LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Digital Rights as Fundamental Rights: Privacy, Ai and Article 21 in the age of the Digital Personal Data Protection Act, 2023

Author
Abhishek Gandhi
Priyanka

Digital Rights as Fundamental Rights: Privacy, Ai and Article 21 in the age of the Digital Personal Data Protection Act, 2023

Abhishek Gandhi
Rayat Bahra University

Priyanka
Assistant Professor
Rayat Bahra University

Abstract

The swift expansion of digital technologies has reshaped interactions among individuals, governmental bodies, and private enterprises, presenting substantial obstacles concerning confidentiality, data security, and digital independence. The verdict in Justice K.S Puttaswamy v. Union of India acknowledges confidentiality as an element inherent to the entitlement to existence and individual autonomy as enshrined in Article 21 of the Indian Constitution. This determination stands as a notable advancement in Indian constitutional jurisprudence, offering assistance to numerous others navigating the digital sphere. The enactment of the Digital Personal Data Protection Act, 2023, further underscores the government's endeavor to oversee the acquisition, handling, and safekeeping of personal data within an increasingly data-driven environment. This Research Paper delves into the significance of Digital Rights as an integral aspect of fundamental rights as guaranteed under Article 21 of the Indian Constitution. It also includes a conversation on how the entitlement has evolved to encompass the entitlement to confidentiality, the entitlement to informational self-determination, and protection against unwarranted digital monitoring. Additionally, the research scrutinizes the Digital Personal Data Protection Act, 2023, to assess its capacity to achieve equilibrium among progress, national interest, and the constitutional entitlements of the populace. While the Act endeavors to institute a framework for data management and responsibility, notable reservations arise from the waivers extended to the government, constrained recourse options for users, and the inadequate provision addressing AI-driven infringements. A comprehensive assessment of the constitutional validity of digital entitlements unveils their nature as indispensable human rights. The study concludes that a regulatory structure rooted in rights and centered around citizens is imperative to uphold democratic principles, dignity, and personal independence in the era of AI and digital administration.

Keywords: *Digital Rights, Article 21 ,Right to Privacy, Artificial Intelligence (AI) , Digital Personal Data Protection Act, 2023*

Introduction

The swift development of digital tech has reshaped contemporary society in remarkable ways. The internet, artificial intelligence (AI), extensive data examination, biometric identification tools, cloud infrastructure, and social networking sites have become indispensable to daily existence. While these tech advancements have bettered communication, administration, trade, medical services, and learning, they have concurrently brought about significant worries about secrecy, monitoring, data exploitation, and algorithmic prejudice. In this digital era, personal data has materialized as one of the most prized assets, frequently called the "new oil." Thus, safeguarding digital entitlements has turned into a crucial facet of constitutional administration. In India, the notion of digital entitlements has steadily taken shape via legal interpretation, particularly under Article 21 of the Constitution, which ensures the entitlement to life and individual autonomy.

The pivotal ruling in Justice K.S. Puttaswamy v. Union of India acknowledged secrecy as a basic entitlement inherent to life and autonomy under Article 21. This ruling established the constitutional basis for data safeguarding and digital secrecy in India. Subsequent to this advancement, Parliament put into effect the Digital Personal Data Protection Act, 2023 to oversee the handling of digital personal data and to equalize the entitlements of individuals with the justifiable requirements of the State and enterprises.Concurrently, the expansion of AI technologies has heightened discussions regarding monitoring, profiling, automated judgment, algorithmic leaning, and the moral utilization of personal data. AI systems depend significantly on vast datasets, frequently encompassing confidential personal information. Therefore, the correlation between AI governance, secrecy entitlements, and constitutional safeguards has gained increasing significance. This research document scrutinizes the unfolding of digital entitlements as basic entitlements in India with particular focus on secrecy, AI, and Article 21 within the framework of the Digital Personal Data Protection Act, 2023 (DPDP Act). It fundamentally assesses constitutional legal concepts, legal stipulations, and arising difficulties in the digital epoch.

