Statutory Interpretation of "Consent" in Non-Physical Crimes

By

Alisha Barnwal & Megha

Abstract

Consent, an intricate and multifaceted concept, holds a paramount position in the realm of criminal jurisprudence. The pervasive nature of digital technology across communication, commerce, and social interaction has necessitated a re-evaluation and redefinition of the established legal standards for consent in criminal jurisprudence. While consent has historically been a valid defense for physical crimes, its relevance is questionable in the context of newer, non-physical crimes like phishing, identity theft, deep fake pornography, and AI fraud, where the notion of consent is much more ambiguous. This study analyzes how Indian laws, specifically the Indian Penal Code (IPC), Information Technology Act (IT Act), Consumer Protection Act and Digital Personal Data Protection Act, define and implement the concept of "consent". The research examines the varying interpretations and applications of consent across these different statutes to understand its legal meaning and use. The paper analyzes data privacy regulations in the EU, US, and UK before proposing a standardized legal definition of "digital consent." Adopting this definition would bolster India's data privacy protections, aid in cybercrime prosecutions, and ensure its laws are consistent with international norms and author posits that this change could strengthen data privacy, streamline cybercrime prosecutions, and better harmonize India's laws with global standards.

Introduction

In criminal law, the topic of consent plays a important role in deciding liability, specifically in offences where physical force or touching is not the main element. In the nonphysical crimes as frauds, warnings, harassments or particular sexual offences termed by communication and exposure whether the person had the consent of the victim's proper consent often determine whether act is criminal or pardonable. Interpreting "consent" in such statues is not only a question of legal settings but also can be seen as a issue of principle that imposes autonomy, fair and a proper scope of criminalization.

Statutory interpretation of "consent" involves a number of challenges. Statutes use a differing definitions of some define consent specifically while others leave it undefined and depend on courts to deliver meaning. These definitions may include or exclude situations such as whether consent might be voluntary, well-informed, and free from duress or misrepresentation or capable of being withdrawn. So because of non-physical crimes often rely on the state of mind or on conduct of communication and than physical act and being selective of kind of assent counts as "consent" actively or impliedly, verbal and non-verbal is complex. Statues must be elucidates in event of their purpose and wide legal and social values: protecting victims, ensures freedom of choice, but also keep away from overbreadth as not to criminalize normal, harmless behaviour.

When courts interpret laws that laws that hinge on "Consent", specifically in non-physical offences, they reply on certain key interpretive principles. They mostly start with literal or meaning of the words and applying them in common interpretation. If doing as such leads to the ambiguity or an unacceptable consequence, the court may start a purposive approach, inspecting the statute's aims, context, underlying policy. In situations where the word alone doesn't solve the doubts, judges look into the legislature history or explaining materials to notice the legislature's intended meaning and since criminal statute must safeguard personal rights, any left ambiguity is specifically is solved in favor of the person, in line with principle of compulsory construction of penal laws. In applying the methods together, courts seek to give effect to legislative intent while safeguarding fundamental liberties and delineated which are penalized, clearing permissible defenses and decided when consent is valid/ void in non-physical wrongdoing.

Statutory and Doctrinal Landscape

Consent, an intricate and multifaceted concept, holds a paramount position in the realm of criminal jurisprudence the term intention. It plays a pivotal role alongside actus reus and mens rea, essential components of any crime. Actus Reus denotes the physical act committed by the perpetrator, while mens rea signifies the intent to commit that act.

1. *Consent under* ***Section 90*** *of the Indian Penal Code (IPC) replaced with* ***BNS Section 28***. states that consent is invalid if given under duress (fear of injury) or a misunderstanding of the facts, provided the person acting knows or should know that the consent was given for these reasons. This means that consent is not valid if it's given because a person feels forced to do so or is acting on false information, and the person obtaining consent is aware of this situation. The original intent of this law was for physical offenses and does not account for modern forms of deception like digital manipulation or algorithmic manipulation.

