SURVEILLANCE, AI AND SYNTHETIC MEDIA: RECLAIMING DIGITAL DIGNITY IN THE AGE OF ALGORITHMIC GOVERNANCE

Malavika Manivannan, SVKM'S Narsee Monjee Institute of Management Studies

1.Introduction

The rapid developing digital era has been boon as well as a ban for the contemporary society, where the individual autonomy and personhood within the digital realm are at stake, and the very essence of human identity hands in precarious balance. These situations do not merely constitute speculative cacotopia but represent the tangible demand of the contemporary digital setting, wherein developing technologies like Artificial Intelligence (hereinafter AI) and deepfakes that inevitably attenuate the judicial and ethical demarcation between real and fake, subjugation and self- determination, in this process of nullification of the borderline between fake and real the Digital Dignity of human beings and the national security of the state are in jeopardy.

Digital Dignity consist of a complex synthesis of individuals digital footprint such as online communication, biometric markers, social media presence and transactional footprints. These are the elements which exceed mere data points. Infringing upon this digital persona leads to intrusion upon individuals' privacy, dignity, integrity and choice. A robust normative protection shall be necessitated due to a profound connection found between the digital dignity and core human experience in the current digital era.

Moreover, Digital Dignity encompasses of three core components: informational integrity, the protection misrepresentation of personal data and unauthorised alteration of personal information; autonomy, the control and authority of individuals over their personal data and digital presence and representation authenticity, the right to control the use of one's likeness, voice and persona in digital media. These elements together ensure that individuals are not mere data point nor algorithmic prediction but are to be treated with dignity and rights- bearing agents with inherent moral and legal worth.

India's Constitution provides a foundation for recognizing and balancing digital rights. In the Puttaswamy [1] Decision the Supreme Court recognized that privacy is a component of Article 21[2] of the Constitution and that autonomy, self-determination, and bodily integrity are parts of human dignity. This important jurisprudence can now look to the digital sphere in determining

[1] *Justice K.S.Puttaswamy(Retd) vs Union of India,* 2019 (1) SCC 1.
[2] INDIA CONST. art. 21.

the extent to which emerging technologies like artificial intelligence, surveillance technologies and deep fakes affect the rights of individuals.

These emerging technologies can disrupt existing rights and relationships. AI algorithms that determine credit, job and service allocation are opaque and can amplify existing social inequities. Spyware like Pegasus and other surveillance technologies that monitor and record communications in real time raise a host of issues related to privacy, confidentiality, and free expression. Deep fakes, particularly in the realm of synthetic media, have the potential to socially manipulate large groups and undermine trust through realistic fraudulent representational attacks. These issues highlight the need to systemically and legally recognize digital dignity as a fundamental principle in India's evolving legal and technological landscape.

By including digital dignity at the intersection of human right, constitutional law and emerging technologies, this article seeks to explore both theoretical and practical dimensions of protecting individuals in the digital age, while offering a rights-based roadmap for law, policy and corporate governance.

2. Components of Digital Dignity

Digital Dignity is not an individual concept; it is a multidimensional concept that combines legal, ethical, philosophical and technological considerations. Its main objective is to ensure that individuals maintain their inherent worth, agency, and control over their digital selves.

2.1. Autonomy

Autonomy in the digital realm is the meaningful ability to control one's personal data, communication, and one's digital presence. It includes the right to determine what information is wanted and to control the processes of collection, treatment, and sharing of data by the state or any private entity. With rapid algorithmic decision systems, autonomy also implies the ability to contest and influence decisions over access to critical resources, jobs, and participation in society. Without such control, one risks being a passive data subject and having opaque algorithms or state-sponsored surveillance systems make key decisions about one's life.[3]

[3]Sandra Wachter, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, IDPL,2017 1, 5, (2020).

In the Indian context, autonomy is grounded Constitutionally in the right to privacy as elaborated in Puttaswamy[4]. The Supreme Court gave primacy to personal autonomy as an essential facet of human dignity and autonomy sequentially extends beyond bodily integrity to encompass the right to control one's information. This principle allows the state or private entities to frame actions or processes concerning data and digital life in a proportionality and legality.

2.2. Representational Authenticity

An individual's right to manage how their image, voice, and likeness are used in digital media is called representational authenticity. The unauthorized use of deepfakes and AI-generated content can amplify risks associated with reputational risks and psychological distress, particularly with women and public and vulnerable people. Even social stigmatization can occur with unauthorized use of likeness.

