International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

CYBERCRIME AND DATA PROTECTION LAWS IN INDIA: EMERGING LEGAL CHALLENGES

Hitesh Lathar
UGC / NET Qualified, Department of Law

ABSTRACT
The digitization of governance, business, banking and social interaction in India has been happening at an unprecedented speed and with it, the rise of the cybercrime and the need for a robust data protection law. This paper explores the statutory landscape of cyberspace in India over the past two decades, first the Information Technology Act, 2000 and then the Information Technology (Amendment) Act, 2008, until the Digital Personal Data Protection Act, 2023, the country's first comprehensive personal-data law, was enacted. The paper is divided into five thematic sections, respectively addressing the statutory framework of cyber law, the data protection regime, cybercrimes against individuals, cybercrimes against property and the State and new challenges created by artificial intelligence, cross-border data flows and cloud jurisdiction. A separate chapter then examines key court rulings such as that in Shreya Singhal v. Union of India, Justice K.S. Puttaswamy's decision in its favour and other privacy, intermediary liability and electronic evidence cases, that have influenced the application of these laws. The paper states that while India has constructed a reasonably developed legal structure, there are still several areas of enforcement, cooperation, victim redressal and regulation of emerging technologies which remain unaddressed. Finally, it provides recommendations on the strengthening of the institutional capacity, harmonisation of the Digital Personal Data Protection Act with sectoral regulation and reform of criminal procedure in order to address the challenges posed by the fast-changing digital environment.

KEYWORDS
Cybercrime; Data Protection; Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Right to Privacy; Cyber Law in India; Data Fiduciary; Intermediary Liability.

INTRODUCTION
Today, India has one of the world's largest populations with an internet presence and the use of digital payments, e-governance apps including Aadhaar and DigiLocker and social media are changing the way hundreds of millions of people live their everyday lives. The "Digital India" initiative, which is part of this revolution, has created huge economic and administrative value, but has also increased the attack areas for cybercrime and created serious concerns over the security of personal data. From the theft of funds to identity theft, from “hacktivism” to hacking critical infrastructure and from the non-consensual dissemination of intimate images to the collection and processing of personal data by both the State and private parties, offences against the integrity of the data have become more frequent, more complex and more constitutionally problematic.

India's legal reaction to these changes has been piecemeal, not holistic. The first Indian law to give legal recognition to electronic transactions and to criminalise some computer related offences was the Information Technology Act, 2000 ("IT Act"). It was significantly expanded

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

in 2008 to expand the reach of the cybercrime provisions and to add, for the first time, a data protection-type requirement for corporate bodies that process sensitive personal data under Section 43A. Despite the progressive recognition of privacy as a dimension of the fundamental right of life and personal liberty, under Article 21 of the Indian Constitution, this provision, read together with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, has been the backbone of data protection in India for more than a decade.

It was the nine-judge bench decision of the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) which clearly stated that the right to privacy is a fundamental right including informational privacy. This judgment provided the constitutional basis to draft a dedicated data protection law which resulted, following multiple draft bills, in the enactment of the Digital Personal Data Protection Act, 2023 ("DPDP Act"). The DPDP Act is a paradigm shift with concepts like data fiduciary, data principal, purpose limitation, an adjudicatory Data Protection Board of India and many such things which have been left for delegated rule making.

In this background, the paper attempts to conduct a structured analysis of the existing legal framework for cybercrime and data protection in India. Part I traces the development of cyber law through the statute books. Part II takes a look at the data protection regime and compares the old Section 43A regime with the DPDP Act, 2023. Part III reviews cybercrime is committed against an individual and Part IV reviews cybercrime is committed against property, financial systems and the State. In Part V, emerging challenges—such as artificial intelligence, deepfakes, cross-border data transfer and cloud jurisdiction—are just starting to be tackled by current law. Each of the case selection is then analyzed under five heads in a separate section and the paper ends with an evaluation of the current system and suggestions for reform.

