Page: 1056-1087 *URL: www.lijdlr.com*

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.194

ANALYZING THE LINK BETWEEN DIGITAL PROFILE AND REAL-WORLD OFFENCES

Harsh Khatri[1]

I. ABSTRACT

The proliferation of digital technologies has sparked a sociotechnical revolution that has fundamentally reorganized the structures of human identity and interpersonal relationships. While digital profiles were first introduced as safe havens of social networking information, their use has been extended to become highly detailed "datafied identities," including personal details such as biometric characteristics, geo-location information, profession, and behavior. They are therefore extremely profitable targets of crime because of the amount of personal data that they provide. This research paper provides a thorough socio-legal, criminological, and comparative investigation of the connection between the abuse of digital identity and actual crime. The environmental criminology theories of Cyber-Routine Activity Theory (CRAT) and Space Transition Theory are applied to explain how structural anonymity and geographical dissociation create opportunities for tangible damage, from economic crime to cyber-stalking and violent attacks. The research investigates the change in the legislative architecture in India from the colonial-era criminal code to the Bharatiya Nyaya Sanhita (BNS) 2023; evidence laws outlined in the Bharatiya Sakshya Adhiniyam (BSA) 2023; and data governance regulations under the Digital Personal Data Protection (DPDP) Act 2023 and its implementation rules in 2025. In addition, the paper discusses the rising challenge posed by generative artificial intelligence (GenAI) and deep-fakes, analyzing the effectiveness of the amendments made to the Information Technology Rules in 2025 and 2026 concerning the regulation of "Synthetically Generated Information" (SGI). Using a comparative jurisprudence framework considering the European Union, the United States, and the United Kingdom, this paper examines important structural weaknesses in current enforcement practices, discusses the development of personality rights, and proposes a preventive approach to legal intervention using technology.

[1] B.A.LL.B. (H), 10th Semester, Student at Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur (India). Email: harshkhatri2311@gmail.com

 (ISSN: 2583-7753)

II. KEYWORDS

Digital Profile, Cyber-Routine Activity Theory (CRAT), DPDP Act 2023, Deep-fake, Digital Doppelgänger.

III. INTRODUCTION AND RESEARCH PROBLEM

Modern day human interactions are deeply embedded within the context of digital spaces. The structure of cyberspace is such that personal data keeps getting aggregated continuously and often involuntarily. In this way, an aggregate picture of the individual emerges which acts as an intermediary for the person's physical presence. Legal experts have acknowledged the fact, based on research related to informational privacy, that the distinction made between the natural and informational self is artificial since there exists a significant blurring of the boundaries between the two selves. The term "datafied identity" refers to this process of data collection which happens in isolation from the individual, and independently within the digital world.

The principal research problem addressed in this paper concerns the growing inadequacy of conventional legal and criminological frameworks in responding to cyber-enabled offences facilitated through digital identities and Generative Artificial Intelligence (GenAI). The paper specifically examines whether the existing Indian legal framework is sufficiently equipped to address the evolving nexus between digital profiling, cybercrime, and offline criminal consequences.

In spite of the fact that this form of digital profiling improves international interconnectedness, streamlines administrative processes, and optimizes business practices, it makes people increasingly vulnerable to previously unknown and extremely imbalanced dangers. The gap between virtual images and physical manifestations has been eroded significantly, permitting criminals to use digital personas as weapons to instigate horrific crimes in the physical world. The progression of cybercrime has followed an unmistakably ominous trend: whereas once simple computer-related crimes like basic network breaches and mass-malware attacks were predominant, they have now been completely outstripped by advanced

sociotechnological crimes that manipulate psychology and identity information. Digital identities have become the new currency that drives an extensive underground digital economy. Digital personas are consistently exploited by cybercriminals to conduct extremely targeted phishing attacks, perpetrate financially motivated crimes, commit cyber-stalking offenses, and deploy deep-fakes for extortion purposes.[2] The repercussions of sociotechnological crimes can be devastating not only on the digital plane but also financially, psychologically, and even physically.[3]

However, with the swift development of GenAI, the paradigm of threats has been entirely reformed, and the challenges that arose exceed the capabilities of conventional laws.[4] Democratization and popularization of advanced technologies created conditions under which the bar for engaging in cybercrime became extremely low, allowing cyber criminals to produce synthetic media at scale. Deep fakes, AI identity fraud, and AI voice cloning created a severe epistemological crisis and shook public confidence in digital content, making authentication of digital identity extremely difficult. Ultimately, this issue led to the appearance of what is now referred to as the Digital Doppelganger—an autonomous existence of an individual's synthesized image within the virtual world that can be used against them on a perpetual basis.[5] In such a manner, one can conclude that the analysis and regulation of the relation between digital profile and criminal conduct have become crucial issues facing contemporary legal practices and constitutional rights.

A. Research Objective

The main objectives of this research are as follows:

1. To analyze the relationship between digital profiles and actual crimes.
2. To evaluate the efficacy of Indian cyber laws, including the 'IT Act' of 2000 and the 'Digital Personal Data Protection Act' of 2023.

[2] BioCatch, "Report: Digital Banking Fraud Trends in India" (2025).
[3] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024); Office for National Statistics, "Crime in England and Wales" (2024).
[4] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).
[5] Alliance Center for Intellectual Property Rights, "The Digital Doppelgänger" (2025); Kamya Buch v. JIX5A39 (2025); Sadhguru Jagadish Vasudev v. Igor Isakov, CS (COMM) 578/2025.

3. To evaluate the comparative legal provisions in the United States, United Kingdom, and the European Union.
4. To suggest legal, regulatory, and policy reforms to prevent the abuse of digital identities.

B. Research Questions

In the present study, the following issues will be investigated:

1. To what extent does the availability of personal information contained in digital profiles contribute to the commission of cyber-enabled and real-world offenses, and whether the existing legal regime in India provides an adequate response to these concerns?
2. Are the current provisions under the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 enough to control the abuse of digital identity or personal data?
3. What legal and technological challenges do law enforcement agencies face in their investigations and prosecution of crimes related to digital profiles?
4. How have the United States, the United Kingdom, and the European Union tackled the issue of digital identity abuse and personal data protection?
5. What legal reforms and policy interventions could be initiated in the country to improve the protection of people from the consequences of digital profiles and personal information misuse?

C. Research Methodology

In order to conduct an accurate and comprehensive study of the relationship between digital identities and offline crimes, this paper will follow a multidimensional research methodology characterized by its doctrinal and analytical features. In this sense, it should be noted that the current work is predominantly qualitative and does not involve the acquisition of primary empirical data; instead, it relies heavily on doctrinal analysis based on existing statutory, case law, and criminological material.

