claim and took nothing further. That is the pattern the Himachal Pradesh High Court later held to be neither dishonest nor fraudulent in Aman Kumar Bhardwaj. The Aadhaar Act as it then stood allowed prosecutions under it only on the Authority's own complaint, so the body whose security was in question also held the key to the criminal process. The sources consulted do not record how the FIR ended.

Why the other two belong here anyway.

- Cyberabad. Nobody sounded an alarm. The accused sold. Wrongful gain was the entire purpose of the enterprise, and this is the conduct Sections 66 and 66B exist to punish. The police notices to the organisations whose data surfaced also anticipate the accountability the DPDP Act will impose on data holders.
- AIIMS. Poor network segmentation is a weakness that authorised testing ordinarily finds. Here it was found after the attack, by the State's own agency, once a national hospital had been forced back to manual working. That is the economic case for bounty programmes in a single example. The episode also shows Section 66F used as intended, against attackers. Part 3.2 notes that the wording of its clause (1)(B) could equally reach a researcher who stumbles on restricted data.

Set side by side, the four episodes mark out the range: tester, journalist, thief, attacker. Section 43 treats the first three alike. Only the mental element in Section 66 tells them apart, and it does so after arrest and not before. That is the practical argument for writing the distinction into the statute.

7.7 Practical consequences

For hunters:

1. Verify Scope First: Read and record the program scope before sending an initial network request.
2. Preserve Evidence of Consent: Maintain an archived, time-stamped copy of the policy terms.
3. Use Dedicated Test Accounts: Never target real user records or production infrastructure.
4. Practice Data Minimization: Extract only the minimum data necessary to confirm the proof-of-concept.
5. Never Demand Compensation: Avoid attaching financial demands or deadlines to an uninvited vulnerability report.

For Systems Owners & Organizations:

1. Explicit Consent Clauses: Draft vulnerability policies explicitly stating that in-scope testing constitutes authorized access "with the permission of the owner" under IT Act Section 43.
2. Data Processing Frameworks: Define strict data-handling boundaries so the researcher acts within controlled data processor terms.
3. Separate Breach Protocols: Maintain clear separation between bug bounty mechanisms and formal incident response workflows under the DPDP Act and CERT-In directions.

VIII. REFORM PROPOSALS

India needs a short statutory safe harbour for good-faith security research, placed in the IT Act or its successor. Policy documents cannot do the job. CERT-In's own disclosure policy records that it cannot exempt anyone from the law, and it is right about that. At present the person who tells you your door is open and the person who walks in and takes the television are caught by the same clause of Section 43. They are separated only by what a magistrate later concludes about their thoughts. A legal system can do better than that with one additional section.

8.1 A draft provision

The draft below borrows the convergent conditions identified in Part 6 and fits them to the structure of Sections 43 and 66.

43B. Good-faith security research. (1) Nothing in section 43, section 66, section 84B or section 84C shall apply to an act of accessing, or attempting to access, a computer resource done solely for the purpose of good-faith testing, investigation or correction of a security vulnerability, where the conditions in sub-section (2) are met.

(2) The conditions are that the person (a) acts without intent to cause wrongful gain or wrongful loss; (b)

does no more than is necessary and proportionate to confirm the vulnerability; (c) does not retain, disclose or use any data accessed, save as necessary to report it; (d) reports the vulnerability to the owner or person in charge, or to the Indian Computer Emergency Response Team, within seventy-two hours of discovery; (e) makes no demand for payment as a condition of reporting or of non-disclosure; and (f) does not publish details of the vulnerability before it is remedied or before the expiry of such period as may be prescribed, whichever is earlier.

(3) This section shall not apply to a protected system declared under section 70 except in accordance with a programme notified by the appropriate Government.

(4) An act done in accordance with a vulnerability disclosure policy or reward programme published by the owner or person in charge shall be deemed to be done with permission for the purposes of section 43.

(5) No term of any contract shall prevent a person from reporting a security vulnerability to the Indian Computer Emergency Response Team or to any authority established by law.