Significance of Sec (90) of IPC includes ***Fear of injury*** means if a person is giving consent because of fear of being harmed that it will be invalid. Then, comes ***misconceptions of facts*** which says 'Consent'is invalid if the person is mistaken about a crucial fact and the other party knows about this misunderstanding. *For example, a court has held that consent given on a false promise of marriage is a misconception of fact and therefore invalid*. Now, ***Knowledge of the actor*** where law requires that the person performing the act must know or have reason to believe that the consent was given due to fear or misconception. At last comes ***Original intent & Other invalid consents*** as was created before the digital age and was intended for physical offenses. It does not directly address modern forms of deception, such as those found in digital environments or through algorithmic manipulation and *Other invalid consents says* consent invalid from individuals who are incapable of giving it, such as those under 12 years of age, of unsound mind, or intoxicated. ***Section (90)(3) IPC*** elucidates what does not constitute consent. This section employs a negative approach, describing situations where permission is deemed invalid. It stipulates that consent given under duress, based on misunderstanding of facts, due to insanity, intoxication, or by a child under the age of 12 incapable of understanding the nature and consequences of the act, is not considered valid.

For example, in ***R. v. Clarence (1888) 22 QBD 23***, the English Court interpreted consent Under misconception narrowly, holding that concealment of venereal disease did not Vitiate consent to intercourse. In contrast, Indian courts in ***State of U.P. v. Naushad (2013) 16 SCC 651*** broadened the meaning of "misconception of fact" in Section 90, holding that false promise of marriage could invalidate consent. This interpretive flexibility suggests that courts could analogously extend Section 90 to cover technological deception—such as phishing or impersonation in digital spaces.

The core Issue is that while physical consent is typically a clear, unambiguous action, digital consent is often a passive, automated, or manipulated process, and existing laws like the Indian Penal Code (IPC) have not kept pace which resulting "interpretive gaps" mean that courts must fit modern digital crimes into archaic legal frameworks, making it difficult to prosecute cases involving deceptive digital consent. Manipulation of digital consent is itself challenging when it comes to proving and presents major evidentiary and procedural hurdles. *The burden of proof can unfairly fall on the victim, who may be blamed for clicking a link or accepting a policy without understanding its full implications.*

2. Consent under the [1]***Information Technology Act, 2000*** legislation in India dealing with cybercrime and electronic commerce but doesn't but contain a specific, dedicated definition for the term "consent" and law derives its prosecutorial power from the fact where certain actions were performed without the victim's approval.

U/s ***(Section 43 and Section 66)*** Penalties are imposed on individuals who access, download, or copy data from a computer system "without the permission of the person in charge". Section 66 specifically criminalizes such actions if done with fraudulent or dishonest intent.

U/s ***(Section 66C)*** 1This provision makes it a crime to fraudulently or dishonestly use another person's electronic signature, password, or any other unique identifying feature. The offense is based on the misuse of identification features without the person's authorizationThis provision makes it a crime to fraudulently or dishonestly use another person's electronic signature, password, or any other unique identifying feature. The offense is based on the misuse of identification features without the person's authorization. At last, ***Violation of privacy (Section 66E)*** it explicitly mentions consent by punishing anyone who captures, publishes, or transmits the image of a person's private area "without his or her consent". The absence of consent is a clear, required element for conviction. The DPDP Act introduces a more formal definition of consent for data processing, specifying that it must be free, specific, informed, unconditional and unambiguous.

In case of , [2]***Shreya Singhal v. Union of India (2015) 5 SCC 1,*** the Supreme Court, by balancing free expression and privacy within the IT framework, indirectly invoked the principle of informed consent regarding online communications. This is echoed by the *case of* [3]***C.B.I. v. Arif Azim (Delhi Cyber Crime Case, 2004)***, which resulted in one of India's

[1] Information Technology Act, 2000, §§ 66C–66E.
[2] Shreya Singhal v. Union of India (2015) 5 SCC 1
[3] C.B.I. v. Arif Azim, Delhi Cyber Crime Court (2004).

first convictions for online fraud and involved obtaining consent for credit card data through deceitful means.

Therefore, the Act remains silent on consent obtained through digital misrepresentation. The outdated IT Rules, 2011, prescribe consent via letter, fax, or email, modes no longer relevant to current digital practices.

3. **Digital Personal Data Protection Act, 2023:** India's DPDP Act of 2023, personal data can only be processed with the data principal's (the individual's) permission. Section (6) of the act tells about personal data processing requires a clear, affirmative action of consent and it must be specific to the purpose, based on clear information, and not coerced or conditional and consent for personal data is consistent with the strict legal requirements of Article 7 of the EU's General Data Protection Regulation.