I. STATUTORY FRAMEWORK OF CYBER LAW

Indian cyber law is founded on the Information Technology Act, 2000 with amendments in 2008. Ten key legal points are set out below in the same point wise format as used for the case law in Part VI in relation to the five thematic headings of this paper.

IT Act, 2000: This act was passed to provide legal status to electronic records and digital signatures. Chapter XI originally penalised a limited set of offences Section 65 (tampering with source code), Section 66 (hacking), Section 67 (publishing obscene material) and Section 70 (unauthorised access to protected systems) while Section 43 created civil liability for unauthorised access, data theft, virus introduction and denial-of-service attacks.

2. IT (Amendment) Act, 2008: Expanded the list of offences with Sections 66A (offensive messages, which were later deleted), 66B (receiving stolen computer resources), 66C (identity theft), 66D (cheating by personation), 66E (violation of privacy) and 66F (cyber terrorism). It also added to Section 43A (data-security liability for bodies corporate), enhanced intermediary safe-harbour under Section 79 and added interception/blocking provision under Sections 69, 69A and 69B and also renamed the evidentiary provisions as Bharatiya Sakshya Adhiniyam, 2023.

These two statistics reveal a definite legislative trend: from an enabling e-commerce law in 2000 to a criminal law for cyberspace in 2008. This multi-layered approach to the registration

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

and investigation of cybercrime, coupled with special rules relating to interception, blocking and intermediary behaviour, continues to underpin the current regime of data protection and sector-specific provisions discussed below (Seth, 2016).

II. DATA PROTECTION REGIME

India's data protection law went from a limited provision of corporate liability to a broad rights-based law in the two points below:

Section 43A & SPDI Rules, 2011: It requires the body corporate to be liable in case of a wrongful loss or gain to any person as a result of negligent failure to take reasonable measures to protect the security of the information or data handled and stored by it, when the information or data of that person is of a sensitive nature. The Rules of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) 2011, otherwise known as the SPDI Rules, further clarify this by listing down sensitive information (including passwords, financial information, medical records, biometric information, health information, sexual orientation information, medical information and biometric information). It is required that organisations have a clear privacy policy, ensure that organisations do not collect sensitive information unless consented, that such information is only used for a lawful and specified purpose, that disclosure and transfer of such information is regulated, that there is a mechanism for correcting information, that there is a mechanism for grievance redressal and that recognised information-security standards are maintained. Combined, Section 43A and the SPDI Rules laid a significant basis for accountability and safeguarding of sensitive personal data of a company in India (Duggal, 2014).

Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection Act, 2023 is a comprehensive Act that regulates the processing of digital personal data in India. It is applicable to digital data processing in India and in some cases, data processing outside India for providing goods or services to persons in India. The Act stipulates that Data Fiduciaries use personal data for lawful purposes, typically relying on free, specific, informed and unambiguous consent and maintain reasonable security measures to prevent personal-data breaches. It provides Data Principals with certain rights such as access to data, the ability to have their personal data corrected or deleted, grievance redressal and authorization of another person to act on their behalf. The Act also mandates greater protection for children's data, imposes stricter duties on significant data fiduciaries and creates the Data Protection Board of India to look into violations and impose monetary penalties, some of which can top out at ₹250 crore for certain offences. Therefore, the Act aims to strike a balance between the rights of the individuals to protect their personal data and the legitimate needs of processing such data for lawful purposes (Ministry of Law and Justice, 2023).