In terms of the research methodology adopted, it can be emphasized that the use of the doctrinal method allows interpreting primary legal material, which includes the *Information Technology Act 2000, Bharatiya Nyaya Sanhita (BNS) 2023, Bharatiya Sakshya*

Adhiniyam (BSA) 2023, and Digital Personal Data Protection (DPDP) Act 2023. Furthermore, an analytical method is also applied to assess how effectively these laws cope with new risks related to artificial intelligence technologies, deep-fake technology, and identity fraud. With regard to the comparative aspect, it involves making direct comparisons between Indian legislative framework on data protection and other established laws, including *GDPR of the European Union*, sectoral privacy frameworks of the USA, and UK Data Protection Act 2018.[6]

IV. CRIMINOLOGICAL FRAMEWORKS OF CYBER-ENABLED OFFENDING

A full understanding of the process by which the exploitation of online profiles can become real damage requires the application of environmental criminological theories, which have been modified to suit the digital era. The conventional theory that views cybercrimes simply as crimes committed using computer technology is inherently flawed since they should instead be regarded as sociotechnical, taking into account human behavioral psychology within the digital space and its legal confines.

A. Cyber-Routine Activity Theory (CRAT)

Routine Activity Theory (RAT), first proposed by criminologists Lawrence Cohen and Marcus Felson back in 1979, suggests that predatorial criminal activity is not exclusively dependent on social disparities that exist in society or a criminal mindset, but rather depends on the coming together of three specific environmental conditions in both time and space: a motivated offender, a vulnerable victim, and the complete absence of any form of competent guardian.[7] Although RAT is primarily focused on describing contact crimes, like assault or burglary, the theoretical structure of CRAT has successfully been applied to the digital realm, including identity theft and cyber bullying.

[6] The Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, "Digital Personal Data Protection Rules" (Government of India, 2025).

[7] Lawrence E. Cohen & Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach", 44(4) *American Sociological Review* 588 (1979); A. Dours & A. Eaton, "Using Routine Activity Theory to Predict Technology-Facilitated Violence", *Journal of Research in Crime and Delinquency* (2025); T.J. Holt & A.M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization", 26 *Deviant Behavior* 428 (2009).

From a CRAT perspective, the condition for spatial and temporal convergence is completely deconstructed. The systematics of cyberspace work asynchronously, without any regard to the jurisdictions that govern it, which allows for the possibility of a crime being committed by the offender and the victim not necessarily using the Internet at the same time and without being physically close to each other. The user's electronic profile – with all the information related to him/her – becomes the suitable target, one that is "always there".[8] The user creates his/her suitability for becoming a victim through the normal activities of using the Internet, such as electronic banking, e-commerce and voluntary provision of personal information on social networking sites. Research using a binary logistic regression analysis on large scale crime surveys shows that there exists a clear relationship between the frequent use of the Internet for such actions as banking, social messaging and downloading and an increased probability of falling victim to identity theft – 50% greater than that of infrequent users.

Moreover, the notion of "capable guardianship" changes significantly and is generally greatly reduced within the digital space. While in the real world, the very presence of other people, whether they be passers-by, neighbors, or even police officers, functions as a highly effective deterrent because the perpetrator's chances of being caught are multiplied. In contrast, the digital world offers no such thing as physical visibility. The anonymous nature of the internet, which can be amplified through encryption, Virtual Private Networks (VPNs), and pseudonyms, makes it impossible to use the deterrent aspect of other people's presence in the digital world. Instead, capable guardianship in the online sphere relies solely on computerized protection mechanisms such as multi-factor authentication and algorithms. Human guardianship can also be considered since the users themselves act as guardians when they know how to navigate the digital world safely.

B. Space Transition Theory

[8] A. Dours and A. Eaton, "Using Routine Activity Theory to Predict Technology-Facilitated Violence," Journal of Research in Crime and Delinquency (2025); T.J. Holt and A.M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," 26 Deviant Behavior 428 (2009).

Whereas CRAT focuses on the opportunities in the situation and the conditions that favor cyber-crime, on the other hand, Space Transition Theory, as articulated by criminologist K. Jaishankar, goes further into understanding the behavior of the offenders as they traverse between the physical space and cyberspace.[9] The theory states that there are predictable fluctuations in the human behavior that occur when one is moving from the physical space to the cyberspace, which are defined through seven basic postulates:

1. The first postulate of this theory states that individuals who have repressed criminal/deviant traits in physical space due to factors such as their social status, professional standing, or fear of facing any criminal consequences, are bound to indulge in those same actions in cyberspace.
2. The second, and maybe the most important, postulate revolves around the concept of dissociative anonymity and identity flexibility. The structure of cyberspace enables offenders to totally dissociate their true identity in the physical world from any activity that takes place online. This psychological dissociation causes a dramatic drop in empathy and the fear of punishment, thereby encouraging the exploitation of online identity, cyber-bullying, and perpetration of heinous crimes not normally undertaken in the face-to-face physical world.
3. The third postulate considers the importation and exportation of criminal activity. Methods developed and honed through cybercrime are often exported to carry out physical crimes. On the other hand, physical crime networks such as human traffickers and drug cartels have increasingly begun importing criminal activity into the virtual world using digital identity theft and crypto-laundering of money raised for their illicit physical activity.
4. The fourth postulate explains the concept of dynamic spatio-temporal escape. The transient and transnational characteristic of cyberspace makes it possible for offenders to execute highly damaging and intermittent attacks

[9] K. Jaishankar, "Space Transition Theory of Cyber Crimes" in F. Schmalleger and M. Pittaro (eds.), Crimes of the Internet 283 (Prentice Hall, 2008).

from locations far away before retreating into the shadows, thus making it highly improbable that they will be intercepted by physical law enforcement agencies.

5. Postulate five considers the unification of strangers and associates. In cyberspace, there is no geographical divide that stops the smooth integration of people with similar ideologies or motives who share technological capabilities and stolen information to carry out crimes against online targets. This can be seen in the development of global cybercriminals syndicates known as "Cybercrime-as-a-Service."
6. Postulates six and seven consider the role of macro-societal factors. People coming from extremely oppressive physical societies might have a high tendency to indulge in cyber-deviance as an act of defiance, self-preservation, or to exploit richer societies.[10] Additionally, great differences in the morality of a physical society and those of subcultures in cyberspace create justifications for such deviant acts, allowing people to systematically misuse online identities without a second thought.

From the holistic perspective provided by Space Transition Theory, the manipulation of digital identities is recognized not only as a set of technological attacks but as a sociological process characterized by the sense of invulnerability, anonymity, and geographical dissociation offered by cyberspace.

V. THE EMPIRICAL REALITY: ESCALATION FROM DIGITAL EXPLOITATION TO TANGIBLE HARM

As evidenced in the empirical manifestation of theoretical risks highlighted by both CRAT and Space Transition Theory, there has been an alarming rise of cyber-physical offenses on a global scale. The non-consensual exploitation of personal digital data is often used as a prerequisite step toward offline victimization, thereby making it clear why it would be erroneous to think of digital privacy simply in theoretical terms.

[10] K. Jaishankar, "Space Transition Theory of Cyber Crimes" in F. Schmalleger and M. Pittaro (eds.), Crimes of the Internet 283 (Prentice Hall, 2008).