In India, there are some legal protections in place, particularly through the IT Act and criminal law in the context of obscene content and non-consensual sharing of material. Although, the rapid innovations in the generic technologies do call for law and policy to catch up. To defend audits and policy gaps, there will need to be specific and tailored approaches to deal with representational authenticity including rapid response content takedown, forensic attribution of harmful content, and holding harmful content creators and distributors accountable.

2.3. Informational integrity

Informational integrity is maintained when data is kept accurate, reliable, secure, and protected from unauthorized access and manipulations. To be more specific, unauthorized access and manipulations of a person's data, as well as falsifications and unauthorized changes, should be maintained to protect a person's reputation and legal rights. This is especially important when it comes to personal finances, biometric data, private health information, and other classified information.

Informational integrity isn't protected in a myriad of ways and, more specifically, unauthorized access via spyware, corporate breaches, and biased data profiling are specific cases. Take the

[4] See Supra note 1.

case of Pegasus spyware[5]. Informational integrity is also a factor of trust, in that case, trust is breached when private and confidential communication is shared with unauthorized persons, the same goes when spyware is used. Trust also needs to be enforced by legal, technological, and procedural means to be maintained.

2.4. Interconnectedness of three components

These three components autonomy, informational integrity, and representational authenticity mutually reinforce one another. Compromised integrity Autonomy often results in damaged integrity. Erosion of Informational integrity undermines representational authenticity. Therefore, any regulatory approach to protecting digital dignity must address all three components concurrently. In doing this, one must ensure that legal, corporate, and technological provisions operate in unison to uphold and defend individual rights and agency.

Structuring digital dignity in this way enables India to formulate a cohesive approach to legal and policy making that aligns technological advancements and constitutional safeguards. This also helps to devise a policy to assess and control surveillance technologies, AI systems, and synthetic media in a manner that safeguards core rights and promotes innovation.

3. Surveillance technologies and Digital Dignity

3.1. Digital surveillance

Digital surveillance refers to the generated data of individuals which is collected, analysed and monitored in digital spaces including metadata, online activity and communications which also includes complex tracking of device activity, location, browsing history, and biometric identifiers. The private actors, governments and corporation use these tools for law enforcement, security, marketing and behavioural analysis.

Even though surveillance may serve legitimate purposes, it poses significant risks to digital dignity. Constant monitoring without consent undermines autonomy by taking the individuals control over their information in the digital space which may lead to the misuse of the data and manipulation of the communication which violates the aspect of informational integrity and also compromise the aspect of representational authenticity. Thus, persuasive surveillance,

[5] Supreme Court Observer, https://www.scobserver.in/cases/manohar-lal-sharma-v-union-of-india-pegasus-spyware-probe-case-background/, (last visited Oct. 20,2025)

especially when unregulated shall pose a direct threat to the normative foundation of digital dignity.

Pegasus is advanced spyware which was developed by NSO Group that can penetrate a smartphone without a user's knowledge. Once spyware is installed, it can capture and access messages, call logs, emails, and GPS location and stream audio and video data. Pegasus can even access and capture data on apps in real time. Pegasus spyware can breach and bypass encryption, leaving no trace. This makes Pegasus spyware one of the most sophisticated digital surveillance spyware.[6]

In India, investigations suggest surveillance of journalists, human rights defenders, advocates, and politicians, bringing the legality and proportionality of such surveillance practices into question. The Supreme Court responded to public interest litigation by appointing an expert committee to investigate the allegations concerning the use of Pegasus. This highlights the constitutional issue. Surveillance of this magnitude involves Article 21, which the surveillance subject K.S. Puttaswamy (Retd.) v. Union of India recognized and defined as the right to life and personal liberty, including the right to informational privacy.

The implications of using Pegasus are alarming, especially in the context of digital dignity in its three dimensions. Individuals suffer a loss of control over their communications, their whereabouts, and other aspects of their personal digital information. Because spyware operates in secrecy, there is no opportunity for an individual to provide consent, thereby losing autonomy. Pegasus lets the user gain control of sensitive information, a user's private and confidential information, and even personal communications. Data loss and manipulation can result in reputational loss, hurt a user's career, or even pose legal risks. Personal images, audio, and messages can be intercepted, and all the information is controlled by the user of the surveillance technology. Such an action can erode a user's trust in the digital platforms, including communication technologies.