III. CYBERCRIMES AGAINST INDIVIDUALS

Cybercrime against persons is an act committed through a computer, mobile phone, communication network, social media or other electronic device, communication service or technology that directly affects a natural person. These crimes could be committed to obtain money, personal details, take another person's identity, breach of privacy, damage to reputation, harassment and threats, or sexual and psychological exploitation. Cybercrimes have

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

several differences from "real" crimes; the perpetrator can hide, be in a different jurisdiction and even use automated tools to spread harmful content and/or spam almost immediately after creation. This means that one illegal act – such as posting an intimate photo or hacking into a bank account – can have ongoing financial, social, emotional and reputational consequences. Offences relating to a computer or digital device which may be used as an instrument of the offence, the target of the offence or in which a computer or digital device is used as the medium of the offence are included. For instance, in phishing and online impersonation, technology is used to mislead and deceive the victim; in hacking, the victim's computer system or account is used to harm the victim; and in cyberstalking or online defamation, the Internet becomes the vehicle for harassment and reputational harm. Thus, cybercrimes committed against the person impact multiple legally protected interests, such as privacy, dignity, personal liberty, property, reputation, identity and bodily autonomy.

These crimes are primarily governed by the Information Technology Act, 2000 along with sections of the Bharatiya Nyaya Sanhita, 2023 (BNS) in India. Special laws such as Protection of Children from Sexual Offences Act, 2012, Digital Personal Data Protection Act, 2023 and other special laws may also be applicable depending on the age of the victim and the nature of the offence. Unauthorised access, identity theft, computer-related cheating, breach of privacy and electronic publication or transmission of obscene and sexually explicit material are specifically covered by the Information Technology Act. The BNS broadens this concept by including offences against the person (e.g. stalking, voyeurism, cheating, criminal intimidation, extortion, forgery and defamation) if committed via digital means (Wall, 2007).

In the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court had extended the constitutional protection of privacy to individuals in the virtual world. The judgment stated that there were two aspects of privacy: bodily privacy and informational privacy and the individual's right to control choices and personal information. Unauthorized surveillance, disclosure of intimate content, misuse of personal information and other forms of electronic intrusion, therefore, requires a consideration of not only a technological misconduct but also the violation of dignity, liberty and autonomy.

MAJOR TYPES OF CYBERCRIMES AGAINST INDIVIDUALS

There are several different kinds of cybercrimes committed against people, which can be grouped based on the harm inflicted. Some offences are directed towards the property and financial interests of the person (e.g. phishing, online banking fraud), while others are directed towards privacy, reputation, dignity or personal safety (e.g. cyberstalking, doxxing, sextortion of personal content, non-consensual dissemination of intimate content). Often the categories overlap. For example, a hacker might possibly initially obtain private photos from a victim's account, threaten to publish the photos and then request cash. Such activities can be in conjunction with unauthorised access, privacy breach, criminal intimidation and extortion.

1. Identity Theft

Identity theft is when an individual lends or uses someone else's password, electronic signature, biometric identifier, Aadhaar-related information, banking details or any other unique ID. The stolen identity can be used to open new accounts, get loans, create social-media

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

profiles, make transactions or be used to offend in the victim's name. Hardly anything can be worse than the financial loss that results from identity theft as well as the long term reputational and legal problems that follow if the crimes seem to have been committed by the victim.

Specific punishment for fraudulent or dishonest use of another person's electronic signature, password or unique identification feature is provided in Section 66C of the Information Technology Act, 2000. Additionally, where the stolen identity is used in order to defraud another person of money or property then Section 66D of the Act and the provisions relating to cheating and cheating by personation found in Sections 318 and 319 of the BNS also apply. It depends on the nature of the method, the purpose and the damage caused by the wrongdoings (McNally, 2005).

2. Phishing and Online Financial Fraud

Phishing is a fraudulent activity where an offender sends an email, short message service (SMS), social media message or website link disguised as a message from a bank, government, online marketplace, or other trusted entity. The victim is induced to reveal an OTP, password, card number, UPI PIN or other financial information. Phishing includes voice phishing or "vishing," SMS phishing or "smishing," fake QR codes, application fraud that utilizes remote-access apps and false customer-care scams. The acts could be covered under section 66D of the Information Technology Act if the offender is deceiving the victim using a communication device or computer by pretending to be another person or institution. Two other provisions of the BNS might also apply to cheating and cheating by personation: Section 318 and Section 319. Sections 43 and 66 of the Information Technology Act may also be applicable where such access, copying, extraction of data from the victim's device or account is done in an unethical manner. The offence is not just committed with the use of technology but when technology is used dishonestly or fraudulently (Legislative Department, 2023).