A. The Surge in Cyber-stalking and the Transition to Physical Violence

The act of cyber-stalking provides one of the clearest examples of the link between digital data exploitation and physical risk. With easy access to publicly available geo-tagged pictures, check-ins to places and work, and social networks through which individuals can find information regarding personal life and relationships, it is quite easy for the wrongdoers to digitally stalk someone and subsequently harass and physically assault them.[11]

Statistical evidence in various regions clearly shows how serious and extensive this shift really is. In the UK, careful longitudinal studies on the Crime Survey of England and Wales (CSEW) showed that the number of instances of cyber-stalking is greatly outnumbered by cases of traditional physical stalking. Over the course of eight years, from 2012 to 2020, the percentage of people who suffered from cyber-stalking victimization grew from 1.0% to 1.7%, mostly targeting females and disadvantaged social groups.[12] The full extent of this issue can be illustrated by the data collected by the police in England and Wales, according to which more than 135,000 criminal acts of stalking were registered in one recent year, which is a nearly fiftyfold increase compared to the previous decade. This unprecedented growth is directly attributed to the fact that stalkers use digital technologies and monitoring capabilities to spy on their victims. Meanwhile, despite the huge amount of objective evidence, there is a problem with diagnostics, since many victims are unaware that digital abuse constitutes an act of stalking and a crime.

Data collected by the National Crime Records Bureau (NCRB) reveals the same situation of another grave threat in India. The high rate of digitization in India, with an internet connection for over 86 percent of Indian families, makes the attack surface wider. There is a sharp increase in cybersecurity threats across India, from 10.29 lakh cases registered in 2022 to 22.68 lakh cases in 2024. Digital profiling and gender-based crimes constitute an extremely concerning threat to Indian women. According to

[11] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024); Office for National Statistics, "Crime in England and Wales" (2024).
[12] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024); Office for National Statistics, "Crime in England and Wales" (2024).

officially verified data published by the National Crime Records Bureau (NCRB), there were 28,903 registered cybercrimes against women in India in 2023.[13] These offences included cyber-stalking, online harassment, identity theft, impersonation, and sexually exploitative digital conduct. Subsequent projections and industry estimates published by cyber-security and fraud-monitoring organizations indicated a substantial rise in cyber-enabled offences against women by 2025, particularly in areas such as cyber-stalking, sextortion, profile impersonation, and AI-enabled identity fraud.[14] However, since official NCRB statistics for the year 2025 have not yet been formally released, these later figures should be understood as analytical estimates and industry projections rather than verified governmental crime statistics. Geographically, the above crimes have been found to occur primarily in technologically rich cities, with Karnataka, Telangana, Uttar Pradesh, and Maharashtra being noted persistent hubs for cybercrime cases. The real damage caused can be seen from various case studies, including an outstanding example in the year 2025 from Mumbai where a famous actress underwent two years of cyber-stalking through the means of using multiple SIM cards by the perpetrator to stalk her online presence until she finally had to take the matter into consideration via invoking laws from the BNS and IT Act.[15] The psychological effects of the stalking crime have now developed with time and advancements in technology; for instance, various case studies have involved VR environments, such as the Meta Company's game Horizon Worlds, which shows that cyber sexual assaults and stalking have a significant psychological impact comparable to actual physical stalking.[16]

B. Economic Devastation, Fraud, and the Weaponization of AI

However, apart from the personal security concerns mentioned above, it can be argued that the abuse of the concept of digital profile is creating immense macroeconomic disturbances. Hackers use the information obtained from the data

[13] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024): Office for National Statistics, "Crime in England and Wales" (2024).
[14] Entrust, *Identity Fraud Report* (2025); BioCatch, *Digital Banking Fraud Trends in India* (2025).
[15] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024); Office for National Statistics, "Crime in England and Wales" (2024).
[16] "The Corporeality Crisis: How Immersive Technology is Outpacing India's Sexual Assault Laws," Jurist (2026).

breaches, social media data scraping, and dark web markets to fabricate believable synthetic online personas, which are then used for financial crimes, corporate spying, and identity theft on a mass scale. With Generative AI in place, the issue has become an industrial-scale phenomenon.

A number of metrics prove the evolution of the problem of synthetic content creation and cybercrime. While the baseline number of deep-fake attacks was relatively low in 2023-2024, by 2025-2026, they have increased to one attack per five minutes. The rate of forgery of digital documents rose by 244% and caused significant degradation of the existing procedures for KYC and identity verification. Moreover, the false chatbot ratio increased from 18% to 35%.[17] The number of AI-powered websites producing fabricated news has grown from around 600 to over 2,089, thus marking an explosion of fake stories and misinformation. Simultaneously, the number of cybercrimes against women in India has risen exponentially from 40,066 cases in 2023 to 76,657 in 2025. By 2025, cybercrime, comprising of frauds, theft of personal information, and ransomware attacks, is expected to cost $10.5 trillion annually according to industry experts.

The cost for India alone is even more exorbitant and organizationally complex. "Digital arrest scams" constitute an advanced form of psychological manipulation wherein criminals disguise themselves as police or customs officials through forged digital identities, arrest warrants, and voice cloning with the aid of artificial intelligence. According to industry analysis, these digital scams alone led to financial losses worth ₹2,000 crore (around $240 million) in India in a single year.[18] Illustrative of the applicability of the concept of Transnational Escape Postulate proposed by the Space Transition Theory, intelligence suggests that over 40% of such digital scams targeting Indians are carried out by transnational cyber syndicates from countries like Myanmar, Cambodia, and Laos.[19]

[17] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).
[18] BioCatch, "Report: Digital Banking Fraud Trends in India" (2025).
[19] BioCatch, "Report: Digital Banking Fraud Trends in India" (2025).

These developments pose significant socio-security threats that could destabilize nations. The idea of "cognitive warfare" has become a tangible reality. State and non-state actors have resorted to using "Smart Propaganda Systems," where millions of AI personas, designed with intricate psychological profiling, imitate actual citizens who are highly involved and engaged. This approach is illustrated by the GoLaxy exposé that took place in September 2025. It infiltrates digital environments with synthetic stories, thus manufacturing artificial public consent, and entirely undermines confidence in validated digital personas.

The devastating consequences of this use of AI technology were vividly highlighted following the Pahalgam Terror Attack of April 2025. Following the unfortunate incident, fake news proliferated social media platforms such as Telegram and X. Actors maliciously employed Generative Adversarial Networks (GANs) to create altered video footage of the attack, distributed false military warnings, and even used deep-fake lip-syncing technology to simulate the conversation between the Defense Department's officials about non-existent "false flag" attacks. The age-old principle that "seeing is believing" in the realm of evidence has completely broken down in the face of generative AI. This principle has been supplanted by the "liar's dividend," a frightening sociological reality that enables bad actors and persons of public interest to deny damning audio and video recordings on the pretext that they were fabricated deep fakes.

C. The Emergence of the "Digital Doppelgänger"

The ultimate outcome of the abuse of digital identity, data scraping, and generative AI is the development of the "Digital Doppelgänger." The digital doppelgänger is the persistent, erroneous, and often artificially created representation of one's identity that lives independently and endlessly in the digital world. In contrast to the organic identity that matures, ages, and has the ability to forget or even get forgotten by society, the digital doppelgänger is entirely unaffected by the effects of aging.[20] It is made up of a collage of non-consensual deep-fake videos, personal information

[20] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).

bought from data brokers, social media content taken out of context, and archived digital information, including old and overturned court decisions.