Concerns regarding a loss of digital dignity are far less speculative. The Pegasus case demonstrates the capacity of unregulated surveillance technologies to transform digital

[6]Amnesty Organisation, https://www.amnesty.org/en/wpcontent/uploads/2021/08/DOC1044872021ENGLISH.pdf, (last visited Oct. 21,2025)

interactions from autonomous, and dignified, interactions to a controlled and dominated experience. Using surveillance technology of this kind is losing dignity.

Surveillance technologies like spyware Pegasus to control the digital spaces of individuals has received global condemnation from UN human rights experts.

The importance of the rational use of surveillance technologies 'must meet the criteria of legality, necessity, proportionality, and oversight' as stated by the UN Special Rapporteur on the use of 'surveillance technologies'. [7]

The absence of comprehensive laws on surveillance in India leads to unresolved legal issues. The limited authorizations for interception laws and the Spyware Pegasus legal frameworks do not offer a complete and comprehensive statute on the Pegasus Spyware and any of the advanced surveillance technologies. The Pegasus case investigations remains the opportunity to focus on aligning the use of surveillance technologies to respect the constitutional right of privacy and uphold the practice of having dignity in the digital space.

There are new challenges in the legal, procedural, and technological aspects where a positive or balanced response is needed to uphold digital dignity and counter the age of surveillance.

The proportionality and necessity of surveillance activities should have a legal warrant, which to be enforced and monitored, means a review mechanism to function. It is a basic democratic right and a means of legal accountability for the public to be informed audits. Surveillance tools that technically preserve privacy and end-to-end encryption are accessible and should be used and the digital rights of the person must have accessible legal remedies.

4. Artificial intelligence and Algorithmic governance.

4.1. AI in Contemporary India

AI is being incorporated into governance, business, and social services. In India, the scope of AI from welfare distribution and predictive policing to credit scoring, recruitment, and content moderation is huge. While AI increases the ability to make efficient decisions, almost constant use of AI raises issues of fairness, transparency, and responsibility. Important decisions that affect livelihoods, the ability to obtain services, and legal outcomes, may result from a decision-making system that is so opaque that individuals may have no way to respond.

[7] U.N Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/44/49 (2020).

4.2 AI and the challenge to digital dignity

Automated decision-making systems limit individuals from contesting and controlling outcomes that affect them, especially in AI-powered systems like credit scoring and recruitment algorithms. Even predictive policing systems can deny people their rights and there may be no meaningful human review of the decision. AI and Automated decision systems in Europe have to comply to legal requirements in the General Data Protection Regulation (GDRP) Article 22 and in India, the DPDP Act Data Protection Act gives individuals access to their data and the processing of it, and the ability to contest AI decisions made about them.

AI systems depend on datasets that may be wrong, imprecise, and biased. Personal and prejudicial outcomes can also happen with poor quality datasets. GDPR Articles 13[8], 14[9], 15[10], and 16,[11] providing the fundamentals of transparency by giving access and the right of correction, allowing individuals describing and incorporating automatic procedures to understand data, and allowing modification of personal data. Similarly, DPDP Act Sections 14[12] and 19[13] in India give individuals the right to access and remedy data misuse, providing transparency.

Moreover, representational authenticity can also be distorted with AI, predictive algorithms, and agents setup to target individuals with certain content. Without consent, algorithmic profiling in credit scoring, law enforcement, or social media content recommending can adversely shape public perception. GDPR Recital 71 and Article 21[14] speak to the provision of mechanistic human overall and the right to contest, to association providing digital representational control.

4.3. Structural Bias and Algorithmic Opacity

From the large datasets AI systems draw, uploaded datasets can reinforce bias targeting disadvantaged people. In India the bias could be caste or gender associated discrimination systemic inequities in the areas of employment, policing, and financial services. Algorithmic opacity and the lack of explainability layer deeper inequity, depriving individuals of the ability to understand, contest, or rectify inequitable and unexplainable outcomes. Scholars observed

[8]INDIA CONST. art.13.
[9]INDIA CONST. art.14.
[10]INDIA CONST. art.15.
[11]INDIA CONST. art.16.
[12] See supra note 9.
[13]INDIA CONST. art.19.
[14]See Supra note 2.

that even GDPR's "right to explanation" may be insufficient to fully generate autonomy or remedy harms caused by AI, emphasising the need for stronger regulations. [15]

4.4. Indian Legal and Policy Frameworks

Currently, India does not have a specific law on AI. But there are several other laws and policies that somewhat regulate AI, and algorithm governance. For example, The Digital Personal Data Protection Act,2023[16] (DPDP Act). Under section 11(1)[17] of the Act, a data fiduciary has the obligation to process a person's data fairly and transparently. Also, under section 14 of the Act, a person has the right to access and amend their personal data, and a right to contest an adverse automated decision. Also, section 19[18] of the same Act gives a person right to misuse personal data which helps in control and informational self-rights.