3. Cyberstalking

Cyberstalking involves repeatedly monitoring, contacting, following or harassing an individual through social media, email, messaging applications, location-tracking services or other electronic means. This can involve sending unsolicited messages, snooping on the internet, registering multiple accounts after being banned, knowing the victim's location or threatening to reveal private information. The constant fear associated with cyberstalking may stem from the fact that the stalker could be on many different websites and could contact the victim at any moment. The BNS is a section of the law devoted to stalking and can include monitoring the use of the internet, email or other electronic communication to monitor a woman. If stalking includes threats, Section 351 of the threats concerning criminal intimidation may apply. Sections 43 and 66 of the Information Technology Act could also be invoked if the perpetrator is guilty of unlawfully accessing the victim's account or device. Provisions are applied based on the identity of the victim, the frequency of the conduct, the intent of the offender and whether the contact was continued despite clear disinterest.

In State of Tamil Nadu v. Suhas Katti (2004), the defendant posted obscene and defamatory messages in an online group about a woman and used her contact details to cause unwanted communications. The case is well known as being one of the first convictions in India for

electronic harassment and the posting of obscene electronic material. It showed that the behaviour that takes place in a virtual forum can cause actual damage to the victim's dignity, reputation and personal security.

4. Cyberbullying and Online Harassment

Cyberbullying is repeated insults, intimidation, shaming, excluding or emotional harming of someone through digital communication. This can include abusive messages, embarrassing comments, tampered photos, rumors, a coordinated attack on the victim, or the creation of a profile dedicated to bullying the person. Children, adolescents, women and those who have public facing jobs may be especially vulnerable. There is no single cyberbullying-related law in India. The legality of the provision hinges on the information sent and the impact of the information. Threatening messages could be covered by the BNS definition of criminal intimidation (Section 351); defamatory statements may be covered by Section 356 of the BNS; obscene electronic material may be covered by Section 67 or 67A of the BNS; and sexually coloured remarks or conduct directed at a woman may be covered by other sections of the BNS. But offensiveness alone isn't enough to be considered a crime, unless the ingredients of a valid penological provision are met (Patchin, 2015).

This was highlighted in the Shreya Singhal v Union of India (2015) case where the Supreme Court had ruled that since Section 66A of the Information Technology Act had been too broadly worded, it had violated the freedom of speech. The judgment drew a clear distinction between discussion and advocacy and the unlawful incitement and also pointed out that an online expression may not be criminalized simply for being annoying, inconvenient or unpopular. In light of this, any real cyber harassment has to be prosecuted on the basis of constitutionally valid provisions with clear legal components.

5. Online Impersonation and Fake Profiles

Online impersonation means when someone impersonates another user by using their name, picture, designation or any personal information to trick other users. Fake profiles can be used to request funds, set up a romance or marriage scam, bully the person or send fake information or ask for sexual photos and videos. Where there is no immediate monetary loss, the abuse of a person's identity can have serious consequences for his or her reputation and personal relationships. Section 66C of the Information Technology Act may be applicable in instances where another person's password or unique identification is dishonestly used and Section 66D may be applicable in instances where impersonation is done by using another person's password or unique identification through a computer resource. The BNS might also apply per the misleading conduct and resulting harm in Sections 318 and 319. The BNS and the Information Technology Act (Ahmad, 2011) Sections 67 and 67A may also impose liability on the offender in case the fake account distributes defamatory or sexually explicit material (Ahmad, 2011).