The digital doppelgänger can continually be turned into a tool for harming the individual, thereby creating an all-pervasive and inescapable digital space where the victim will always be stalked, financially harmed, or socially isolated through a digital doppelgänger created out of them.[21] For example, those who are found not guilty of any crime may lose out on all career opportunities because their digital doppelganger can never leave behind the first impression made by their arrest record indexed in search engines. Moreover, the ease of generating fake and extremely sexual images of people through an AI such as Grok that can generate sexual images based on the input of a user's profile picture demonstrates just how easy it is to abuse the digital doppelganger to cause harm to someone's reputation.

VI. THE INDIAN LEGISLATIVE METAMORPHOSIS: ADAPTING TO THE DIGITAL THREAT

Conscious of the inherent inadequacies in its colonial legal framework to deal with the intricacies associated with sociotechnical crimes and digital identity theft, the government of India embarked on an unprecedented effort at overhauling its laws relating to criminal law, evidence, and data protection. The simultaneous enforcement of the Bharatiya Nyaya Sanhita (BNS) 2023, the Bharatiya Sakshya Adhiniyam (BSA) 2023, and the sweeping regulatory regime of the Digital Personal Data Protection (DPDP) Act 2023 indicates a long-overdue move towards modernization of its legal landscape.[22]

A. The Bharatiya Nyaya Sanhita (BNS) 2023: Modernizing the Penal Code

The effective enforcement of the BNS 2023 replaced the outdated Indian Penal Code (IPC) of 1860 from July 1, 2024. As evident from the name itself, the IPC was enacted before the discovery of electricity, leaving alone the Internet, which left the judiciary

[21] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).

[22] The Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, "Digital Personal Data Protection Rules" (Government of India, 2025).

helpless in handling cases of sophisticated cyber-crimes by resorting to an exaggerated interpretation of its provisions pertaining to cheating, forgery, and intimidation. The BNS is an attempt at overcoming these limitations by incorporating terms that are flexible enough to include criminal acts perpetrated in the digital space. Unlike the IPC, which contains a specific section on 'Cyber Crime', the absence of such a provision in the BNS appears deliberate.[23]

B. Statutory Recognition of Organized Cybercrime

By far, the most crucial doctrinal innovation introduced within the BNS is the statutory introduction of "organized crime" under Section 111, along with its criminalization and imposition of hefty penalties.[24] It is vital to note that Section 111(1) categorically mentions "cyber-crimes" along with other syndicated acts such as human trafficking, extortion, and contract killings when such acts are committed by an individual or a gang in conjunction to gain material or financial advantages either directly or indirectly.

Prior to the advent of the BNS, a multi-faceted and complicated prosecution of any sophisticated cyber syndicate (e.g., digital arrest scams and ransomware gangs) was a herculean feat since one had to piece together a general charge of conspiracy along with specific acts of violating the IT Act, 2000. To solve this structural problem, Section 111 of the BNS takes cognizance of the fact that modern-day digital identity theft is highly organized and corporate in nature. The penalties provided under Section 111 BNS are structured in two types. Where organized crime results in death, the punishment may extend to death penalty or life imprisonment along with a mandatory minimum fine of Rs. 10 lakhs. In all other organized crime cases, including most organized cybercrime prosecutions, the punishment ranges from imprisonment of five years to life imprisonment along with a mandatory minimum fine of Rs. 5 lakhs. Nevertheless, there are several issues regarding potential zones of serious conflict between jurisdictions. For instance, the definition of organized crime by BNS is very similar to definitions used in certain specialized laws dealing with anti-terrorism and

[23] The Bharatiya Nyaya Sanhita, 2023.
[24] The Bharatiya Nyaya Sanhita, 2023.

organized crime, such as the Maharashtra Control of Organized Crime Act (MCOCA) and the Gujarat Control of Terrorism and Organized Crime Act (GCTOCA). It should be noted that the concept of "cyber-crime," which refers to such crimes as identity theft and hacking, is actually defined within the scope of a specialized act dealing with IT-related offenses.[25] Thus, the challenge for the judiciary in this particular case lies in harmonization of provisions concerning organized crime and the definitions and procedures prescribed by the specialized IT Act.

C. Recontextualizing Traditional Offences in Cyberspace

Apart from organized crime, the BNS makes appropriate adaptations to traditional physical crimes, taking into consideration the unique nature of digital profiles and cyberspace:

1. **Fraud and Deceit (Section 318):** In the IPC, charges of online financial fraud were based on provisions relating to deception and cheating in general terms. The BNS updates this provision, guaranteeing that deceit involving the use of electronic communication or the creation of false digital identities—addressing phishing attacks, investment schemes, and impersonation by means of a "deep-fake"—is adequately punished.
2. **Stalking and Harassment (Sections 78, 79, and 356):** Section 78 of the Bharatiya Nyaya Sanhita, 2023 specifically criminalizes the offence of stalking, including repeated monitoring of a woman's online activities, internet usage, or electronic communication. The provision substantially corresponds to Section 354D of the erstwhile Indian Penal Code and recognizes cyber-stalking as a punishable offence within the broader framework of crimes against women.[26] Additionally, Section 79—prohibiting actions meant to offend the modesty of a woman—includes the necessary ambiguity to cover new offenses of creating non-consensual explicit deep-fakes, as well as the harassment of others through avatars in

[25] The Bharatiya Nyaya Sanhita, 2023.
[26] "The Corporeality Crisis: How Immersive Technology is Outpacing India's Sexual Assault Laws," Jurist (2026).

virtual reality environments. Section 356 updates defamation, ensuring that any defamation committed through digital and social media is covered.[27]

3. **Public Misconduct and Misleading Information (Sections 353 and 212):** Section 353 of the Bharatiya Nyaya Sanhita, 2023 specifically criminalizes statements, misinformation, rumors, or electronic content capable of causing public mischief, social unrest, communal disharmony, or panic, thereby making it directly relevant to malicious deep-fake dissemination and synthetic misinformation campaigns.[28] In contrast, Section 212 BNS narrowly addresses the furnishing of false information to a public servant by a person legally obligated to provide truthful information and therefore functions primarily as an obstruction-of-justice provision rather than a general anti-misinformation offence.[29]
4. **Extraterritorial Jurisdiction:** By taking direct cognizance of the "dynamic spatiotemporal escape" aspect of the Space Transition Theory, the BNS explicitly exercises extraterritorial jurisdiction. The BNS empowers prosecution of offences committed beyond the territorial boundaries of India, where such criminal activity is directed against computer systems, infrastructure, and profiles based in India or adversely affecting Indian nationals.

D. The Bharatiya Sakshya Adhiniyam (BSA) 2023: The Evidentiary Revolution

The evolution from IEA 1872 to the BSA 2023 marks a much-needed paradigm shift in the prosecution of computer-related offenses. The BSA grants legal recognition to digital and electronic documents by broadening the meaning of the statutory term "document" under Section 2(1) (d) to encompass all electronic or digital documents.