Other laws, such as the Informational Technology Act, 2000[19], which also has provisions that touch on the governance of AI, help to complete the picture. For example, section 43A [20]of the IT Act imposes a duty on an organization to protect data as one of the reasonable security practices. This obligation was designed to secure the data that AI systems and other technologies use. The law also tackles the issue of identity theft under section 66C[21] of the Act. This includes the use of AI for impersonation and data theft, an issue of informational integrity and representational authenticity.

Additionally, under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[22] mandates, intermediaries are required to implement grievance redress systems and ensure accountability in the moderation of automated systems. This touches, somewhat, on transparency and the safeguards on individuals' digital profiles on the web. Strategically, the National Strategy for Artificial Intelligence (NITI Aayog, 2018) positions ethical AI adoption, the human-in-the-loop principle, and bias mitigation as core strategies which closely align with securing an individuals' digital dignity.

---

[15] GDPR, Regulation (EU) 2016/679, arts. 13-16, 21-22, Recital 71.
[16]Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023(India).
[17] Digital Personal Data Protection Act, S.11(1), No. 22, Acts of Parliament, 2023(India).
[18]Digital Personal Data Protection Act, S.19, No. 22, Acts of Parliament, 2023(India).
[19]Informational Technology Act, No.21, Acts of Parliament, 2000(India).
[20] Informational Technology Act, S.43A, No.21, Acts of Parliament, 2000(India).
[21] Informational Technology Act, S.66C, No.21, Acts of Parliament, 2000(India).
[22]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,G.S.R(E), Gazette of India, Extra., Pt.II, (India).

Notwithstanding these initiatives, the extent of the regulatory vacuum is still much. In contrast with the GDPR of the European Union, India still does not have specific regulations on the mandatory performing of algorithmic impact assessments, accountability, and explainability of high-stakes AI systems, as well as the provision of damages for harms caused by algorithmic bias or errors. While the GDPR Articles 13-16, 21-22, and Recital 71 deal with the issues of transparency, contestability, and human oversight, these are the fundamental building blocks to protecting an individual's digital dignity in automated decision-making systems.

5. Synthetic media and deepfakes

Artificial intelligence tools can generate or alter media content such as audio, videos, and images, creating content that imitates real people with extraordinary likeness. A more advanced and hyper-realistic version of a person's image or likeness can be created and distorted using deep learning and other advanced tools. One can swap heads, alter bodies, and change voices and other features in a way that makes it almost impossible to detect. This makes a person's digital image, privacy, and information integrity a potential target for abuse to extremes.

Synthetic media, and especially deepfake technology, can profoundly and horizontally harm people. A person subjected to deepfake abuse can be manipulated by harassment, character assassination, blackmail, and ruining their reputation. This technology can create false and illegally manipulated images or videos of a person, create non-consensual pornographic material, and carry out financial scams. The risks this technology poses are more than evident in some highly publicised cases in India.

The potential for deepfake misuse, especially for gender abuse, is disturbing. Vulnerable populations and women face the brunt of this technology's abuse. Non-consensual sexual content exploitation deepfakes proliferate gender-based violence within digital spaces. Such gendered abuse profoundly violates a person's dignity and reflects the greater societal misogyny and harassment a person endures.

In the case of Ankur Warikoo and Anr v. John Doe[23] and Ors, the Delhi High Court John Doe injunction restraining the circulation of deepfake videos impersonating Ankur Warikoo, a prominent personal finance educator and content creator. It was Warikoo's image, voice, and likeness that was used in circulating AI-generated deepfake videos on social media in which

[23] *Ankur Warikoo and Anr v. John Doe,* SCC OnLine Del 3727.

he was recorded giving testimonials for stock market Ponzi schemes and inviting patrons to WhatsApp groups to share tips and tricks for investing, something his critics claim he does. Justice Amit Bansal described the deepfakes as "active and complete impersonation" and infringed Warikoo's personality, publicity, and commercial rights, ordering content removal from Meta and other platforms within a designated period. Warikoo's case is the first in India to consider deepfake technology, personality rights, and emotional and economic abuse.