6. Hacking and Unauthorised Access

Hacking—with regard to crimes against individuals means obtaining access to a person's computer, mobile device, e-mail, cloud storage, or social-media account without his or her consent. The offender could make copies, change data, remove data, or allow them to be

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

released; install spyware; activate a camera or microphone; or, prevent the lawful owner from accessing the account. The damage can encompass financial loss, damage to crucial paperwork, monitoring and disclosure of private communications.

Unauthorized access, downloading, copying or extraction of data, introduction of malware, computer systems disruption and denial of access to authorised computer systems becomes liable as per Section 43 of the Information Technology Act. If those acts are carried out dishonestly or fraudulently, then Section 66 creates criminal liability. A misuse of passwords or identifying credentials may also apply to the misappropriation of the same under Section 66C. Therefore, the existence of unauthorised access alone may be sufficient for consequences pursuant to Section 43, but a criminal liability pursuant to Section 66 is normally based on proof of dishonest or fraudulent intention (Brenner, 2010).

7. Violation of Privacy and Voyeurism

Digital violation of privacy is when an offense is committed by the capture, storage, access, publication or transmission (without the consent of the person concerned) of his/her private images, videos, communications or personal information. It can be via screenshots, hidden cameras, hacking of a cloud account, or another device. It can also be as a result of a material being recorded by someone else that was meant for a private purpose. When creating or sharing an image with another person, there is no assumption of permission for the image to be published or circulated without explicit permission.

Section 66E of the Information Technology Act prohibits the intentional or knowing taking, publication or transmission of an image of the private area of a person without his/her consent in circumstances that infringe on privacy. Voyeurism is covered by Section 77 of the BNS, which covers a woman being observed or photographed while performing a private act or her image being broadcasted. The constitutional recognition of privacy and dignity in K.S. Puttaswamy (2017) provides further protection to the legal rights.

8. Non-consensual Intimate Images and Revenge Pornography

Non-consensual intimate-image abuse is when an intimate photograph or video is made without the consent of the person in it, or without the person's consent being obtained. Where a former partner shares consensually created intimate content with others as a way to punish, humiliate or control the victim, the expression "revenge pornography" is generally applied. The more general term is better, however, as the motive of the offender may not be revenge, but rather financial gain, or coercion/harassment/exploitation for sexual purposes. Various Sections in the Information Technology Act may be applicable depending on the content and circumstances, such as 66E, 67 and 67A. Section 67 is on obscene material in electronic form and the Section 67A is on material that contains sexually explicit acts or conduct. The BNS Section 77 may come into play when images are shared that are linked to voyeurism and provisions for stalking, intimidation or defamation may apply (Franks, 2014).

In the State of West Bengal vs Animesh Boxi (2018), the intimate images and videos of the victim were posted online without their consent after the relationship had come to an end. The accused was convicted by the trial court under the provisions of relevant sections of the Information Technology Act and the then prevailing penal law. It was a notable case as it

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

acknowledged the exhaustive infringement on privacy, dignity and sexual autonomy arising from the non-consensual dissemination of intimate content online.

9. Sextortion

Sextortion is a type of digital extortion that takes the form of showing intimate content, videos or fabricated sexual content if the victim does not provide money, more intimate content, or some other benefit. The offender can obtain the material through hacking, recording an online video call, faking a relationship with the victim and getting them to share material. This offence incorporates aspects of sexual exploitation, blackmail, invasion of privacy and financial extortion. Sextortion can be subjected to the provisions of Sections 66C, 66D, 66E, 67 and 67A of the Information Technology Act based on the facts. Part of the BNS relating to extortion, criminal intimidation, stalking and voyeurism might also be applicable. Where the victim is a child, the provisions of section 67B of the Information Technology Act and POCSO Act, 2012, can be invoked. An earlier consent to share an image is not consent to later be used or released (Powell, 2018).