Sub-section (1) establishes the core safe harbor. By explicitly referencing the offense of attempt and abetment, it ensures that an incomplete or failed security test receives the exact same legal immunity as a successful one. By explicitly referencing the offense of attempt and abetment, it ensures that an incomplete or failed security test receives the exact same legal immunity as a successful one. Sub-section (2) keeps it narrow; each condition has a counterpart in the Belgian, Dutch or American model. Sub-section (3) protects critical infrastructure while leaving room for government programmes. Sub-section (4) puts beyond doubt what Part 4.6 argues is already the law. Sub-section (5) prevents private contracts or non-disclosure agreements from barring good-faith disclosures to designated public authorities.

8.2 Supporting measures

1. A designated coordinator. CERT-In should be given the statutory role that Article 12 of NIS2 gives a national CSIRT, which is to receive reports, keep the reporter's identity confidential on request, and certify compliance with the conditions.
2. A filter before registration of an FIR. Where the accused holds a CERT-In acknowledgement of a timely report, a preliminary inquiry should be required before any case under Section 66 is registered. This addresses the decentralised policing problem noted in Part 6.6.
3. Mandatory disclosure policies for high-risk entities. Significant Data Fiduciaries under the DPDP Act and operators of Critical Information Infrastructure should be legally required to publish a Vulnerability Disclosure Policy (VDP). Security researchers cannot report vulnerabilities responsibly through channels that do not exist.
4. Clarification under the DPDP Rules. Rules framed under the DPDP Act should explicitly clarify that access by a researcher operating strictly within a published program's scope does not constitute a reportable personal data breach. Furthermore, a bug hunter acting under program terms should be classified as a Data Processor acting on written instructions.
5. Leveraging International Treaties. India's signature of the UN Convention against Cybercrime will require a review of domestic offences before ratification. The safe harbour should be part of that exercise.
6. A fixed statutory disclosure clock. The CBSE episode shows what happens without one. The rules should prescribe a single period, ninety days being the common industry figure, after which a researcher who has reported and heard nothing may publish, and should oblige CERT-In to tell the reporter within that period what has been done.

8.3 Model programme clauses for use now

Until Parliament acts, organisations can close most of the gap by drafting. Three clauses do the essential work.

- Authorisation. "Testing carried out in accordance with this policy is carried out with our permission as owner and person in charge of the systems in scope, for the purposes of section 43 of the Information Technology Act, 2000."
- Data handling. "Where testing unavoidably exposes personal data, you act on our behalf and on our instructions. You must access the minimum necessary, must not copy or retain it beyond what is needed for your report, and must delete it once the report is acknowledged."
- No adverse action. "We will not initiate or support any civil claim or criminal complaint against you for conduct within this policy, and if a third party

does so we will state in writing that your conduct was authorised."

The third clause matters more than it looks. It cannot stop the State, but a written statement from the owner that access was permitted removes the first ingredient of every relevant offence.

IX. CONCLUSION

The question in the title has a clear answer and an awkward remainder. Bug bounty hunting is legal in India when it is done by invitation and within the invitation's terms. The IT Act penalises access "without permission", a published programme is permission, and the Supreme Court has confirmed that Section 66 does not reach a person who has authority and no dishonest intent. The bounty itself is an ordinary unilateral contract of the kind Indian courts have enforced since the reward cases of the early twentieth century.

The difficulty lies with the uninvited researcher. Under current Indian law, an unsolicited finder might have a credible defense against a criminal charge, but they remain completely exposed to civil liability for unauthorized access. Worse still, the distinction between a helpful security disclosure and a criminal offense is drawn after the fact by whoever happens to read the initial police complaint.

Other jurisdictions have recognised that this arrangement discourages the conduct a digital economy most needs. Belgium has legislated, the Netherlands and the United States have issued prosecutorial policies, and the United Kingdom has said it is considering a statutory defence. In India the CBSE episode of 2026 ended well for the researcher because the public took his side, which is a different thing from the law taking it.

India has three compelling reasons to modernize its cyber framework now:

1. Regulatory Risk under the DPDP Act: As the Digital Personal Data Protection Act framework becomes fully operational by May 2027, data breaches carry statutory penalties reaching up to ₹250 crore. Organizations desperately need proactive, authorized security testing to identify vulnerabilities before exploitation.
2. International Treaty Harmonization: Having signed the UN Convention Against Cybercrime, India must review and update its domestic cyber offense provisions prior to ratification.
3. Protecting Domestic Talent: India boasts a vast community of skilled security researchers. Without local legal safe harbors, these talent pools will continue directing their efforts toward foreign bug bounty programs that offer clear legal protections.