This [4]Article 7 emphasis ***Active, affirmative action*** where Individuals must provide consent through a clear, opt-in action, such as signing a form or checking an unticked box online. You cannot use pre-checked boxes, inactivity, or silence as a way to assume consent. Must be unconditional and not buried within other terms and conditions. Therefore, *Proof of consent & Easy withdrawing of consent must be documented and revocable.*

The Digital Personal Data Protection (DPDP) Act of 2023 institutes a fundamental shift from implied consent to explicit, active, and informed consent from the data principal. This act clearly affirm action from the individual. This disallows passive consent methods like pre-ticked boxes or assuming consent through a user's inaction (Shift from passive to Active consent).

In case, ***Justice K.S. Puttaswamy (Retd) v. Union of India (2017)*** the court unanimously affirmed that privacy is a fundamental right under Article 21 of the Constitution. This judgment laid the legal and philosophical groundwork for comprehensive data protection legislation like the DPDP Act by establishing that individuals have a right to control their personal information.

4. **Consumer Protection and E-Commerce:** The Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules,2020 regulate consent in online transactions. It has two legal measures governing digital consent. First, ***The prohibition of automatic consent mechanisms*** it says the Consumer Protection (E-Commerce) Rules, 2020, e-commerce platforms are forbidden from automatically recording a consumer's agreement to a transaction. Rule 5(3) specifically outlaws the use of pre-ticked checkboxes and similar defaults to obtain consent. Instead, the law mandates that consumers must give their permission for a purchase or action through a clear, intentional, and affirmative step. Secondly, ***The ban on deceptive design***

[4] 12.General Data Protection Regulation, Art. 7, 2016 O.J. (L 119).

practices known as "dark patterns" The Central Consumer Protection Authority (CCPA) has officially made manipulative user interfaces, or "dark patterns," illegal. These are defined as design elements that intentionally trick, mislead, or pressure consumers into making choices they would not otherwise make, such as sharing personal data or making unintended purchases. By outlawing these deceptive tactics, the CCPA aims to uphold consumer autonomy and ensure that digital transactions are based on transparent and ethical practices.

The growing intersection of consumer law and data protection, both of which aim to empower individuals by ensuring they have genuine and un-coerced control over their digital consent. ***Transparency and genuine comprehension*** this include companies and platform explaining their data practices in clear, understandable language, rather than hiding details in complex, lengthy legal documents also, informing consumers about what data is being collected, how it will be used, who it will be shared with, and for how long it will be stored. ***Affirmative and voluntary action*** include No pre-checked boxes, Freedom from coercion and ***Protection from manipulative design*** Comes up Banning "dark pattern and Preserving autonomy.

Part II: Technology and doctrinal problems- Case Studies

Case Study 1: Phishing Scams

Phishing scams are among the most widespread and deceptive types of cybercrime, designed to deceive individuals into sharing confidential personal or financial details. The word *"phishing"* originates from *"fishing,"* reflecting the idea of baiting victims—in this case, through false messages that appear to come from credible institutions like banks, corporations, or government bodies. During a phishing attempt, attackers typically exploit emails, phone calls, text messages, or fake websites to pose as trustworthy sources. According to CERT-In's 2023 annual report, over 1,314 cases of phishing scams were reported in the year 2022 and total around 14 lakh cases were reported in India related to cybersecurity in India[5] .The fraudulent communications often instill panic or urgency for example, by warning of hacked accounts, delayed deliveries, or pending transactions to trick users into clicking on harmful links or revealing private information such as passwords, credit card data, or one-time password (OTPs).

Indian courts have prosecuted such cases like in the case of Hare Singh v. Reserve Bank of India & Ors.[6] Of which details are given below:

Facts:- Hare Ram Singh, a 55-year-old academic, lost ₹2.6 lakh due to a voice phishing (vishing) scam on April 18, 2021. He received a fraudulent phone call instructing him to click a malicious link, which resulted in unauthorized withdrawals from his State Bank of India (SBI) account. Despite promptly reporting the incident to SBI's customer service, branch officials, and the police, the bank did not act quickly. SBI later

[5] CERT-In Annual Report 2022 (Ministry of electronics and information technology)
[6] Hare Singh V. Reserve Bank of India and Ors. (2024) (W.P.(C) 13497/2022)

denied his claim, arguing that the transactions occurred due to the customer's use of One-Time Passwords (OTPs) and engagement with the suspicious link.

Issues:-

1. **Jurisdiction** – Whether the Delhi High Court could adjudicate the matter, given that the transactions took place in Greater Noida.
2. **Customer Negligence** – Whether Singh's actions could be considered negligent, affecting his responsibility for the losses.
3. **Bank's Duty** – Whether SBI failed in its obligation to secure the customer's account and respond promptly to the reported fraud.
4. **RBI Guidelines Compliance** – Whether the bank acted in accordance with the Reserve Bank of India's guidelines on unauthorized electronic banking transactions.