10. Doxxing

Doxxing is the practice of gathering and publishing personal or identifying information regarding another person, including their home address, telephone number, place of work, finances or information about other family members, without proper authorization. Typically used to threaten, harass, or expose the victim to physical and/or digital abuse. Doxxing can be particularly threatening when paired with threats and/or stalking or coordinated online abuse. As of now, indian law does not specifically identify every act as a crime under any one provision, but there may be several laws that are each applicable. It may be possible to face Sections 43 and 66 of the Information Technology Act for unauthorised access and extraction of information. Threatening to publish or to cause alarm with the information disclosed may lead to Section 351 of the BNS being called into action. If a regulated entity improperly processes or discloses digital personal data without lawful justification, the provisions of the Digital Personal Data Protection Act, 2023 also may apply, depending on its scope, commencement and exceptions.

IV. CYBERCRIMES AGAINST PROPERTY & STATE

Two points focus on offences against property and financial systems and critical State infrastructure. Hacking, unauthorised access, denial-of-service attacks and ransomware are covered by the same Sections 43 and 66 that already penalise hacking and unauthorised access and denial-of-service attacks. Phishing, vishing, SIM-swap fraud and unauthorised fund transfers are dealt with under Section 66C and 66D and RBI's customer liability directions and six-hour incident-reporting time imposed on CERT-In under Section 70B.

Cyber Terrorism and Critical Infrastructure Section 66F of IPC criminalise cyber terrorism act which threatens the unity, integrity and security of India and which causes denial of access or introduction of harmful contaminants for which life imprisonment is prescribed. The introduction of Section 70 protects designated systems (known as “protected systems”) and the Prevention of Money Laundering Act, 2002, as amended, provides for virtual-digital-asset misuse.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

V. EMERGING LEGAL CHALLENGES

The remaining two points cover technological advances that surpass the current legislation.

AI and Algorithmic Accountability Deepfakes present issues under Sections 66C, 66D and 66E of the IT Act, as well as defamation law, but India does not have a specific legislation to define and criminalise synthetic media – MeitY will rely on advisories and proposed labelling rules. The right to explanation in the DPDP Act does not cover algorithmic decision-making in credit scoring, moderation and policing.

Permissive transfer regime in DPDP Act is concurrent with sectoral localization requirements (e.g., RBI's payment data localization direction) leading to compliance uncertainty. Cross border cybercrime investigation is still being impeded by cloud storage abroad, slow Mutual Legal Assistance Treaties and India's non-signature of Budapest Convention.

VI. LANDMARK CASE LAWS

The above statutory provisions have been significantly moulded, developed and at times restricted by judicial interpretation. This Part looks at some significant cases under each of five heads.

A. Privacy and Free Speech

The historic judgement which laid the foundation of India's data protection jurisprudence is Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, handed down by a nine-judge bench of the Supreme Court of India. The Court had set aside the previous precedent which had ruled that privacy was not a fundamental right and said that the right to privacy was embedded in the right to life and the right to personal liberty guaranteed under Article 21 of the Constitution of India and it included the informational privacy, which is the right of an individual to control the dissemination of personal information. The judgment explicitly acknowledged any action by any State infringing upon privacy must be found to be "legitimate" and "proportional" to the aims of the state and must be "legal", a standard later referenced in the cases related to Aadhaar, facial recognition and surveillance.

In Shreya Singhal v. Union of India, (2015) 5 SCC 1, the Court ruled on the constitutionality of Section 66A of the IT Act, which criminalises sending information which is "grossly offensive," "menacing" or "causes annoyance" through a computer resource. The Supreme Court unanimously declared Section 66A to be unconstitutional for being open-ended enough to have a chilling effect on free speech and not being reasonably covered by Article 19(2). While the judgment is the most influential to date on the boundaries of State power to criminalise online expression, there have been subsequent reports of the continued, unlawful use of the struck-down provision by police in some jurisdictions, leading to further judicial intervention (Matthan, 2018).