Kant's test for a rule of conduct was whether one could will it as universal law. A rule that every stranger may probe any system he likes fails that test at once. So does a rule that anyone who reports an open door may be prosecuted as a burglar. The rule that passes is the one proposed in Part 8: enter only as far as needed, take nothing, ask for nothing, and tell the owner promptly. A legal system that can state that rule in one section has little excuse for leaving it unwritten.

Until it is written, the working advice is the maxim this paper began with. Volenti non fit injuria protects the hunter exactly as far as the owner was willing, and no further.

TABLE OF CASES Supreme Court of India and Privy Council

Case	Citation	Point relied on
Abhayanand Mishra v. State of Bihar	AIR 1961 SC 1698	Elements of attempt: intention and an act towards commission
Anuradha Bhasin v. Union of India	(2020) 3 SCC 637	Trade through the internet protected under Article 19(1)(g); proportionality
Anvar P.V. v. P.K. Basheer	(2014) 10 SCC 473	Certificate for electronic evidence
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	(2020) 7 SCC 1	Certificate for electronic evidence
Central Inland Water Transport	(1986) 3 SCC 156	Unconscionable standard-form terms

Case	Citation	Point relied on
Corp. v. Brojo Nath Ganguly		
Dalpat Kumar v. Prahlad Singh	(1992) 1 SCC 719	Tests for an interim injunction
Dr. Vimla v. Delhi Administration	AIR 1963 SC 1572	Meaning of "defraud"
K.S. Puttaswamy v. Union of India	(2017) 10 SCC 1	Informational privacy
Maharaj Saran v. State of Punjab	2026 SCC OnLine SC 1378	Section 66 is bailable by virtue of Section 77B
Malkiat Singh v. State of Punjab	(1969) 1 SCC 157	Preparation distinguished from attempt
Mohori Bibee v. Dharmodas Ghose	(1903) ILR 30 Cal 539 (PC)	Minor's agreement void
R. Rajagopal v. State of Tamil Nadu	(1994) 6 SCC 632	Public authorities cannot sue for defamation over official conduct
Ramesh Rajagopal v. Devi Polymers Pvt. Ltd.	(2016) 6 SCC 310	Authority to access and absence of dishonest intent defeat Sections 65 and 66
Sharat Babu Digumarti v. Government (NCT of Delhi)	(2017) 2 SCC 18	Special law prevails where it covers the field
Shreya Singhal v. Union of India	(2015) 5 SCC 1	Vagueness; mens rea as an ingredient of Section 66
State of Maharashtra v. Mohd. Yakub	(1980) 3 SCC 57	Proximity test for attempt
State of Punjab v. Amritsar Beverages Ltd.	(2006) 7 SCC 607	Technology-sensitive interpretation
State of West Bengal v. B.K. Mondal & Sons	AIR 1962 SC 779	Conditions of Section 70, Contract Act
Subramanian Swamy v. Union of India	(2016) 7 SCC 221	Criminal defamation upheld
Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.	(2010) 3 SCC 1	Contract concluded by electronic exchange

High Courts

Case	Citation	Point relied on
Abhinav Gupta v. State of Haryana	2008 Cri LJ 4536 (P&H)	Authorised access limited by purpose
Aman Kumar Bhardwaj v. State of Himachal Pradesh	2022 LiveLaw (HP) 16	Good-faith testing of a system is not fraud
A. Shankar v. State	Madras High Court, 2010	Refusal to quash unauthorised-access prosecution
Awadhesh Kumar Parasnath Pathak v. State of Maharashtra	2024 SCC OnLine Bom 1074 (FB)	Penal Code offences may be tried with IT Act offences
Gagan Harsh Sharma v. State of Maharashtra	2018 SCC OnLine Bom 17705	Sections 43 and 66 as special law (since narrowed)
Har Bhajan Lal v. Har Charan Lal	AIR 1925 All 539	General offer accepted by performance

Case	Citation	Point relied on
Lalman Shukla v. Gauri Dutt	(1913) 11 All LJ 489	No acceptance without knowledge of offer
Raghava Chariar v. Srinivasa Raghava Chariar	(1916) ILR 40 Mad 308 (FB)	Minor may enforce a promise he has performed for
Syed Asifuddin v. State of Andhra Pradesh	2005 Cri LJ 4314 (AP)	Broad reading of Section 65

Quasi-judicial: Vinod Kaushik v. Madhvika Joshi, Adjudicating Officer, Maharashtra (on remand from the Cyber Appellate Tribunal, order of 29 June 2011).