Judgment:- The Delhi High Court, under Justice Dharmesh Sharma, ruled in favor of Hare Ram Singh. The court held that SBI had a responsibility to protect its customers and did not respond promptly to the fraud report. The delay and inadequate security measures demonstrated negligence on the bank's part.

The judgment clarified that under RBI guidelines, the bank carries the burden of proving customer liability in cases of unauthorized electronic transactions. As a result, SBI was directed to refund ₹2.6 lakh to Singh with 9% interest from April 18, 2021, along with ₹25,000 as legal costs. The court stressed the importance of banks maintaining strong security protocols and acting swiftly to address reported frauds.

Internationally, the Experi-metal, Inc. V. Comerica Bank (2011)[7], states the following;

Facts

Experi-Metal, Inc., a company based in Michigan, used Comerica Bank's online wire transfer platform, TM Connect, to handle its financial transactions. The company authorized an employee, Keith Maslowski, to initiate transfers. In January 2009, Maslowski became a victim of a phishing attack and inadvertently shared his login credentials with a fraudulent website. As a result, cybercriminals gained access to Experi-Metal's accounts and carried out 93 unauthorized wire transfers totaling over $1.9 million within six hours. While Comerica Bank was able to recover some of the stolen funds, roughly $560,000 remained unrecovered.

Issue

1. Authorization of Transfers- Whether the transactions carried out using the employee's credentials legally bound Experi-Metal.
2. Bank's Duty of Good Faith – Whether Comerica Bank acted in good faith and adhered to reasonable commercial standards in handling the transfers, as required under Michigan's Uniform Commercial Code (UCC) § 440.4702.
3. Recovery of Funds – Whether Experi-Metal could claim the remaining unrecovered funds from the bank.

[7] Experi-metal, Inc. V. Comerica Bank (U.S. Eastern District of Michigan, 2011)

Judgment

The U.S. District Court for the Eastern District of Michigan ruled in favor of Experi-Metal, holding Comerica Bank responsible for the unrecovered $560,000. The court found that although the transfers used valid credentials, the bank did not meet the "good faith" standard outlined in the UCC. Comerica Bank failed to follow reasonable commercial practices, especially in monitoring unusual overdrafts in Experi-Metal's accounts. The court concluded that the bank's inability to detect the fraudulent transactions constituted a breach of its duty to act in good faith .

Case Study 2: Deepfake Pornography

Deepfake pornography is a form of digital exploitation where artificial intelligence (AI) and machine learning are used to create realistic but entirely fabricated sexual images or videos of people without their permission. The term *"deepfake"* is derived from *"deep learning"* (a type of AI) and *"fake,"* reflecting the technology's ability to produce highly convincing audio-visual content that is completely synthetic. This phenomenon presents major ethical, legal, and technological challenges. It raises concerns about privacy violations, consent, sexual harassment, cybercrime, and intellectual property misuse. As shown in the research " Deepfake Porn: why we need to make it a crime to creat it, not just share it"[8]. Around the world, governments are struggling to establish laws, implement regulations, and protect victims, largely due to how easily such content can be generated, circulated, and anonymized.

Indian cases such as Babydoll Archi case (2025)[9] gives us a deep glance about the danger under:-

Facts

In July 2025, Archita Phukan, a married woman from Dibrugarh, Assam, became the target of a cyber defamation scheme carried out by her ex-boyfriend, Pratim Bora, a mechanical engineer from Tinsukia. Bora used AI platforms such as Midjourney, Desire AI, and OpenArt to fabricate explicit images and videos by placing Phukan's face onto artificial bodies. He then created an Instagram account under the pseudonym *"Babydoll Archi,"* which quickly amassed over 1.4 million followers. The account posted misleading content implying Phukan's involvement in the adult entertainment industry, including AI-generated images featuring adult film actress Kendra Lust. Bora monetized this fake identity through subscription services, earning approximately ₹10 lakh.

Issues

- Jurisdiction: Whether the Dibrugarh Police had the legal authority to investigate and detain Bora, given that he resided in Tinsukia.
- Negligence: Whether Phukan's online sharing of personal photos contributed to the misuse of her image.
- Financial Oversight: Whether banks or payment platforms failed to detect or prevent transactions related to the monetization of the fabricated account.
- Regulatory Guidelines: Whether the Reserve Bank of India's protocols on unauthorized digital transactions applied in this context.