Meaning and Breadth of Digital Entitlements

Digital entitlements denote the privileges and liberties of persons in the electronic realm. These entitlements encompass the entitlement to confidentiality, data security, the ability to communicate ideas unrestrictedly via the internet, access to the internet, safeguarding against unlawful monitoring, and authority over private data. In contemporary constitutional republics, digital

entitlements are progressively perceived as expansions of established human entitlements.[1]

The notion of digital entitlements takes in multiple aspects:

- Entitlement to Seclusion in the Digital Environment
- Entitlement to Data Security
- Entitlement to Informational Independence
- Liberty of Speech and Articulation Online
- Entitlement to Internet Access
- Safeguarding from Broad Monitoring
- Entitlement to Protection from Algorithmic Bias

Digital entitlements are vital because digital infrastructures and AI systems constantly gather, handle, keep, and assess private data. Absent sufficient legal shields, people could be at risk of identity fraud, data infringements, online offenses, and governmental monitoring.[2]

In India, the constitutional justification for digital entitlements mainly stems from Articles 14, 19, and 21 of the Constitution. Among them, Article 21 has been the most vital in widening the purview of privacy and respect in the digital epoch. The Supreme Court has construed Article 21 extensively to encompass assorted derivative entitlements crucial for residing with respect, including the entitlement to privacy, self-determination, and informational command.[3]

When the Puttaswamy ruling acknowledged privacy as a basic right, it signaled a groundbreaking change in constitutional law. The Court asserted that privacy is inherent to human dignity and individual freedom. It underscored that informational privacy is a vital element of self-determination in the age of digital technology. The ruling also stipulated that any limits on privacy must meet the standards of legality, necessity, and proportionality.

The rise of AI innovations has additionally muddled the matter of digital rights. AI systems can handle enormous volumes of data, detect conduct trends, anticipate inclinations, and execute automated choices. These technologies are commonly utilized in financial services, medical care, law enforcement, administration, and online retail. Despite the considerable advantages of AI, it also provokes constitutional and moral dilemmas.[4]

---

[1] N.S. Nappinai, *Cyber Law and Privacy in India* 45 (LexisNexis, New Delhi, 2021).

[2] Usha Ramanathan, "Privacy, Security and Information," 52(1) *Economic and Political Weekly* 35 (2017).

[3] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

[4] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," 51 *U.C. Davis Law Review* 399 (2017).

Algorithmic discrimination is one of the main issues. AI systems frequently use opaque algorithms that have been trained on skewed datasets. Because of this, these systems may discriminate based on socioeconomic class, gender, caste, or religion. Automated decision-making may have a negative impact on social benefit distribution, financial access, and employment prospects. Thus, the ideals of equality under Article 14 and dignity under Article 21 may be violated by the lack of accountability and transparency in AI governance.[5]

A further worry involves monitoring and data categorization. State entities and private companies are utilizing facial recognition technology, biometric data banks, and forecasting methods to observe people more and more. Too much monitoring might create a "suppressing impact" on the freedom to speak and express oneself, as guaranteed by Article 19(1)(a). It could also weaken democratic involvement and individual independence.[6]

By establishing a legal framework for handling personal data, the Digital Personal Data Protection Act of 2023 aims to ease some of these concerns. The Act recognizes the rights of "Data Principals," including the right to see facts, data rectification, data deletion, complaint settlement, and consent-driven processing. Additionally, it imposes obligations on "Data Fiduciaries" to ensure the proper and trustworthy handling of personal information..[7]

But there has also been criticism of the DPDP Act. The State's extensive exclusions in issues pertaining to national security, public order, and sovereignty are one of the main criticisms. Opponents contend that these exceptions could allow for excessive state surveillance and erode the right to privacy. Additionally, there are major loopholes in the Act's protection of citizens from automated harms because it does not fully control AI systems or algorithmic accountability.

Another significant aspect of digital rights is the ability to access the internet. Under Articles 19(1)(a) and 19(1)(g), the Supreme Court acknowledged internet connectivity as essential to freedom of speech and commerce in Anuradha Bhasin v. Union of India.[8] In today's world, having the ability to connect to the internet is critical for learning, work, medical care, finance, and taking part in discussions about democracy. As a result, being left out of the digital world can cause individuals to be excluded socially and economically.

---

[5] Katharina Zweig, *Algorithmic Decision-Making and Human Rights* 88 (Oxford University Press, Oxford, 2022).

[6] Shoshana Zuboff, *The Age of Surveillance Capitalism* 210 (Profile Books, London, 2019).

[7] Digital Personal Data Protection Act, 2023, ss. 4–15.