Foreign cases

- Carlill v. Carbolic Smoke Ball Co. [1893] 1 QB 256 (CA)
- hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022)
- Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin [1999] 3 SLR(R) 653 (Singapore HC)
- R v. Bow Street Metropolitan Stipendiary Magistrate, ex parte Government of the United States (Allison) [2000] 2 AC 216 (HL)
- R v. Cuthbert (Horseferry Road Magistrates' Court, 2005, unreported)
- R v. Gold and Schifreen [1988] AC 1063 (HL)
- Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C. 2020)
- United States v. Sullivan (N.D. Cal. 2022; affirmed 9th Cir. 2025)
- Van Buren v. United States, 593 U.S. 374 (2021)

TABLE OF LEGISLATION

India

- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Sections 36, 37, 38 and 47
- Bharatiya Nagarik Suraksha Sanhita, 2023, Section 173
- Bharatiya Nyaya Sanhita, 2023, Sections 2(7), 2(9), 2(11), 19, 33, 62, 238, 239, 308, 316, 318, 324, 351, 356
- Bharatiya Sakshya Adhiniyam, 2023, Section 63
- Copyright Act, 1957, Sections 52(1)(ac) and 65A
- Digital Personal Data Protection Act, 2023, Sections 2(i), 2(k), 2(u), 4, 8 and the Schedule
- Digital Personal Data Protection Rules, 2025, Rules 6 and 7 (G.S.R. 846(E), 13 November 2025)
- Foreign Exchange Management Act, 1999
- Income-tax Act, 2025
- Indian Contract Act, 1872, Sections 8, 23, 29 and 70
- Information Technology Act, 2000, Sections 1(2), 2(1)(a), 10A, 43, 43A, 46, 65, 66, 66B to 66F, 70, 70B, 72A, 75, 77A, 77B, 78, 81, 84B and 84C
- Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013
- Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013
- Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- CERT-In Directions under Section 70B(6), 28 April 2022
- CERT-In Responsible Vulnerability Disclosure and Coordination Policy, 2021
- Jan Vishwas (Amendment of Provisions) Act, 2023
- Juvenile Justice (Care and Protection of Children) Act, 2015
- Official Secrets Act, 1923
- Telecommunications Act, 2023, Section 42
- Telecommunications (Telecom Cyber Security) Rules, 2024
- Whistle Blowers Protection Act, 2014 (not brought into force)

Foreign and international

- Budapest Convention on Cybercrime, ETS No. 185 (2001), Articles 2 and 6

- United Nations Convention against Cybercrime (General Assembly Resolution 79/243, 24 December 2024), Articles 7 and 11
- Directive 2013/40/EU on attacks against information systems
- Directive (EU) 2022/2555 (NIS2), Article 12 and Recital 60
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 (United States)
- Digital Millennium Copyright Act, 17 U.S.C. Section 1201 (United States)
- Computer Misuse Act 1990 (United Kingdom)
- Computer Misuse Act 1993 (Singapore)
- Criminal Code Act 1995 (Cth), Part 10.7 (Australia)
- Belgian laws of 28 November 2022 (whistleblower protection) and 26 April 2024 (NIS2 transposition)
- Code de la défense, Article L.2321-4 (France)
- Regulations on the Management of Network Product Security Vulnerabilities, 2021 (China)

REFERENCES

[1]. Akgul, O., Eghtesad, T., Elazari, A., Gnawali, O., Grossklags, J., Mazurek, M. L., Votipka, D., & Laszka, A. (2023). Bug hunters' perspectives on the challenges and benefits of the bug bounty ecosystem. In Proceedings of the 32nd USENIX Security Symposium. USENIX Association.

[2]. Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. Management Science, 54(4), 642–656.

[3]. Bambauer, D. E., & Day, O. (2011). The hacker's aegis. Emory Law Journal, 60(5), 1051–1107.

[4]. Bellia, P. L. (2016). A code-based approach to unauthorized access under the Computer Fraud and Abuse Act. George Washington Law Review, 84(6), 1442–1476.