1. **Parity of Primary v. Secondary Electronic Evidence:** Under the archaic IEA laws, the role of digital evidence would often times be minimized owing to its perceived tendency to tamper and be considered as secondary evidence

[27] The Bharatiya Nyaya Sanhita, 2023.
[28] Bharatiya Nyaya Sanhita, 2023, Section 353.
[29] Bharatiya Nyaya Sanhita, 2023, Section 212.

that required a cumbersome procedure before admission as evidence.[30] The BSA makes a fundamental transformation in this regard. Explanations 5, 6, and 7 attached to Section 57 state that any electronic or digital document emanating from proper custody, video recording both stored and transmitted concurrently, and digital documents that are held in more than one automated storage space (including the temporary file/cache) will be considered as primary evidence unless the authenticity of such evidence is questioned. Besides this, the creation of Section 61 expressly provides that there should be no reason for excluding any electronic or digital document from use as evidence based on its digital nature.

2. **The Section 63 Certification Labyrinth:** While the BSA seeks to provide easier admission of digital evidence, it provides elaborate new procedural protections that pose the threat of complicating criminal proceedings. Section 63 of the BSA replaces controversial Section 65B of the IEA pertaining to the admissibility of electronic records. While Section 63(4) of the BSA maintains the same principle of certification of an electronic record as required under Section 65B of the IEA, it provides for a stringent, standardized two-part certification provided specifically in the BSA's Schedule.[31] These two parts include:
    - **Part A:** To be prepared by the party tendering the electronic record, stating that the record was produced using the computer system under lawful control of that person and that the computer functioned properly while the document was made.
    - **Part B:** Explicitly stated to be prepared by an "Expert."

The abrupt imposition by legislation of the mandatory “Part B” expert certificate has resulted in considerable jurisprudential confusion. The provisions of the BSA contain no mention of the exact qualifications or identity of the “expert” required to certify this portion of the document. There is uncertainty amongst lawyers and judges whether the person should be an officially certified forensic expert as stipulated in

[30] The Bharatiya Sakshya Adhiniyam, 2023.
[31] The Bharatiya Sakshya Adhiniyam, 2023.

Section 39 of the BSA, or just someone who possesses functional competency in computers and is working on behalf of the party submitting evidence.

The issue of jurisdictional ambiguity has once again been stirred up by this provision, which concerns electronic evidence. In the landmark decisions of the Supreme Court of India in Anvar P.V. v P.K. Basheer (2014) and Arjun Panditrao Khotkar (2020), it was held that the certification of documents under the old Section 65B of the Evidence Act was an absolute sine qua non for the admission of electronic evidence. On the contrary, there are other decisions made in the High Courts, such as Alukas Jewelerry v. Anil (2025), which contend that failure of certification constitutes only a "curable procedural deficiency" concerning the "mode of proof" and not one that renders the document inherently inadmissible.

The rigid requirement of dual certification under the BSA, especially as applied to an "expert," may lead to extreme procedural problems. The defense counsel will inevitably make use of this technicality if the requirement is strictly enforced in terms of a certified forensic expert under Part B, leading to the possible catastrophic disqualification of crucial pieces of evidence, such as WhatsApp messages, CCTV videos, or server logs, in cases dealing with identity theft, cyber-stalking, and fraud.[32]

E. Data Governance: The DPDP Act 2023 and the 2025 Rules

Whereas the BNS and BSA are geared towards the penalization and adjudication of crimes after the fact, the inherent foundational weakness of digital identities requires the implementation of an affirmative regulatory framework. This is achieved via the DPDP Act, which represents India's first holistic, cross-cutting legislation on data protection and security. Moving beyond the limitations of the penal paradigm, the DPDP Act seeks to drastically restrict the collection, use, and negligent disclosure of personal data, which forms the underlying basis for any kind of digital fraud and deep faking.[33]

Accordingly, the DPDP Act creates a regulation dichotomy between "Data Fiduciaries" (organizations or persons who define the purposes and methods for the

[32] The Bharatiya Sakshya Adhiniyam, 2023.

[33] The Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, "Digital Personal Data Protection Rules" (Government of India, 2025).

processing of data) and "Data Principals" (individuals associated with the data collected). The implementation of the DPDP Act received an important boost with the official notification of the DPDP Rules on November 14, 2025, by the Ministry of Electronics & IT (MeitY). The DPDP Rules of 2025 implement the principles outlined in the DPDP Act by laying out a phase-wise 18-month implementation timeline.

The enforcement architecture governing cybercrime and digital evidence in India continues to suffer from several structural bottlenecks, including technological illiteracy among investigating agencies, ambiguities surrounding expert certification under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, persistent jurisdictional complications in transnational cyber offences, and emerging institutional concerns surrounding the operational effectiveness of the Data Protection Board of India (DPBI) under the Digital Personal Data Protection framework.

A further structural bottleneck arises from the still-evolving enforcement capacity of the Data Protection Board of India (DPBI), constituted under the DPDP Rules, 2025. Although the Board has been envisaged as the principal adjudicatory authority for personal data protection violations, its institutional effectiveness remains largely untested in practice. Concerns have also been raised regarding the extent of its operational independence owing to the Central Government's significant role in appointments and administrative oversight. Additionally, questions persist as to whether the predominantly civil and financial penalty-based enforcement mechanism under the DPDP Act will be sufficient to deter large-scale data fiduciary negligence, particularly in cases involving digital profiling abuse, algorithmic manipulation, and cyber-enabled harms with serious offline consequences.

Important regulatory measures which have been put in place through the DPDP framework are:

1. **Stricter Consent and Purpose Limitations:** It is strictly forbidden for any Data Fiduciary to process digital data unless such processing is done only after taking explicit and free consent of the concerned Data Principal. Such a requirement also entails affirmative action taken by the Data Principle in this regard. Detailed notices should be given prior to obtaining such consent.

2. **Data Breach Notification Requirement:** The guidelines provide clear and strict mechanisms for responding to data breaches. In case of a breach involving personal data, Data Fiduciaries will be required to notify affected Data Principals without delay upon becoming aware of a personal data breach, while a detailed report regarding the incident must be submitted to the Data Protection Board of India (DPBI) within a strict 72-hour timeline in accordance with Rule 7 of the DPDP Rules, 2025.
3. **Significant Data Fiduciaries (SDF):** Digital platforms that process huge amounts of personal and sensitive data or that are highly risky to electoral democracy or national security will be considered as SDFs. They will be subject to stringent regulatory requirements, including appointments of an independent Data Protection Officer, annual DPIAs, data audit, and algorithmic discrimination test.
4. **Data Retention & Destruction:** It is essential to have a defined timeline based on specific purposes. More importantly, a distinct class of fiduciaries, like large e-commerce portals and social media intermediaries, is obligated to irreversibly destroy personal information after three years since its last use by the individual concerned, and thereby address the risks posed due to the continuous accumulation of the digital doppelgänger.[34]
5. **Deterrent Financial Penalties:** Under the DPDP Act, penalties will not be criminal in nature but rather huge financial ones to ensure deterrence. In line with the law, the maximum penalty to be imposed in case the Data Fiduciary fails to undertake adequate measures to secure personal information from any breach can amount to as much as ₹250 crores (€28 million or $30 million).

F. Regulating Deep fakes: The 2025/2026 IT Rules Amendments

In response to the rapidly developing issue of the use of Generative AI, deep fakes, and synthetic identity theft, the MeitY made aggressive changes to the Information

[34] The Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, "Digital Personal Data Protection Rules" (Government of India, 2025).