More recently in Sadhguru Jagadish Vasudev & Anr v. Igor Isakov & Ors[24], the Delhi High Court ordered the Department of Telecommunications and the Ministry of Electronics and Information Technology to block websites and social media accounts that distribute AI-generated deepfake impersonations of Sadhguru. This case contained misleading content, including fake arrest videos, and drew attention to the potential of deepfakes being used to spread disinformation and perpetrate scams. A 57-year-old woman from Bengaluru was reported to have lost ₹3.75 crore after coming across a deepfake video of Sadhguru promoting a trading platform.

5.1 Legal Gaps in the Indian Framework

Even with the ongoing case laws and applications of a few provisions of the Indian law, there could still be reluctance in taking legal action against the misuse of synthetic media technologies. For example, the Information Technology Act, 2000, has provisions that may be applicable to tackling a few deepfake cases, such as:

• Section 66C[25] (identity theft)

• Section 66D [26](cheating by personation using computer resources)

• Section 66E [27](violation of privacy)

• Sections 67[28], 67A[29], and 67B[30] (publishing or transmitting obscene or sexually explicit content in electronic form).

[24]Sadhguru Jagadish Vasudev & Anr v. Igor Isakov & Ors, CS(COMM) 578/2025.
[25]See Supra note 21.
[26]Informational Technology Act, S.66D, No.21, Acts of Parliament, 2000(India).
[27]Informational Technology Act, S.66E, No.21, Acts of Parliament, 2000(India).
[28]Informational Technology Act, S.67, No.21, Acts of Parliament, 2000(India).
[29]Informational Technology Act, S.67A, No.21, Acts of Parliament, 2000(India).
[30]Informational Technology Act, S.67B, No.21, Acts of Parliament, 2000(India).

These provisions were created long before the emergence of deepfake technology and certainly do not deal with the creation, circulation, or harm of synthetically created information. Legally speaking, "deepfake" and "synthetic media" do not exist as terms in Indian law, which makes legal enforcement near impossible. Furthermore, the law fails to attend to issues of consent, algorithmic harm, and responsibility of the content hosting platforms.

5.2. Proposed Remedies

The Indian government responded to these gaps with regulatory reforms. In October 2025, the Ministry of Electronics and Information Technology introduced draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the regulation of "synthetically generated information" in the legislation. The amendments propose:

• Embedding clear labels and metadata so that users can tell real information from synthetic content.

• Synethic content must meet certain visibility and audibility thresholds, including the 10% rule.

• Intermediaries having reasonable technological means to verify, identify, and synthesize labeled content.

• Platforms that do not take down unlawful synthetic content must takedown mechanisms and accountability to it.

Regulatory reform is only the beginning. The remaining reforms would need forensic attribution targeting deepfake perpetrators, proportional criminal punishment, removal of post-processed content, and restoring the victim's reputation.

6. Cyber Crime in India: NCRB Report (2022-2023)

As noted in the NCRB report on Crime in India 2023, the most recent report notes an increasing trend on the number of Cybercrime incidents in India. There is an increasing need for advocacy around the legal and the policy fronts in the domain. 86,420 cybercrime incidents were registered which reflects a 31.2% increase compared to 2022 at 65,893 cases. Increased reporting is one of the explanations, but the scope and the sophistication of the digital crimes are on the rise at an exponential rate.

In 2023, the cybercrime incidents registered per lakh population, went from 4.8 in 2022, to 6.2, which is an increase of 1.4. Within the 19 major metro areas where a majority of the digital transactions take place, this trend is worse. In 2023, the number of cases in these cities increased from 24,420 to 33,955 (39%) and the population crime rate in these cities went from 21.4 to 29.8 per 1 lakh. Cybercrime in India is largely located in urban areas, specifically cities like Delhi, Mumbai, Bengaluru, and Hyderabad. This indicates that urban places are more likely to show a higher concentration of digital vulnerabilities.

Cybercrime case distribution patterns are a function of actors' criminal intent and the vulnerability of the targets. In 2023, the most significant proportion of cases attributed to a form of cybercrime involved the financial exploitation of victims:

- Out of 2023 registered cybercrimes, fraud, which is a motive of financial exploitation, accounted for 59,526 cases (68.9 percent). This category includes deceitful online banking, e-commerce scams, phishing schemes, unauthorized online transactions, and a gamut of deceitful transactions to victims at the hands of offenders.