[8] https://www.durham.ac.uk/research/current/thought-leadership/2024/04/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it.

[9] Archita Phukan v. Pratim Bora" or "State of Assam v. Pratim Bora (July 2025)

Judgment

Following Phukan's complaint, the Dibrugarh Police arrested Pratim Bora on July 12, 2025. Bora confessed to using a single photograph of Phukan to generate explicit AI content and profited from subscription-based platforms. He faced charges under various provisions of the Bharatiya Nyaya Sanhita (BNS), covering cyber harassment, defamation, obscenity, and privacy invasion. The court authorized five days of police custody for further investigation.

On international level cases like in Spain School child Sentenced for AI-Generated Images

In July 2024, a Spanish court handed down one-year probation sentences to 15 schoolchildren who had created and circulated AI-generated nude images of their female classmates. The images were shared within WhatsApp groups, resulting in charges related to child abuse and violations of moral integrity. The court also requred the students to attend educational programs on gender equality and responsible technology use, highlighting the role of awareness and education in preventing such misconduct.

Case Study 3: Data Theft and Consent Fatigue

Data theft refers to the unauthorized acquisition, use, or collection of personal or sensitive information by cybercriminals, organizations, or other parties without permission. In today's digital era, vast amounts of personal data—ranging from financial information to behavioral patterns and location details—are continuously gathered, often without individuals fully understanding how it will be used. Such unauthorized access can result in identity theft, financial harm, privacy breaches, and reputational damage. Consent fatigue occurs when individuals are repeatedly asked to grant permission for data collection, app access, cookies, or privacy policies. This constant stream of requests can lead people to accept terms quickly without careful review, increasing their vulnerability to data misuse and theft.

One of the notable Indian cases like Big Basket Data Breach (2020)[10] :-

Facts

- Incident Timeline: The data breach took place on October 14, 2020, but was publicly revealed by cybersecurity firm Cyble Inc. on November 7, 2020.
- Data Compromised: Over 20 million users' personal information was exposed, including names, email addresses, phone numbers, physical addresses, dates of birth, IP addresses, password hashes, PINs, and order details.
- Cause of Breach: The breach resulted from an insecure SQL file, likely exploited through an SQL injection attack, containing more than 15 GB of user data.
- Monetary Value: The stolen data was reportedly being sold on the dark web for roughly ₹30 lakh (around $40,000 USD).

Issues

- Regulatory Gaps: At the time, India did not have comprehensive data protection legislation, making it difficult to hold companies accountable for lapses in data security.

[10] Yarlagadda Kiran Chandra vs. Union of India & Anr..

- Corporate Responsibility: BigBasket's delay in publicly acknowledging the breach and lack of immediate remedial measures raised questions regarding its accountability in safeguarding user information.

Judgment

- Legal Actions: BigBasket lodge a First Information Report (FIR) with the Bengaluru Cyber Crime Cell on November 6, 2020, a day prior to the breach being publicly disclosed.
- Company Response: The company clarify that it did not store financial details such as credit card numbers and emphasized its commitment to protecting user privacy and confidentiality.
- Regulatory Response: Despite the scale of the breach, no major penalties or enforcement actions were taken against BigBasket due to absence of specific provisions under the Information Technology Act, 2000, and the lack of a comprehensive data protection law in India at that time

Comparitive Jurisprudence and Global Lessons

Comparative jurisprudence examines the legal systems, doctrines, and judicial practices of different countries to understand their similarities, differences, and foundational philosophies. By exploring how various nations interpret and enforce laws, this discipline offers valuable insights into the development of legal concepts, the effectiveness of statutes, and the operation of judicial institutions. Its significance goes beyond academic study, providing practical advantages as well. Lawmakers, judges, and legal scholars can draw lessons from international experiences, adopt effective legal mechanisms, and avoid errors seen in other jurisdictions.

In India one of the most notable case Vishakha & Ors. v. State of Rajasthan[11] :

Facts

The case originated after Bhanwari Devi, a social worker from Rajasthan, was gang-raped while trying to prevent a child marriage in her village. At that time, India had no specific legislation addressing sexual harassment at the workplace or measures to protect women against such crimes. A group of women's organizations approached the Supreme Court of India, requesting judicial guidelines to prevent workplace harassment and ensure proper remedies for victims.