[8] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

Digital freedoms are strongly associated with the concept of moral principles within a constitutional framework and democratic administration. The Constitution seeks to safeguard individual self-respect, freedom, and fairness against unreasonable government interference. In today's digital world, these constitutional principles must apply to the online world and technological management. Consequently, legal structures governing AI, monitoring, and information handling must function within constitutional boundaries and uphold essential rights..[9]

In summary, digital entitlements have grown into vital facets of contemporary constitutional systems. The proliferation of AI innovations and virtual infrastructures has produced both novel prospects and fresh menaces to confidentiality, respect, and independence. Article 21 within the Indian Constitution has risen to prominence as the foundation for safeguarding digital entitlements via judicial elucidation. The Digital Personal Data Protection Act, 2023 signifies a noteworthy legislative action regarding data management; nevertheless, considerable obstacles persist concerning monitoring, governmental waivers, and AI responsibility. Consequently, India should embrace a rights-focused digital management structure that harmonizes technological progress with constitutional liberties, thereby guaranteeing that human respect and individual independence are safeguarded in the digital epoch.

Article 21 and the Progression of Privacy Entitlements

Article 21 of the Constitution of India stipulates that:

"No individual shall be stripped of their life or individual freedom apart from according to protocol sanctioned by legislation.[10]

This clause has surfaced as a particularly vibrant and far-reaching basic right within the Indian constitutional system. The judiciary has, over time, construed Article 21 broadly to encompass different rights vital for guaranteeing human worth and significant living. The Supreme Court has asserted that the right to life as per Article 21 isn't just limited to mere physical survival but also entails the entitlement to exist with self-respect, liberty, and independence. As a result, entitlements like the right to a means of support, well-being, learning, a unpolluted surrounding, housing, and confidentiality have been acknowledged as essential elements of Article 21.

At first, though, the entitlement to confidentiality wasn't explicitly acknowledged in the Constitution of India. In earlier constitutional legal theory,

[9] Gautam Bhatia, *The Transformative Constitution* 315 (HarperCollins, New Delhi, 2019).

[10] INDIA CONST. art. 21.

the Supreme Court took on a limited understanding of privacy entitlements. In M.P. Sharma v. Satish Chandra, the Court stated that the Constitution didn't openly recognize an entitlement to confidentiality equivalent to the Fourth Amendment of the United States Constitution.[11] Similar to this, the majority ruling in Kharak Singh v. State of Uttar Pradesh rejected police domiciliary visits as a violation of individual liberty while refusing to acknowledge privacy as a fundamental constitutional right.[12]

Despite these initial restrictions, judges' views on privacy eventually changed. The Supreme Court started recognizing privacy as a crucial component of liberty and dignity in later instances like Gobind v. State of Madhya Pradesh and R. Rajagopal v. State of Tamil Nadu. The Court acknowledged that people have the right to protect private affairs from needless government interference. The eventual constitutional recognition of privacy as a basic right was made possible by these rulings.

The most significant change came in 2017 with the historic ruling in Justice K.S. Puttaswamy v. Union of India. The right to privacy is a fundamental right safeguarded by Article 21 and Part III of the Constitution, according to a unanimous ruling by a nine-judge Supreme Court constitutional bench..[13] The Bench stated that personal space is fundamental to existence, independence, self-respect, and personal freedom. This verdict reversed the prior limited viewpoints articulated in M.P. Sharma and Kharak Singh insofar as they rejected constitutional safeguards for personal space.

The Puttaswamy verdict greatly broadened the sense and reach of personal space in the Indian constitutional framework. The Bench noted that personal space isn't a uniform idea but encompasses various aspects crucial for human independence and self-respect.

These encompass:

- Physical personal space
- Knowledge-based personal space
- Freedom to choose
- Safeguarding of private details
- Self-respect and personal freedom

Physical personal space shields people from bodily invasions and unapproved healthcare interventions. Freedom to choose encompasses the liberty to make intimate individual decisions regarding matrimony, relatives, reproductive entitlements, and way of life. Knowledge-based personal space, which has

---

[11] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

[12] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

[13] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

attained enormous significance in the electronic period, alludes to a person's entitlement to manage private details and decide how such details are amassed, handled, and disseminated.[7]