B. Data Protection Enforcement

Television to Electronic Surveillance, (1997) 1 SCC 301, an earlier decision, which predates the current digital age, but is relevant here, held that the use of a telephone tap by the police was a serious infringement of privacy and identified procedural safeguards for interception which were later adopted, virtually by way of analogy, to electronic surveillance by the police,

under Sections 69 and 69A of the IT Act, 1985. In 2016–17, the Delhi High Court ruled in Karmanya Singh Sareen against Union of India, which was about WhatsApp's update to its privacy policy that allowed it to share user data with its parent company Facebook (now Meta). In addition to the notification to non-opting users - a directive now broadly accepted by courts worldwide - the High Court ruled that the information of those who already deleted their accounts before the policy took effect cannot be shared, highlighting the early engagement of the court with data sharing practices on platforms without a specific data protection statute. The competition law enforcement in India, as highlighted in the case of WhatsApp's 2021 privacy policy update alleging misuse of dominant position by imposing coercive data-sharing provisions, are another example of how competition law and data protection law enforcement in India will intersect once the DPDP Act is fully operational (Bhatia, 2016).

C. Cybercrimes Against Individuals

The important case of State of Tamil Nadu v. Suhas Katti, 2004, is considered as one of the early cases of cybercrime convictions in India which were handled by the Additional Chief Metropolitan Magistrate Court in Chennai. This case stands out for the speedy conviction of the accused within approximately seven months of filing charges in the case, for publishing obscene and defamatory messages regarding the complainant on an online forum under Sections 469 and 509 of the old Indian Penal Code and Section 67 of the IT Act and for laying down early precedence regarding the admissibility of electronic messages as evidence.

Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427 is a case where an obscene video was sold on the auction site Baazee.com. In an early and precedent-setting discussion with intermediary and officer liability, the Delhi High Court quashed the criminal proceedings against the individual director while allowing the criminal proceedings against the company to proceed, in the context of content uploaded by a third-party user.

The same is reiterated in Sharat Babu Digumarti v. State (NCT of Delhi) (2017) 2 SCC 18 where the Court had held that in the area of electronic publication, the IT Act is a special Act that displaces the general provisions of Indian Penal Code for obscenity and therefore a person could not be prosecuted under both the Act and IPC for the same act of obscenity.

D. Cyber Fraud & Electronic Evidence

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, is the supreme court of India's most important decision pertaining to admissibility of electronic evidence in court. The Supreme Court has ruled that secondary electronic evidence, like CDs and pen drives or call data records, can be admitted only with a certificate under Section 65B (4) of the erstwhile Indian Evidence Act (now under the Bharatiya Sakshya Adhiniyam, 2023) which was not permitted earlier as the same could be proved only by oral evidence. The three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, held that the requirement of a certificate was mandatory but allowed it to be produced thereafter when the original document itself was produced and the certifying authority was not available to attend the Court, weighing evidentiary rigour against the difficulties it often posed to courts in the prosecution of cybercrime and financial fraud. (Lal, 2018).

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

In Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485, the court ruled that an electronic document recorded on a compact disc (CD) is a 'document' and provided guidance on the procedure to be followed for evidence to be admitted during the trial of a case involving electronic documentation of such evidence, which has become an integral evidentiary category in cyber and financial fraud in general and in online banking fraud, ATM skimming and unauthorised electronic fund transfers which are routinely prosecuted under Sections 66C and 66D of the IT Act.

E. Technology & Jurisdiction

In Google India Pvt. Ltd. v. Visaka Industries, (2020) 4 SCC 162, the Supreme Court reviewed the liability of an intermediary for defamatory content on its platform before the amendment to the IT Act in 2008 and held that Section 79's concept of safe-harbour protection, as it existed at the relevant time, was not available for defamatory content that existed prior to the amendment and the concept of due diligence, leaving the scope of intermediary immunity unchanged and continuing to apply in cases involving platform liability disputes between cross-border technology companies and intermediaries operating in India.