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[35] Passed for the first time in October 2025 and later updated early in 2026, the new rules represent one of the most comprehensive legal efforts globally to regulate synthetic media without adopting extreme censorship that stunts technological innovations.

1. **Synthetically Generated Information (SGI):** The amendments include defining the legal concept of "synthetically generated information" (SGI). SGI is legally defined in a technologically neutral way as "information which has been generated, created, manipulated or changed using a computer resource such that it is reasonably likely to pass as genuine or authentic."[36] The broad definition of SGI is necessary for future-proofing since it encompasses audio manipulation, deep fake videos, and even fakes metadata constructions, although AI writing is not included under this umbrella term.
2. **Mandatory Labeling, Transparency, and Traceability:** In order to address the deception inherent in the Digital Doppelgänger and deep-fake scam, New Rule 3(3) mandates strict and non-negotiable transparency obligations. The platform intermediaries using AI content generator technologies are required to clearly mark all generated content. Video deep-fakes shall have a mandatory label or watermark, indicating “Synthetically Generated,” which should cover at least 10% of the screen area for the complete duration of the video content. Likewise, the audio deep-fakes shall mandatorily contain a disclosure note, which covers at least 10% of the beginning of the audio recording. Further, the technology companies generating digital content are obligated to incorporate unique and non-removable metadata tags in the digital file before distribution to users. Significant Social Media Intermediaries are also required to take proactive measures to obtain users’ agreement for the generation of any synthetic digital content. Further, they

[35] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).
[36] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025).

are required to caution users on quarterly basis about severe legal repercussions of misusing SGI technologies for the purposes of impersonation, exploitation, production, or dissemination of non-consensual intimate content, or financial scams.

3. **The Safe Harbor Paradox and Fiduciary Accountability:** The amendments in the IT Rules of 2025/2026 highlight a crucial yet unsettled legal dilemma concerning intermediary liability. Section 79 of the primary IT Act of 2000 is the key provision providing the "safe harbor" protection, whereby all passive digital intermediaries would be immune to the liability for any unlawful content generated by their users, provided they acted in good faith and promptly removed all offending material post-formal notice (based on the ruling precedent of Shreya Singhal).[37] Nevertheless, the swift emergence of native integrations of GenAI tools, such as image generator or voice-cloning services incorporated into social media platforms themselves, drastically obliterates the legally recognized boundary between a passive facilitator and an active manufacturer of the content. According to the legal experts, in cases where a social media company uses GenAI technology in order to generate a particular user's image, without receiving the necessary consent in compliance with the DPDP requirements, the company stops acting as a mere intermediary and becomes a "Data Fiduciary" or a producer. This automatically stripes the company off its protection under Section 79 and subjects it to direct responsibility under the DPDP Act (with penalties going up to ₹250 crores) and BNS.

VII. JURISPRUDENTIAL EVOLUTION: PERSONALITY RIGHTS AND THE RIGHT TO BE FORGOTTEN

However, regardless of how updated the legislative framework may be, it is incapable of predicting all the nuances involved in cyber injuries. Therefore, the lack of a comprehensive law that regulates personality rights or the RTBF in India necessitates

[37] Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025); Entrust, "Identity Fraud Report" (2025)

judicial innovation. The courts are now turning to profound readings of the constitution in order to protect people against the insidious dangers that arise out of digital profiling and artificial intelligence.[38]

A. The Evolution of Personality Rights against Synthetic Misuse

For instance, personality rights and the right to publicity in India have always been understood solely in terms of the intellectual property law associated with business. Celebrities have relied upon trademark law and passing off cases in order to stop any unauthorized use of their likeness for profit (e.g., stopping an unauthorized third party from selling merchandise bearing the name of a celebrity). Unfortunately, this legal doctrine has proven entirely inadequate against privacy abuses that are not commercially motivated, such as the creation of deep-fake pornographic material or malicious impersonation of a political figure.

The emergence of GenAI technology requires a drastic jurisprudential turn where personality rights move away from the scope of Intellectual Property laws and take refuge under the basic human rights provided in Article 21 of the Indian Constitution (Right to Life and Personal Liberty). Indian High Courts, especially the Delhi High Court, have been using dynamic injunctions in their protective measures for a long time now.

The contemporary jurisprudence surrounding synthetic misuse and AI-enabled identity exploitation did not emerge in isolation. Prior to the 2025 deep-fake-related rulings, Indian courts had already begun recognizing personality rights as independently protectable legal interests within digital environments. In *Amitabh Bachchan v. Rajat Nagi* (2022), the Delhi High Court granted one of India's earliest John Doe injunctions protecting celebrity personality rights against unauthorized digital exploitation across existing as well as future technological mediums.[39] This doctrinal expansion was further strengthened in *Anil Kapoor v. Simply Life India & Ors.* (2023), where the Court expressly acknowledged that artificial intelligence technologies are

[38] Alliance Center for Intellectual Property Rights, "The Digital Doppelgänger" (2025); Kamya Buch v. JIX5A39 (2025); Sadhguru Jagadish Vasudev v. Igor Isakov, CS (COMM) 578/2025.
[39] *Amitabh Bachchan v. Rajat Nagi*, CS (Comm) No. 819/2022, Delhi High Court, decided on November 25, 2022.

capable of replicating an individual's voice, likeness, image, mannerisms, and persona without consent, thereby recognizing the commercial and dignitary value of AI-replicable identity attributes.[40] These decisions collectively laid the jurisprudential foundation upon which subsequent 2025 rulings addressing synthetic media, deep-fakes, and digital impersonation were constructed

In the precedent-setting 2025 case of Sadhguru Jagadish Vasudev v. Igor Isakov, the Delhi High Court had to deal with a well-organized international network using technologically advanced AI-morphed deep fakes of the plaintiff to post endorsement videos and make false allegations about his arrest. It is acknowledged openly that conventional intellectual property laws would be ineffective against "digital pandemic" in this case, therefore, Justice Saurabh Banerjee had passed an unheard-of "dynamic+ injunction". Not only did it require removal of specific offending videos, but it also made the online platforms responsible for continuous detection and deletion of any other synthetic videos similar to these offending ones.

Judicial activism does not stop here either. In Ankur Warikoo v. John Doe, a social media celebrity was able to get a full John Doe order against everyone who would exploit his name and likeness via their creation using AI for fraudulent purposes.[41] Furthermore, in Kamya Buch v. JIX5A39, the Delhi High Court ruled in favor of a public academic and activist who suffered severe reputational and dignitary harm because of non-consensual deep-fake content circulated online. The Court grounded its protection primarily in the constitutional right to dignity under Article 21, thereby extending meaningful protection beyond celebrities and commercial personality-rights claimants.