The Bench acknowledged that technological progress and digitalization have altered the essence of personal space worries. In today's world, people regularly exchange personal details via smartphones, biometric identification systems, monetary dealings, web platforms, and social networking sites. Governments and private firms progressively depend on data examination, artificial intelligence (AI), and monitoring technologies to oversee and forecast human conduct. Consequently, knowledge-based personal space has turned into one of the most vital constitutional worries in the electronic age.[14]

- Crucially, the Supreme Court established a three-part test in Puttaswamy to assess whether limitations on privacy rights are constitutional. The Court states that any interference with privacy must meet the following requirements:
- Legality: The restriction must be permitted by a legitimate legislation.
- Legitimate State Goal: A legitimate governmental goal must be pursued by the restriction.
- Proportionality: The degree of interference must be commensurate with the desired outcome.[15]

The constitutional standard controlling state actions pertaining to data collecting, digital monitoring, surveillance, and AI-driven governance tools is now this three-fold test. It guarantees that the government cannot arbitrarily interfere with private affairs without a constitutional basis.

A key role in the larger context of privacy rights is played by informational privacy. An individual's control over the gathering, storing, using, and sharing of personal data is known as informational privacy. Every day, massive volumes of personal data are created and processed in the digital ecosystem via online activities, biometric systems, e-commerce platforms, artificial intelligence applications, and cloud-based services.[16]

Unauthorized data sharing, data breaches, profiling, behavioral manipulation, cybersecurity threats, and identity theft have become major concerns due to the growing commercialization and exploitation of personal data. Sensitive personal data is frequently gathered by digital networks without meaningful consent,

---

[14] Shoshana Zuboff, *The Age of Surveillance Capitalism* 221 (Profile Books, London, 2019).
[15] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[16] N.S. Nappinai, *Cyber Law and Privacy in India* 63 (LexisNexis, New Delhi, 2021).

raising the possibility of abuse and exploitation. These issues are made worse by AI systems' heavy reliance on large datasets for algorithm training and automated decision-making.[17]
Recognizing these risks, the Supreme Court in Puttaswamy underscored the pressing requirement for a strong data protection system in India. The Court remarked that informational privacy is a crucial element of human dignity, freedom, and self-determination. It recognized that both governmental and non-governmental bodies have the technological capacity to encroach on personal lives via surveillance infrastructures, data interpretation, and algorithmic monitoring.

This constitutional acknowledgement of informational privacy had a direct impact on the passage of the Digital Personal Data Protection Act, 2023. The Act aims to govern the handling of digital personal data, protect individual entitlements, and define responsibilities for organizations dealing with personal information. It signifies a key legislative measure toward harmonizing technological advancement with constitutional assurances of privacy and personal freedom in the digital era.

The Digital Personal Data Protection Act, 2023
The Digital Personal Data Protection Act, 2023 represents India's inaugural all-inclusive legislation exclusively focused on safeguarding digital personal data. The Act endeavors to harmonize the rights of individuals with the legitimate processing requirements of governments and enterprises.

Objectives of the Act
The DPDP Act seeks:

- To safeguard digital personal data
- To govern legitimate data handling
- To define responsibilities for data fiduciaries
- To grant rights to data principals
- To ensure accountability and openness

The Act is applicable to digital personal data obtained online or digitized data from offline sources. It also has extraterritorial reach where handling pertains to providing goods or services within India.

[17] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," 51 *U.C. Davis Law Review* 399 (2017).

Key Attributes of the Act

1. Consent-Based Structure

The Act places emphasis on consent-based handling of personal data. Data fiduciaries must secure explicit and informed consent before handling personal data.

2. Rights of Data Principals

The Act grants numerous rights to individuals, including:

• Entitlement to access information

- Entitlement to rectification and deletion
- Entitlement to resolution of grievances
- Entitlement to revoke consent
- Entitlement to designate representatives

3. Obligations of Data Fiduciaries

Organizations handling data must:

- Guarantee data security
- Avert data infringements
- Inform authorities regarding infringements
- Erase unnecessary data
- Uphold transparency

4. Protection of Children's Data

The Act mandates stricter responsibilities concerning children's personal data and prohibits tracking and targeted marketing aimed at minors.

5. Data Protection Board

The Act establishes the Data Protection Board of India to address complaints and ensure adherence.