- Sexual exploitation form the second major problem with 4,199 cases (4.9 percent), which involved non-consensual private photo sharing, cyber harassment, and online sexual abuse.

- Extortion, which includes ransom demands, submission of sensitive data, ransom threats, and payment demands, constituted 3,326 cases (3.8 percent).

The examination of motives reveals that in India, most cybercrimes occur due to the pursuit of profit. The data criminals who perpetrate financial fraud, misuse personal data to breach financial accounts, and commit credit-based impersonation and account fraud are the bulk of the criminals. Even though identity theft is not the main motive, it is a significant overlapping motive.[31]

6.1. The paradox: Dignity vs. surveillance.

Cybercrime may have resulted in policies that prioritize surveillance, increased monitoring of individuals and activities, and the argument of national security. However, the surveillance of citizens using facial recognition, predictive policing, and digital capture securitize users' dignity and privacy. In the extreme, the Pegasus spyware surveillance of citizens, such as

[31]National Crime Records Bureau, Crime in India 2022, (Ministry of Home Affairs 2023) www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf.

journalists, lawyers and activists, demonstrates how technologies of protection can, paradoxically, serve as instruments of ambush and active surveillance.

This is an illustration of the "governance paradox." Surveillance technologies, intended as protective shields, may simultaneously infringe population members' self-determination, dignity. This antagonism of security vs. dignity is exacerbated when there is no transparency, no ex-post judicial review, and no accountability regarding the use of surveillance technologies. In India, while the Information Technology Act, 2000 (S69, 6) allows the government to oversee and intercept communication, the gaps in judicial oversight and the limited avenues available for the citizens' redress undermine the protective intent of the law.

The expansion of surveillance by the government should not be justified by the increasing rates of cybercrime. A state cantered on human dignity should adopt a model of cybercrime control strategies that protect the dignity of the individual through the legally permissible tiers of justified and balanced surveillance defined under the proportionality principle, as ruled in the Puttaswamy v. Union of India case on privacy in 2017, and the Anuradha Bhasin v. Union of India (2020) case which reiterates the principles of proportionality and procedural safeguards.

The state must appreciate that the dignity of the individual must be respected, even while protecting the individual from the cybercrime. The empirical data from the NCRB reports illustrates the need to bolster the state's institutional capacity vis-a-vis cyber offences structurally and, even more, the need to self-regulate and normative limit surveillance. Embedding digital dignity in and all the governance and enforcement systems in place means technology serves as a means of empowerment, and not a means of oppression.

7. Legal Framework in India

7.1. Constitutional Protections

The foundation of India's digital dignity framework is located in the Indian Constitution, primarily in Article 21[32]: "No person shall be deprived of his life or personal liberty except according to procedure established by law." The Supreme Court has included the 'Right to Live with Dignity' as an implicit right under Article 21, [33]along with dignity, autonomy, and the right to 'Privacy' as well.

[32]See Supra note 2.
[33]*Ibid*

In Anuradha Bhasin v. Union of India[34], the Court applied proportionality to digital restrictions and held that an indefinite internet shutdown constitutes a violation of free speech and a disproportionate infringement of the right to privacy. In the same manner, Faheema Shirin R.K. v. State of Kerala[35] recognized that access to the internet is a component of the right to education and expression within the scope of Article 21. All of these precedents together highlight that the protection of life and liberty under the Constitution has a dimension ascribed to digital exclusion, which includes arbitrary surveillance, unauthorized extraction of personal data, and disproportionate embarrassment, which are the elements of digital dignity.

7.2 Statutory Framework

In India, the major laws that form the basis for the regulation of technology and data protection are the Information Technology Act, 2000 (IT Act)[36] and the Digital Personal Data Protection Act, 2023 (DPDP Act)[37].

The IT Act, India's major piece of legislation governing cyberspace, was passed to legally recognize electronic records and address laws related to cyber offences. It also contains several provisions for the punishment of cyber crimes, for example, Section 43[38] punishes unauthorized access and data breach, Section 66 and its sub-sections punish computer hacking and identity theft (S 66C[39]), and cheating by impersonation using digital devices (S 66D[40]). The Act also contains provisions under Section 69 that empower the government to intercept, monitor, or decrypt information for the purpose of national security, maintenance of public order, or for the prevention of any crimes. The lack of independent judicial oversight of this and broad surveillance power has raised concerns regarding its proportionality and possible misuse.