Issues

1. Absence of Legislation: Whether the lack of statutor provisions to prevent sexual harassment infringed upon women's fundamental rights under Articles 14, 19, and 21 of the Constitution.
2. State Responsibility: Whether the state was obligate to ensure a safe working environment for women and protect them from harassment.
3. Application of International Law: Whether international treaties, including the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), could guide the formulation of domestic guidelines.

Judgment

The Supreme Court of India ruled that sexual harassment in the workplace constitutes a violation of fundamental rights. In the absence of dedicate legislation, the Court issued the Vishakha Guidelines, which remained in force until formal laws were enacted. Key directions included:

[11] Vishakha and Others v. State of Rajasthan (1997)

- Establishing mandatory preventive and grievance redressal mechanisms in workplaces.
- Requiring employers to provide a safe work environment for women.
- Setting up Internal Complaints Committees (ICCs) to address complaints.

The judgment drew on international conventions, particularly CEDAW, emphasizing India's duty to uphold gender equality and protect women's rights.

Proposal for a Unified Definition of Digital Consent

Digital consent is a freely given, specific, and informed agreement by a competent person through a clear, affirmative digital action. A valid digital consent have five fundamental characteristics:-

- Free: The consent must be given voluntarily, without being forced or coerced. This implies that refusing to give consent should not result in any penalty or loss of benefits to which a person is otherwise entitled.
- Expression of will by a competent person: The individual giving consent must have the legal and mental capacity to do so. For example, a child may not have the capacity to give consent, requiring a parent to act on their behalf.
- Specific: Consent must be clearly tied to a particular digital act or data processing activity. It cannot be a broad, all-encompassing "blanket consent" for any possible future use.
- Informed
- Unambiguous: The agreement must be indicated through a clear and positive action from the person.

Prohibited methods for obtaining consent include *Coercion*, which Compels a person to act involuntarily through the use of force, threats, or intimidation. *Impersonation* which Falsely assuming someone else's identity to provide consent on their behalf. *Deception* Misleading or tricking a person into giving consent, such as misrepresenting what their data will be used for. *Undue influence* Exploiting a position of power or a relationship of trust to pressure someone into a decision against their best interests.

Rationale and Structure

- Freedom: Recognizes coercion in digital contexts—threats, blackmail, or extortion Via technology—as vitiating consent.
- Specificity: Prevents broad, bundled consent across unrelated services.
- Informedness: Mandates disclosure in plain language, following GDPR Recital 42.
- Unambiguous Expression: Requires affirmative, documented consent (no implied or default consent).
- Anti-Manipulation Clause: Acknowledges psychological and AI-driven manipulation as invalidating consent.

In order to address modern digital threats, Section 66D of the IT Act should be modified to explicitly encompass deep fake-induced or AI-simulated impersonation within the legal definition of *cheating by personation* and Amend Section 90 of IPC to include deception by digital or automated means.

Enforcement, Evidentiary, and Institutional Reforms

Enforcement, evidentiary, and institutional reforms are measures aimed at improving the execution of laws, optimizing the collection and utilization of evidence, and strengthening the efficiency and capacity of institutions responsible for administering justice. These reforms help ensure that legal provisions are

implemented effectively, providing fair, transparent, and dependable processes for dispute resolution and accountability.

Enforcement reforms emphasiz making laws actionable through better monitoring, compliance systems, and strict penalties for violations.

Evidentiary reforms focus on enhance the methods for gathering, preserving, and presenting evidence to ensure decisions are accurate and reliable.

Institutional reforms seek to bolster the function of courts, regulatory authorities, and law enforcement agencies by improving resources, training personnel, ensuring accountability, and streamlining procedures.

Conclusion

Consent in criminal law must evolve beyond its corporeal origins. The legal understanding of consent traditionally rooted in physical interactions and bodily integrity, is insufficient for the modern digital world and criminal offenses involving a lack of consent like assault or battery, were defined by physical acts. By adopting global standards and embedding anti-deception safeguards Indian law can reclaim the normative essence of consent autonomy, transparency and dignity also the problem with the current legal framework is in lacks a single, consistent, and comprehensive definition of "digital consent" that is applicable across all these laws. This creates gaps and ambiguities that criminals can exploit and solution for this legal system must unify these disparate regulations into a coherent and coordinated framework. Instead of using physical threats or force (coercion) to gain compliance, malicious actors in the digital realm use psychological tactics like deception, disinformation, and social engineering (manipulation).