Artificial Intelligence and Privacy Worries

Artificial Intelligence (AI) has surfaced as one of the most groundbreaking technologies of the twenty-first century. AI-powered systems are progressively utilized in governance, commerce, healthcare, policing, education, banking, transportation, and finance. These systems process vast quantities of personal and behavioral data to discern patterns, generate predictions, and automate determinations. AI technologies have greatly enhanced efficiency, productivity, and public service provision. Nevertheless, alongside these merits, AI also presents significant constitutional, ethical, and legal issues pertaining to privacy, freedom, equality, and human dignity.[18]

[18] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," 51 *U.C. Davis Law Review* 399 (2017).

A particularly serious worry linked to AI is widespread monitoring. AI-driven face identification systems, biometric authentication technologies, predictive law enforcement tools, and electronic monitoring systems empower governments and businesses to oversee people to an unparalleled degree. Monitoring technologies can constantly gather and examine private data such as geographical position, facial gestures, communication styles, and internet habits. While monitoring might be defended for homeland security or law enforcement objectives, extreme and unrestricted monitoring puts at risk individual freedoms and informational privacy safeguarded by Article 21 of the Constitution. Continuous observation might produce a repressive effect on free expression and democratic involvement because people might be afraid of being observed or categorized by the powers that be. Another substantial worry is algorithmic partiality and prejudice. AI systems are educated utilizing vast datasets that might harbor past biases and societal disparities. As a result, AI algorithms might discriminate against people based on race, gender, social class, religion, heritage, or financial standing. For instance, skewed AI systems might unjustly reject credit, job prospects, insurance coverage, or civic amenities to marginalized populations. Such unjust results directly jeopardize the constitutional assurance of equality under Article 14 of the Constitution. Because a lot of AI systems function as impenetrable entities, it turns out to be demanding to pinpoint or contest unfair decision-making procedures.

AI likewise gives rise to apprehensions with respect to automated judgment. Progressively, AI systems impact judgments pertaining to employing, healthcare detection, criminal equity, policing, monetary administrations, and academic opportunities. Automated systems can make judgments without substantial human contribution. Nevertheless, insufficient openness and responsibility in automated judgment may contravene standards of procedural impartiality and natural law. Individuals impacted by AI-prompted judgments may not understand how or the reasons for a certain result..[19] Within constitutional democracies, impartiality and openness form integral elements of legal principles. Thus, obscure algorithmic governance presents significant judicial and moral quandaries.

User profiling and behavioral manipulation embody another escalating menace within the digital era. Social media venues, e-commerce enterprises, and digital promotional networks employ AI algorithms to assess user actions, inclinations, emotions, and political leanings. These mechanisms forecast and sway consumer decisions, online participation, and even voting patterns. Tailored commercials and suggestion algorithms exist to amplify user focus and behavioral impact. These actions could compromise individual independence

[19] Frank Pasquale, *The Black Box Society* 34 (Harvard University Press, Massachusetts, 2015).

and intellectual liberty by delicately affecting human conduct absent explicit consent. AI technologies furthermore rely significantly on broad data compilation and utilization. AI frameworks necessitate extensive datasets for instruction and enhancement. Frequently, private details are amassed lacking substantial or knowledgeable authorization. Digital platforms accumulate delicate data concerning well-being, funds, location, correspondence, and individual predilections. Unapproved acquisition, retention, and dissemination of such details engender grave confidentiality hazards, potentially including identity fraud, cybersecurity transgressions, and abuse of private data. Academics and policy specialists have accordingly contended that established judicial structures are inadequate for overseeing AI-related detriments and digital exploitation proficiently.

AI Governance and the DPDP Act

Even though the Digital Personal Data Protection Act, 2023 does not explicitly oversee artificial intelligence, it institutes several crucial protections pertinent to AI-driven mechanisms handling private data. The Act establishes duties concerning authorization, objective constraints, liability, and data defense that indirectly pertain to AI technologies.[20]

A foundational tenet of the DPDP Act revolves around agreement and openness. AI architectures utilizing private data must adhere to legitimate agreement mandates. People must be kept abreast of the manner in which their private data is obtained, handled, kept, and put to use. Openness is vital to guarantee that people maintain authority over their virtual identities and private details.

The Act also encourages the tenet of data lessening, which limits needless or extreme data procurement by AI architectures. Organizations are asked to procure only data that is vital for a definite and lawful intention. This tenet is geared toward diminishing the hazard of extensive data misuse and meddlesome profiling.