[5]. Elazari Bar On, A. (2019). Private ordering shaping cybersecurity policy: The case of bug bounties. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity governance. Wiley.

[6]. Fuller, L. L. (1969). The morality of law (Rev. ed.). Yale University Press.

[7]. Holmes, O. W., Jr. (1897). The path of the law. Harvard Law Review, 10(8), 457–478.

[8]. Householder, A. D., Wassermann, G., Manion, A., & King, C. (2017). The CERT guide to coordinated vulnerability disclosure (Special Report CMU/SEI-2017-SR-022). Software Engineering Institute, Carnegie Mellon University.

[9]. Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. Management Science, 51(5), 726–740.

[10]. Kant, I. (1998). Groundwork of the metaphysics of morals (M. Gregor, Trans.). Cambridge University Press. (Original work published 1785)

[11]. Kerr, O. S. (2003). Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. New York University Law Review, 78(5), 1596–1668.

[12]. Kerr, O. S. (2016). Norms of computer trespass. Columbia Law Review, 116(4), 1143–1183.

[13]. Laszka, A., Zhao, M., Malbari, A., & Grossklags, J. (2018). The rules of engagement for bug bounty programs. In S. Meiklejohn & K. Sako (Eds.), Financial Cryptography and Data Security (Lecture Notes in Computer Science, Vol. 10957, pp. 138–159). Springer.

[14]. Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. Journal of Cybersecurity, 3(2), 81–90.

[15]. Plato. (1992). Republic (G. M. A. Grube, Trans.; C. D. C. Reeve, Rev.). Hackett. (Original work c. 375 BCE)

[16]. Rampášek, M., Andraško, J., Sokol, P., & Hamuľák, O. (2026). Hunting for vulnerabilities: Call for European protection of security researchers. Journal of Cybersecurity, 12(1), tyag002.

[17]. Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P., & Malinka, K. (2024). The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. Computer Law & Security Review, 53, 105988.

[18]. Walshe, T., & Simpson, A. C. (2022). Coordinated vulnerability disclosure programme effectiveness: Issues and recommendations. Computers & Security, 123, 102936.

[19]. Walshe, T., & Simpson, A. C. (2023). Towards a greater understanding of coordinated vulnerability disclosure policy documents. Digital Threats: Research and Practice, 4(2). https://doi.org/10.1145/3586180

[20]. Weulen Kranenbarg, M., Holt, T. J., & van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. Crime Science, 7, Article 16.

Further reading consulted

[21]. Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press.

[22]. Finifter, M., Akhawe, D., & Wagner, D. (2013). An empirical study of vulnerability rewards programs. In Proceedings of the 22nd USENIX Security Symposium (pp. 273–288). USENIX Association.

[23]. Kesan, J. P., & Hayes, C. M. (2016). Bugs in the market: Creating a legitimate, transparent, and vendor-focused market for software vulnerabilities. Arizona Law Review, 58(3), 753–830.

[24]. Malladi, S. S., & Subramanian, H. C. (2020). Bug bounty programs for cybersecurity: Practices, issues, and recommendations. IEEE Software, 37(1), 31–39.

[25]. Maurushat, A. (2013). Disclosure of security vulnerabilities: Legal and ethical issues. Springer.

[26]. Pollock, F., & Mulla, D. F. The Indian Contract Act, 1872 (current ed.). LexisNexis.

[27]. Rampášek, M., & Mesarčík, M. (2025). Rethinking cybersecurity research governance: Lessons from the Act on Digital Services? European Journal of Risk Regulation. https://doi.org/10.1017/err.2025.10060

[28]. Sharma, V., & Sharma, S. Information technology: Law and practice (current ed.). LexisNexis.

[29]. Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of bug bounties. Journal of Cybersecurity, 7(1), tyab007.

[30]. Walden, I. (2016). Computer crimes and digital investigations (2nd ed.). Oxford University Press.

[31]. Walshe, T., & Simpson, A. (2020). An empirical study of bug bounty programs. In 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF) (pp. 35–44). IEEE.

[32]. Zhao, M., Laszka, A., & Grossklags, J. (2017). Devising effective policies for bug-bounty platforms and security vulnerability discovery. Journal of Information Policy, 7, 372–418.