B. The Right to be Forgotten (RTBF) and the Battle Over the Digital Doppelgänger

Although dynamic injunctions seek to deal with the imminent problem of creating deep-fakes, the Right to be Forgotten is the key legal framework that can be used by

[40] *Anil Kapoor v. Simply Life India & Ors.*, CS (Comm) No. 652/2023, Delhi High Court, decided on September 20, 2023.
[41] Alliance Center for Intellectual Property Rights, "The Digital Doppelgänger" (2025); Kamya Buch v. JIX5A39 (2025); Sadhguru Jagadish Vasudev v. Igor Isakov, CS (COMM) 578/2025

individuals to cure the temporality of the digital doppelgänger.[42] The Right to be Forgotten is a tool that enables individuals to request the deletion or non-indexation of outdated or irrelevant data, or data associated with extreme stigma, stored in online search engines or digital libraries. The basis of such a law was provided by the landmark Supreme Court decision in Justice K.S. Puttaswamy (Retd.) v. Union of India in 2017.[43] In this ruling, a nine-member bench declared privacy as an implicit right guaranteed under Article 21, observing that although humans have a forgettable memory, the internet has a "long memory" that must be constitutionally constrained. However, despite the Puttaswamy precedent, the implementation of RTBF in India is riddled with constitutional conflicts. Presently, there is a tug-of-war between the individual's right to privacy and rehabilitation (Article 21) against the public's right to information and open justice (Article 19(1)(a)).[44]

The Indian judiciary displays a marked difference of opinion in relation to this matter:

1. **Pro-Privacy / Rehabilitation Approach:** In critically important cases like Jorawar Singh Mundy v. Union of India and Rakesh Jagdish Kalra v. India Today Group (2024), the High Court of Delhi awarded significant RTBF benefits to those who were legally cleared from any criminal proceedings. The Court emphasized that the persistent presence of online links to any criminal accusation against a person who has been legally declared innocent holds no relevance in serving any public good whatsoever. Rather, it imposes a grave social stigma, limits employment opportunities, and violates the right to dignity, thus rendering the media's right to free speech irrelevant, calling for the removal or de-indexation of the damaging material.
2. **Anti-RTBF / Open Justice Approach:** On the other hand, in instances where judicial transparency is highly implicated, courts have strongly limited the invocation of RTBF. In its important decision of January 2026, the Delhi High

[42] Jorawar Singh Mundy v. Union of India, WP(C) 3918/2021; Rakesh Jagdish Kalra v. India Today Group, 2024 SCC OnLine Del 5113
[43] Jorawar Singh Mundy v. Union of India, WP(C) 3918/2021; Rakesh Jagdish Kalra v. India Today Group, 2024 SCC OnLine Del 5113
[44] Jorawar Singh Mundy v. Union of India, WP(C) 3918/2021; Rakesh Jagdish Kalra v. India Today Group, 2024 SCC OnLine Del 5113

Court rejected the writ petition filed by a university professor demanding the deletion of confidential, extremely private information about their severe level of disability (79% permanent disability) which was systematically documented and made available through earlier judicial decisions. According to the Delhi High Court, without there being a specific statutory provision for the amendment/deletion of official judicial records, the use of powers under Article 226 to alter the public record in light of the petitioner's serious mental distress and violation of DPDP Act could not be entertained. Similarly, in the case of IKanoon Software Development Pvt. Ltd. v. Karthick Theodore (2024), the Supreme Court of India issued a stay against the Madras High Court decision that allowed an acquitted person to remove their name from a published judgment relating to sexual assaults.

The Right to Be Forgotten (RTBF) in India is very unpredictable until either the Supreme Court makes a unifying judgment regarding the issue based on the Constitution or the scope of the Right to Erasure provision, enshrined in the DPDP Act 2023, gets thoroughly tested in accordance with the principle of openness in court proceedings.

VIII. COMPARATIVE GLOBAL LEGAL FRAMEWORKS: ASSESSING INDIA'S TRAJECTORY

Any regulation concerning digital identity and cybercrime naturally goes beyond geographic borders. Therefore, a comparative study of the legal frameworks regulating such issues can be valuable in assessing the effectiveness of the Indian model of regulation.

The comparative legal study of different countries' legal systems in relation to digital identity regulation and cybercrime prevention highlights different approaches. For example, the European Union uses a fundamentally rights-oriented and proactive approach based on the GDPR (2016) and EU AI Act. The system provides data protection by design, imposes stringent limits on cross-border data transfer, provides a general Right to Erasure (Article 17), and prescribes risk management requirements for AI developers. In contrast, the US government follows a reactionary, market-

based, and fragmented approach. An important feature of the European Union's regulatory framework is Article 50 of the EU AI Act, which imposes transparency obligations for AI-generated and deep-fake content by requiring clear disclosure and visible labeling mechanisms where synthetic media may mislead viewers regarding authenticity.[45] This approach bears significant similarity to India's 2025 IT Rules framework mandating 'Synthetically Generated Information' labels, metadata tagging, and watermarking obligations for AI-generated content. The basis of its legal framework includes the CFAA (1986) and various state laws, such as CCPA/CPRA. There is no single federal privacy act, and the laws are predominantly based on opt-outs and state-based regulations focused on corporate data use. Finally, the UK, following the GDPR after Brexit, has adopted a proactive and institutionalized approach via the Data Protection Act (2018), including a very powerful independent regulatory body.

The Indian IT Act (2000), BNS/BSA (2023), DPDP Act (2023), and IT Rules (2025/26) put India currently in a hybrid transitional stage, shifting its paradigm from being purely reactive to more proactive. India is in the middle of an extremely significant transition from purely punitive enforcement to data governance encompassing proactive, statutory regulation of deep fakes (e.g., the labeling of SGI) that is even more rigorous than the western one while imposing a very wide range of extraterritorial digital harms jurisdiction. Europe's GDPR is currently the absolute global gold standard in the field of personal data protection, relying on a very proactive and fundamental rights-based paradigm. Under the GDPR, there exist extensive and inflexible legal bases for data processing operations, mandatory rules regarding data protection by design and by default, and explicit right to erasure which gives citizens enormous power when it comes to dealing with their digital doppelgängers.

In comparison, the American approach to digital protection is rather highly fragmented, market-based, and sectoral. Despite the presence of quite outdated

[45] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (EU AI Act), art. 50, 2024 O.J. (L 1689) 1.

legislation such as CFAA, regulating unauthorized network access, there currently exists no federal privacy law in the United States. However, the US employs a hodgepodge of state interventions like CCPA that mostly utilize the "opt-out" transparency framework, which is less stringent compared to the "opt-in" standard employed by EU laws.

It is noteworthy how India's journey of regulation is an example of a fast-tracked hybrid strategy. Historically, India's stance as provided for in the IT Act 2000 was extremely reactive, concentrating predominantly on post-facto punishment of financial and identity thefts. Nevertheless, with the introduction of the DPDP Act 2023 and subsequent major IT Rules amendments for 2025, there is a clear shift towards the EU model, which is proactive and based on rights. As opposed to the GDPR, which applies universally, carries hefty fines, and operates with a consent-focused approach; the DPDP Act mirrors some of these aspects but diverges from others, providing fewer grounds for processing personal data.

Particularly, the DPDP Act adopts a considerably narrowed Right to Erasure compared to the GDPR one, which can be applied to any type of processing, while in India, the right only exists for explicit consent-based digital data processing. But the unique strength of India on the world stage is its bold, highly targeted regulation of GenAI and deep fakes through the 2025 IT Rules. It is an area where even the stringent EU AI Act that came into force recently cannot claim to have gone beyond generalities and concentrate on systemic risks when compared with the deep-fake-focused labeling requirements mandated by India.