Moreover, the DPDP Act places accountability responsibilities upon Data Fiduciaries. Organizations employing AI architectures may be deemed accountable for careless handling, abuse, or unapproved revelation of private details. AI enterprises and virtual platforms are asked to embrace sensible protections to safeguard data security and avert unapproved access, violations, or cyberattacks. In spite of these protections, the DPDP Act is subject to multiple constraints pertaining to AI governance. The Act does not expressly control algorithmic leaning or biased automated decision-making. It also neglects to grant a "right to explanation," which would permit people to grasp

[20] Digital Personal Data Protection Act, 2023, ss. 4–15.

how AI architectures reach conclusions impacting them. Furthermore, there are scant stipulations concerning algorithmic openness and detached oversight. Critics also contend that the sweeping exceptions extended to government bodies may impair privacy safeguards and elevate the chance of surveillance abuse. Therefore, numerous academics assert that India necessitates a thorough and committed AI regulatory structure in conjunction with the DPDP Act.

Virtual Rights and Human Decency

Human decency creates the fundamental worth underlying Article 21 of the Constitution. Privacy, independence, liberty, and personal freedom are vital facets of decency. In the virtual age, constant surveillance, profiling, and data misuse can weaken individual decency and human personality.[21]

In Justice K.S. Puttaswamy v. Union of India, the Supreme Court highlighted that privacy allows people to make their own decisions free from outside influence. Therefore, digital rights safeguard not just private data but also individual liberty and democratic liberties. By influencing decisions and limiting individual autonomy, artificial intelligence (AI) technology that can forecast and impact human behavior could jeopardize constitutional liberties.
Similar to this, extensive data collecting could lead to a "surveillance society" in which people are always afraid of being watched by businesses or governments. The rule of law and constitutional democracy are incompatible with such circumstances. Thus, in the era of AI, safeguarding digital rights has become crucial to maintaining human dignity, freedom, and democratic governance.[22]

State Surveillance and Constitutional Challenges

a) A chief constitutional quandary of the information age is the growth of governmental monitoring capabilities. Administrations are progressively dependent on technological tools for governance, policing, and purposes of national safety. In India, worries have surfaced concerning systems for facial identification, Aadhaar-connected data repositories, wiretapping, monitoring of social media, suspension of internet service, and monitoring via biometrics.
b) Even though national safety is a valid aim of the government, too much monitoring could encroach upon the right to privacy as guaranteed by Article 21. The constitutional legitimacy of monitoring methods must adhere to the criteria specified in the Puttaswamy ruling, specifically:

- A law must exist.
- A legitimate governmental objective must be in place.
- Monitoring must be necessary and proportionate.

---

[21] *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608.
[22] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

- There must be procedural protections against misuse.[23]

Opponents contend that the DPDP Act allows significant exceptions for governmental bodies regarding sovereignty, public order, and State security. These wide-ranging exceptions could weaken constitutional protections if used without sufficient judicial or legislative supervision.

Thus, strong checks and balances are crucial to guarantee that monitoring capabilities do not turn into tools of unchecked governmental power.

Related View: GDPR and Indian System

In today's digital age, data security has become a key issue for constitutional democracies globally. The growing use of artificial intelligence (AI), cloud computing, social media platforms, and digital governance tools has heightened the demand for strong legal protections to safeguard informational privacy and individual independence. Among worldwide data security systems, the General Data Protection Regulation (GDPR) is generally considered a leading and thorough regulatory approach. The GDPR acknowledges data security as a basic right and sets up detailed protections for the gathering, handling, storage, and sharing of personal data.[24]

India's first comprehensive law pertaining to the protection of digital personal data is the Digital Personal Data Protection Act, 2023 (DPDP Act). The constitutional acknowledgment of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India had a major impact on the DPDP Act's passage.[25] Even though the Indian structure has some traits in common with the GDPR, noteworthy discrepancies exist concerning the extent, legal arrangement, and individual safety measures.

One key contrast between the GDPR and the DPDP Act pertains to the reach of implementation. The GDPR broadly relates to all types of personal data handling, whether electronic or physical, performed within the European Union or impacting EU citizens. Conversely, the DPDP Act mainly oversees electronic personal data and personal data converted to digital form from physical origins. This more confined scope restricts how far the Indian structure extends compared to the GDPR.