The recent court challenges by digital news publishers to information disclosure norms brought by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and by WhatsApp to the requirement for the identification of the first originator under Rule 4(2) of the Rules are illustrative examples of judicial negotiations between the State regulatory concerns, the end to end encryption architecture of the platforms and the privacy rights recognised in Puttaswamy. The proceedings continue to hold relevance because of the scope of traceability obligations that they may give rise to and, consequently, the extent to which Indian regulation is to reach out to messaging and cloud infrastructure that is operated around the globe (Gupta, 2023).

CONCLUSION

The legal landscape in India regarding cybercrime and data protection has come a long way in the last 25 years from the old and narrow Information Technology Act, 2000, to the much-broadened amendment in 2008, then to the constitutionalisation of the right to privacy in the case of Puttaswamy and, most recently, to the passage of the Digital Personal Data Protection Act, 2023. This is a more general (and mostly positive) move from a technology facilitating statute with penal elements to a more thoughtful approach to the rights regulation of personal data along with a dedicated cybercrime regime.

Despite this, this paper's analysis, which takes place through five substantive headings and five lines of judicial authority, shows that there is a structural gap between the two. The first is that the capacity to enforce the laws of the land through investigative expertise, digital forensic infrastructure and inter-State and international coordination is still not as sophisticated and cross-border as the nature of contemporary cybercrime, especially ransomware, financial fraud syndicates and cyber-terrorism. Second, the wide exemptions provided to the State under the DPDP Act, the very limited independence and capacity of the Data Protection Board of India and the lack of a proper automated-decision making or algorithmic accountability mechanism leave unintended gaps between the constitutional guarantee of Puttaswamy and its statutory

implementation. Third, the existing provisions of the IT Act and also the DPDP Act do not directly cover emerging technologies such as generative AI and deepfakes, biometric and facial recognition systems and cloud-based cross-border data storage, thus leaving individuals vulnerable to harms that the IT Act and DPDP Act drafters did not foresee. Fourth, procedural delays in electronic evidence remain as a cause of litigation and delay, especially for victims of financial and identity-based cybercrime, who may not have the resources to defend long and drawn-out court cases.

To address these challenges, a solution is required to be multi-fold: timely notification and implementation of the Digital Personal Data Protection Rules and providing adequate resources to the Data Protection Board of India; consistency and convergence of sectoral data-localisation requirements with the cross-border transfer provisions in the DPDP Act to mitigate compliance uncertainty; dedicated focus on legislative or regulatory measures pertaining to AI generated synthetic media and algorithmic accountability; robust cyber-forensic and investigation resources at the State level with the Indian Cyber Crime Coordination Centre and concerted treaty-based cooperation between countries for cross-border evidence sharing and cybercrime investigation, with reconsideration of India's participation in instruments like the Budapest Convention. It is only through constant engagement of legislation, institutions and judiciary that India's cyber law framework can evolve from a reactive ‘when it happens’ model to a rights-protecting and future-oriented framework that will ensure protection of digital innovation and individual liberty.

REFERENCES

A. Statutes and Legislative Materials

1. The Information Technology Act, 2000 (Act No. 21 of 2000).
2. The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).
3. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
4. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
6. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
7. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
8. The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
9. The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012).
10. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act No. 18 of 2016).
11. Ministry of Electronics and Information Technology, Government of India, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

B. Case Law

12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

13. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
14. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
15. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Addl. CMM, Egmore, Chennai).
16. Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427.
17. Sharat Babu Digumarti v. State (NCT of Delhi), (2017) 2 SCC 18.
18. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
19. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
20. Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485.
21. Google India Pvt. Ltd. v. Visaka Industries, (2020) 4 SCC 162.

C. Books, Reports and Journal Articles

22. Pavan Duggal, Cyber Law: The Indian Perspective (Universal Law Publishing, 5th edn., 2021).
23. Vakul Sharma, Information Technology Law and Practice: Cyber Laws and Laws Relating to E-Commerce (Universal Law Publishing, 6th edn., 2021).
24. Apar Gupta, Commentary on Information Technology Act (LexisNexis, 3rd edn., 2016).
25. Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018).