IX. CRITICAL STRUCTURAL BOTTLENECKS IN ENFORCEMENT

Although there is no denying that the legislation in question, which consists of the BNS, BSA, DPDP Act, and IT Rules, is undoubtedly a strong and up-to-date legal framework for dealing with this issue, the actual implementation of the laws into practice is seriously hindered due to a number of structural issues.

First, an overall lack of technological literacy among officers of state and municipal police forces is the most crucial factor undermining the effectiveness of the legislation in question. Investigating sociotechnical crimes necessitates using digital forensics,

which includes tracing concealed IP addresses, analyzing complicated sets of metadata, decrypting money laundering schemes involving crypto currencies, and conducting stylometric analysis of voice samples. Currently, many law enforcement agencies simply do not have access to necessary technologies or expertise necessary to conduct these procedures and enforce the mandates put forth in the 2025 IT Rules.

First, the deliberate procedural difficulty built into the BSA 2023 poses a potential risk to rendering criminal proceedings involving digital evidence completely unmanageable. The extremely unclear statutory provisions regarding the qualification requirements for the "Part B" expert certification for electronic evidence (Section 63) may lead to a difficult and antagonistic judicial situation. Completely legitimate, highly relevant digital evidence proving identity theft, cyber-stalking, or digital arrest fraud may be ruled inadmissible under the most technical of procedural default conditions concerning the certification procedure. If lawyers and judges waste time fighting over what constitutes a digital expert in an antagonistic atmosphere, the BSA will render itself completely ineffective due to procedural warfare.

Third, cyberspace's non-territoriality inherently poses a significant challenge to jurisdictional enforcement efforts. In accordance with predictions made by the Space Transition Theory, the individuals responsible for the worst cases of digital arrest fraud, cognitive warfare, and deep-fake extortion rings tend to act freely within cyberspace from such cyber havens as Southeast Asia and Eastern Europe. Although the BNS explicitly establishes extraterritorial jurisdiction on paper, the political and logistical impossibility of enforcing MLATs, international law, and physical extradition of criminals makes the process a very difficult task.

X. SUGGESTIONS AND RECOMMENDATIONS

To narrow the perilous chasm separating legislative aspirations from practical execution, and to effectively neutralize the persistent menace posed by the digital doppelgänger, a multi-pronged strategy for legislative reform is immediately necessary:

1. **Passage of a Comprehensive Digital Identity Protection Act:** In order to consolidate the existing but disjointed provisions found within the IT Act, the

DPDP Act, the BNS, and even common law tort actions, a dedicated Digital Identity Protection Act needs to be drafted and passed as soon as possible. This act should explicitly delineate the contours of the Right to be Forgotten, setting out objective standards that consider both individual dignity and rehabilitation against the backdrop of the larger public good, including considerations of open justice and freedom of expression.

2. **Consistency between Safe Harbor and Data Fiduciary Obligations:** The intermediary safe harbor regime in India is primarily derived from Section 79 of the Information Technology Act, 2000, as amended in 2008, which grants conditional immunity to intermediaries for third-party content hosted on their platforms. The operational obligations necessary for retaining such protection are further elaborated under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The Supreme Court's decision in *Shreya Singhal v. Union of India, 2015 5 SCC 1* subsequently clarified the 'actual knowledge' standard and established the procedural safeguards governing intermediary liability and the removal of unlawful online content.
3. **Institutional Capacity Building and Digital Forensic Standards:** The judicial officers, public prosecutors, and law enforcement officials need to engage in extensive training in technology laws. Most importantly, the Ministry of Home Affairs needs to urgently develop SOPs on expert witness certification procedures as per Section 63, Part B, of the BSA, establishing a high standard of scientific evidence while making it accessible enough for routine court processes involving digital documents.
4. **Institutions for Algorithmic Transparency and AI Safety:** In order to implement the lofty demands of the IT Rules regarding deep-fakes labeling and ensure continued credibility in times of crisis, the government must create an AI Safety Institute with ample resources and the authority to conduct quick and effective forensic digital scans in case of cognitive war or disinformation campaigns.

XI. CONCLUSION

The improper use of digital identities has turned cybercrime into a socio-legal problem that has concrete ramifications in the real world. Cybercrimes that include offenses such as identity theft, cyber-stalking, deep-fake technology, synthetic identity impersonations, and artificial intelligence frauds do not just affect the financial interests of people but can also harm their reputation and psychological well-being.

India has tried to adapt itself in terms of legal reforms by way of the Bharatiya Nyaya Sanhita, the Bharatiya Sakshya Adhiniyam, the Digital Personal Data Protection Act, and amendments in the Information Technology Rules. This shows a change in the pattern of Indian jurisprudence from a purely repressive one to a regulatory and preventive system. Meanwhile, practical problems related to digital evidence, technical knowledge, liability of intermediaries, and cross-jurisdictional enforcement persist.

With the advent of generative artificial intelligence, the task of manipulating identities digitally becomes much easier and cost-effective. Under such circumstances, the question of legal protection for the digital identity of individuals cannot just be seen from the perspective of privacy but involves aspects of dignity, individual liberty, democracy, and public safety.

XII. BIBLIOGRAPHY

A. Statutes and Rules

1. The Bharatiya Nyaya Sanhita, 2023.
2. The Bharatiya Sakshya Adhiniyam, 2023.
3. The Digital Personal Data Protection Act, 2023.
4. Digital Personal Data Protection Rules, 2025.
5. Data Protection Act, 2018 (United Kingdom).

B. Case Laws

1. Jorawar Singh Mundy v. Union of India, WP(C) 3918/2021.
2. Kamya Buch v. JIX5A39 (2025).
3. Rakesh Jagdish Kalra v. India Today Group, 2024 SCC Online Del 5113.

4. Sadhguru Jagadish Vasudev v. Igor Isakov, CS (COMM) 578/2025.
5. Anvar PV v PK Basheer (2014) 10 SCC 473 (SC).
6. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (SC).

C. Books

1. F. Schmalleger and M. Pittaro (eds.), Crimes of the Internet (Prentice Hall, 2008).

D. Journal Articles

1. Dours and A. Eaton, "Using Routine Activity Theory to Predict Technology-Facilitated Violence," Journal of Research in Crime and Delinquency (2025).
2. T.J. Holt and A.M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," 26 Deviant Behavior 428 (2009).

E. Reports and Online Sources

1. Alliance Center for Intellectual Property Rights, "The Digital Doppelgänger" (2025).
2. BioCatch, "Report: Digital Banking Fraud Trends in India" (2025). Entrust, "Identity Fraud Report" (2025).
3. Ministry of Electronics and Information Technology, "Explanatory Note: Proposed Amendments to the Information Technology Rules, 2021" (Government of India, 2025).
4. National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024). Office for National Statistics, "Crime in England and Wales" (2024).
5. "The Corporeality Crisis: How Immersive Technology is Outpacing India's Sexual Assault Laws," Jurist (2026).