Another significant divergence involves delicate personal data. Under the GDPR, particular groupings of delicate personal information like biometric details, health information, racial heritage, political views, religious convictions, and sexual preference are given stronger legal safety. Handling of such

---

[23] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

[24] Paul De Hert & Vagelis Papakonstantinou, "The New General Data Protection Regulation," 35(3) *Computer Law and Security Review* 179 (2016).

[25] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

information faces stricter stipulations and defenses. However, the DPDP Act doesn't form a separate grouping for delicate personal information. Detractors contend that the lack of distinct safety could undermine defenses pertaining to highly sensitive information like biometric and health details.
The GDPR also furnishes clear safety measures against automated decision-making and profiling. Article 22 of the GDPR awards people the entitlement to not be exposed to verdicts grounded only in automated handling that considerably affect their entitlements or interests. People are also entitled to substantial details regarding the logic involved within such automated systems. By comparison, the DPDP Act furnishes only reduced safety measures concerning automated decision-making and algorithmic clarity. The absence of an "entitlement to explanation" has been criticized as a major void in India's data protection arrangement, notably in the age of AI governance.

Organizational systems also vary considerably between the two structures. The GDPR sets up robust and autonomous supervisory bodies in each member nation to guarantee adherence and enforcement. These bodies hold extensive investigatory and corrective authorities. In contrast, the DPDP Act forms the Data Protection Board of India as the main regulatory authority. However, worries have been voiced regarding the autonomy, authorities, and effectiveness of the Board, especially because the Central Government keeps considerable influence over its makeup and operation.

Another vital contrast relates to waivers granted to the State. Under the GDPR, waivers pertaining to national security and public order are comparatively constrained and subject to strict proportionality mandates. Conversely, the DPDP Act grants broader waivers to government bodies on reasons such as sovereignty, security of the State, public order, and prevention of offenses. Detractors argue that these broad waivers may undermine constitutional safety measures pertaining to privacy and informational independence under Article 21.[26]

Regardless of these variations, the DPDP Act signifies a noteworthy move toward acknowledging digital entitlements within India's charter. It sets forth authorized responsibilities pertaining to permission, data defense, answerability, and problem resolution. It also embodies India's endeavor to even out technological advancement, financial expansion, and charter entitlements in the digital period.

[26] Apar Gupta, "Data Protection and Surveillance Concerns under the DPDP Act," 58(42) *Economic and Political Weekly* 12 (2023).

Hindrances in Application

Even though the DPDP Act is a groundbreaking enactment, several hindrances are still present concerning its successful application. One of the key hindrances is the insufficient community understanding regarding digital secrecy entitlements. A considerable section of the populace is still ignorant of how private data is gathered, handled, and utilized by digital platforms. Without sufficient understanding and digital proficiency, citizens may be incapable of using their entitlements successfully.

Technological convolution introduces another hindrance. AI systems and digital technologies advance swiftly, frequently exceeding legal and regulatory systems. Regulatory bodies may find it difficult to tackle emerging technologies such as facial recognition, generative AI, predictive analytics, and algorithmic characterization.

Cross-border data transmissions also create enforcement hardships. Global technology firms habitually store and handle data across numerous territories. Discrepancies between national legal systems complicate regulatory enforcement and data defense adherence. The global characteristic of digital platforms consequently necessitates international collaboration and unified standards.

Cybersecurity menaces additionally undermine successful application. Data infringements, ransomware assaults, hacking occurrences, and cyber deceit continue to escalate in spite of legal protections. Organizations managing private data must capitalize intensely in cybersecurity infrastructure and technical proficiency to avert unauthorized access and abuse.[27]

Another significant worry pertains to extensive governmental exemptions under the DPDP Act. Overly broad exemptions for government bodies could weaken privacy safeguards and heighten the possibility of unjustified monitoring. Critics contend that efficient judicial oversight and autonomous review systems are crucial for preventing the misuse of surveillance authorities.

The absence of explicit AI regulation also stands out as a noteworthy constraint. The DPDP Act doesn't thoroughly tackle issues such as algorithmic responsibility, automated judgment processes, deepfakes, AI prejudice, or requirements for explainability. As AI increasingly shapes governance and commerce, India might need a dedicated AI regulatory structure in addition to data protection laws.

[27] Usha Ramanathan, "Privacy and Data Protection in India," 52(1) *Economic and Political Weekly* 35 (2017)

Successful execution also relies on institutional capabilities and technical know-how. Regulatory bodies should have enough independence, technological insight, and enforcement authority to oversee compliance successfully. Without robust institutional systems, legal safeguards may stay ineffective in actual application.