Along with the IT Act, the DPDP Act (2023) and its amendments is noted as India's first comprehensive data protection legislation. It establishes the responsibilities of data fiduciaries to handle data in a fair and legal manner and for legitimate and specified purposes (S4, S11). Individuals, referred to as "data principals" have the right and access to personally held data, and can correct or erase data (S12–14). Furthermore, the Act sets up a Data Protection Board

[34]See Supra note 33.
[35]*Faheema Shirin R.K. v. State of Kerala,* 2019 SCC OnLine Ker 2976.
[36]See Supra note 19.
[37]See Supra note 16.
[38]Informational Technology Act, S.43, No.21, Acts of Parliament, 2000(India).
[39]See Supra note 21.
[40]See Supra note 26.

of India to handle complaints and will have the power to levy fines (S 27–29). Not with standing, the DPDP Act still has, and made clear, considerable gaps in relation to algorithmic transparency, protections against automated decision-making, and independent oversight over state surveillance. It will hide and, expose, digital dignity from harm, including emerging issues with AI profiling, misuse of spyware, and manipulation of synthetic media.

Apart from this, the absence of harmonized principles in the laws and rules governing interception of communications, as well as the the laws from 1885 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[41], leads to principles, overlapping responsibilities and legal ambiguity.

The Supreme Court took cognizance of the matter and appointed a Technical Committee to investigate the allegations and claim of unrestricted surveillance strikes at privacy and dignity. The Court also reaffirmed that the "national security" exception could be advanced, only, if it contained substantiate reasoning and procedural safeguards.

The Pegasus inquiry carried the ethos of Puttaswamy. Surveillance, he said, exercised a right of a citizen that must be governed by the laws of legality, necessity and proportionality. While it is true that the absence of a dedicated surveillance regulation law contractor and executive discretion, judicial review still remains the core check against abuse of discretion.

The Indian judiciary's evolving technology jurisprudence, now, places the right to privacy and dignity and, within the digital era, establishes the presence of digital rights as modern dignity. This is a foundational step to propelling the right of 'digital dignity' to a constitutional and substantive statutory status in India.

8. International perspectives

8.1. Global frameworks

Digital dignity is an established right under many international frameworks. UDHR Article 12 and ICCPR Article 17 endorse the right to not have one's "privacy, family, home or correspondence" arbitrarily interfered with. These rights formed the basis of informational autonomy and dignity in cyberspace and the digital context. More pertinently, the UNGPs extend these obligations to the private sector to an extent, such as tech companies and digitally

[41]See Supra 22.

driven businesses who are human rights due diligence and the rights of affected third parties in the context of digital anti-personnel systems.

In the UN High Commissioner for Human Rights (2021-2023) reports, the focus is on the erosion of autonomy, equality, and psychological integrity by digital technologies. The deployment of AI, facial recognition, and biometric systems without rights and safeguards can trigger systemic dignity and identity risks. Thus, international frameworks and digital technologies have shifted the understanding of privacy from secrecy to enhancing human worth, autonomy, and self-determination.

8.2 EU's GDPR and Human Centric Regulation

The EU's General Data Protection Regulation (GDPR) is the most extensive legal manifestation of 'data dignity.' Recital 1 of the GDPR claims 'The protection of natural persons in relation to the processing of personal data is a fundamental right.' It embodies operational data dignity through the principles of lawfulness, fairness, purpose limitation, data minimization, and accountability.

Relevant for India, in particular, is Article 22 (rights against automated decision making and profiling) and Article 35 (Data Protection Impact Assessments). These are anticipatory regulations that go beyond data misuse to address algorithmic harm and discrimination as well. The right to explanation and right to erasure (the 'right to be forgotten'), together, offer agency over one's digital self.

While the 2023 Digital Personal Data Protection Act is informed by principles of consent, purpose limitation, and accountability, it does not specifically address automated decision systems, AI profiling, or cross-border data flows. The EU approach demonstrates a dignity-centric framework where technology serves the individual, not the other way around.

8.3. Council of Europe and AI Ethics

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+). Revised in 2018, this instrument went beyond data protection to consider the "inherent dignity of the human person." It requires states to ensure that any AI or data-processing operation treats an individual fairly, transparently, and without discrimination. In its 2021 Recommendation on the Ethical Principles of AI, the Council cited dignity as an inviolable principle and insisted on human discretion in matters that impact individuals' rights, welfare, or reputation.

This is also heightened by the European Commission's AI Act (2024), which categorizes AI systems according to risk—unacceptable, high, limited, and minimal. AI systems that manipulate human conduct or permit real-time biometric surveillance of individuals in public places are deemed an unacceptable risk and thus illegal. The Act exemplifies the risk-based, human-rights-aligned governance framework which India could adopt in the evolution of its AI policy.

European Court of Human Rights (ECHR) focuses on the 'surveillance and biometric retention' aspects in 'Peck v. United Kingdom' (2003) and 'S. and Marper v. United Kingdom' (2008) cases, and stresses the importance of 'proportionality and legality' in these cases.

8.4. Lessons for India

Although Puttaswamy and the DPDP Act of 2023 still leaves India's framework evolving and institutionally frail, foundational values still intertwine with Puttaswamy and global regimes. While best practices bypass foundational values in the case of the EU, the absence of independent oversight and unregulated AI ethics starkly contrast with the EU's rights-first approach. Hence, sustaining the integration of international best practices would require:

1. Including dignity as a statutory principle in the next round of amendments to the DPDP Act and future AI governance legislation.
2. Automated decision-making systems, especially those with welfare, policing, and biometric ID functions, must have reliable human oversight.
3. An independent office of the proposed consolidated Data and AI Regulator, equivalent to the European Data Protection Board.
4. Compliance with international due diligence standards under the UNGPs to ensure digital platforms and AI developers anticipate, mitigate, and address rights infringements.

9. Conclusion and Suggestions

Digital dignity sees the governance and the technologisation of the human right within the moral and legal human rights framework. Given the empirical and the moral realities of the digital and the physical worlds, the ability to control one's data, one's image, and one's algorithmic representation is increasingly the desiderata of personhood. The Supreme Court recognized, K. S. Puttaswamy v. Union of India, that the right of privacy is a facet of the dignity

and liberty. In contrast, the uses of surveillance technologies, artificial intelligence and synthetic media freely speak to the need for more potent defenses.

The case of Pegasus spyware and the completely unregulated use of deepfakes is a unilateral collapse of technological dominion that, threatens individual self-determination and social trust. The right to a balanced and proportionate law that is accountable and transparent, must govern the State's interest in the control of crime and security. The Digital Personal Data Protection Act, 2023 is a step, in India, towards data constitutionalism, but algorithmic unaccountability, the absence of human oversight, and the absence of independent regulation remain gaps.

According to the National Crime Records Bureau, the latest figures reveal near doubling trends in the disguised impersonation, identity theft, and cyber-harassment. This reflects the advancement of technology and the inadequate response to weak countermeasures. Expanding scepticism on the monitoring of these crimes may, however, entail greater violations of dignity. This, combined with the most recently developed digital technologies, calls for the development of the digital policy in India to encompass digital loss governance, or the governance loss in the digital rights of constituents.

Suggestions

1. Consolidated Digital Rights Legislation - Complete and consolidate the digital rights and technology ethics legislation by substituting 'digital dignity' as a legal right, and integrating the disparate laws with the DPDP, IT Act, and AI governance legislation.
2. Autonomous Oversight - Establish a standalone Data and AI Regulatory Authority to over-sight and sanction the use of predicated surveillance, governance AI, and accountability.
3. Transparency in Algorithms - Legislation on public Algorithmic Impact Assessments, and in assessments the disclosure of patterns demonstrating bias and accuracy on high-stake AI instruments.
4. Deepfake Legislation - Amend the IT Act to include the criminalization of rampant distribution of deepfake technology aimed to deceive and of deepfake technology to be used in the arts or for discourse in the public

5. Reform in Surveillance- Introduce a necessary policy of requiring judicial authorization in the use of spyware and interception tools. Incorporate civilian accountability through public audits and oversight of civilian surveillance systems.
6. Evolving Jurisprudence and Policy- Add protection of digital freedom and harvest-based algorithms as part of Article 21.

In the digital dispensation, the element of a person's dignity to be preserved is their digital persona. For the said dignity to be preserved, there must be a clear, concrete, and rights-based regulation that integrates technology within a human rights and constitutional framework.