Judicial Function in Protecting Digital Entitlements

The judiciary is essential for protecting digital entitlements within India's constitutional structure. Indian courts have regularly broadened the scope of fundamental entitlements to adjust to evolving technological landscapes. Through innovative constitutional interpretation, the judiciary has acknowledged privacy, dignity, independence, and informational authority as vital elements of Article 21.

Significant judicial contributions encompass the recognition of privacy as a fundamental entitlement, defense against unjustified monitoring, creation of the proportionality principle, and emphasis on human dignity and individual independence. The Supreme Court has repeatedly asserted that technological progress cannot supersede constitutional liberties.

Looking ahead, constitutional lawsuits are anticipated to handle various rising digital issues, including:

- AI prejudice and discrimination
- Facial recognition technologies
- Deepfakes and disinformation
- Biometric monitoring
- Data localization mandates
- Algorithmic transparency and responsibility

As technology advances further, the judiciary will stay crucial in determining the constitutional parameters of digital governance in India. Courts will have a vital role in harmonizing innovation, national security, and individual liberties to guarantee that constitutional democracy and human dignity are preserved in the digital era.

Conclusion

The digital transformation has profoundly reshaped society, governance, and personal life. In this swiftly changing technological setting, digital entitlements have surfaced as vital components of constitutional democracy and human dignity. The acknowledgment of privacy as a fundamental entitlement under Article 21 via the Puttaswamy ruling signified a watershed moment in Indian constitutional legal principles. It established the constitutional groundwork for safeguarding informational privacy, independence, and personal freedom in the digital age.

The passage of the Digital Personal Data Protection Act, 2023 signifies a noteworthy legislative endeavor to protect personal data and regulate digital ecosystems. The Act presents significant tenets like consent, responsibility, transparency, and data security. However, the swift advancement of AI technologies introduces fresh legal and ethical quandaries that go beyond standard data protection worries.

AI systems hold immense capacity to influence decisions, monitor conduct, and mold public dialogue. Absent suitable protections, they can jeopardize privacy, equality, independence, and democratic freedoms. Therefore, India must create a thorough AI governance structure that complements the DPDP Act and guarantees constitutional responsibility.

Ultimately, digital entitlements aren't merely technological concerns but fundamental human rights matters. The protection of privacy, dignity, and independence in cyberspace is vital for upholding constitutional values in the twenty-first century. The destiny of Indian democracy will hinge significantly on how successfully the State, judiciary, legislature, and civil society balance technological innovation with the protection of fundamental entitlements.

Bibliography

- Binns, R. (2018). Understandings of Privacy in AI and Data-Driven Technologies. Journal of Data Protection & Privacy, 1(1), 4-15.
- Solove, D. J. (2008). Understanding Privacy. Harvard Law Review, 117(7), 2057-2084.
- Westin, A. F. (1967). Privacy and Freedom. New York: Atheneum.
- Kuner, C., Bygrave, L. A., & Docksey, C. (2020). The GDPR: General Data Protection Regulation (EU) 2016/679. Oxford University Press.
- Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13, 203-218.

- Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
- Greenleaf, G. (2014). Global Data Privacy Laws 2013: Thirty-nine Laws, and Still Counting. 24(9), 663-679.
- Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. Proceedings of the 2008 IEEE Symposium on Security and Privacy, 111-125.
- Chandrasekaran, R., & Kumar, S. (2022). AI and Privacy Rights in the Context of Data Protection Laws. International Journal of Law and Information Technology, 30(2), 123-139.

- Sharma, P., & Singh, R. (2023). Digital Personal Data Protection Act, 2023: A New Dawn for Privacy Rights in India. Indian Journal of Law and Technology, 19(1), 45-67.
- Agarwal, P. (2023). Privacy as a Fundamental Right in the Digital Era: An Analysis of Article 21. Journal of Indian Law and Society, 10(2), 89-105.
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1), 119-157.
- Regan, P. M. (2015). When Privacy Fails: The Ethics of Surveillance. University of Chicago Press.
- Gurses, S., & Durmus, S. (2022). AI Governance and Privacy Rights under New Data Protection Frameworks. International Review of Information Ethics, 36, 1-12.
- Shapiro, J. M., & Varian, H. R. (1998). Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618